SECTION 1

1.0 EXECUTIVE SUMMARY

SoftServe Inc. has adopted a HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

SoftServe Inc. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

SoftServe Inc. is a Business Entity, the major goal of the Privacy Rule is to assure individuals healthcare information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and well-being: while satisfying the goals of Covered Entities and HIPAA "Omnibus" final rule.

TABLE OF CONTENT

Section 1

Section 2

Section 3

Section 4

Section 10

Section 11

Section 1.2

Scope of Policies

This policies governs General HIPAA Compliance for **SoftServe Inc.** All personnel of **SoftServe Inc.** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with the Sanction Policies of **SoftServe Inc.**

SECTION 2

Policy Number: 2.0
Effective Date: 3/26/2013
Last Revised: 7/28/14

General HIPAA Compliance Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- ❑ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- ❑ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- ❑ Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to become and to remain in full compliance with all the requirements of HIPAA.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
- ❑ All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with the Document Retention policies of **SoftServe Inc.**

Procedures

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **SoftServe Inc.** commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- ❑ **Privacy Policies and Procedures** -- **SoftServe Inc.** shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.
- ❑ **Privacy Personnel** -- **SoftServe Inc.** shall designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the privacy practices of **SoftServe Inc.**
- ❑ **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the **SoftServe Inc.** (whether or not they are paid by **SoftServe Inc.**). **SoftServe Inc.** shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.
- ❑ **Sanctions** -- **SoftServe Inc.** shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
- ❑ **Mitigation** -- **SoftServe Inc.** shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
- ❑ **Data Safeguards** -- **SoftServe Inc.** shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
- ❑ **Complaints** -- **SoftServe Inc.** shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **SoftServe Inc.** shall explain those procedures in its privacy practices notice.
- ❑ **Retaliation and Waiver** -- **SoftServe Inc.** shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **SoftServe Inc.** shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

- ❑ **Documentation and Record Retention** -- **SoftServe Inc.** shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

HHS Regulations as Amended January 2013
General Rules for Uses and Disclosures of Protected Health Information: Use and Disclosure for Treatment, Payment and Health Care Operations - § 164.502(a)

Standard. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

1. *Covered entities: Permitted uses and disclosures*. A covered entity is permitted to use or disclose protected health information as follows:
   i. To the individual;
   ii. For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
   iii. Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
   iv. Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;
   v. Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
   vi. As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).
2. *Covered entities: Required disclosures*. A covered entity is required to disclose protected health information:
   i. To an individual, when requested under, and required by § 164.524 or § 164.528; and
   ii. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.
3. *Business associates: Permitted uses and disclosures*. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.
4. *Business associates: Required uses and disclosures*. A business associate is required to disclose protected health information:
   i. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

ii. To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

5. *Prohibited uses and disclosures*.

i. *Use and disclosure of genetic information for underwriting purposes*:

Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

A. Except as provided in paragraph (a)(5)(i)(B) of this section:
   1. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
   2. The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
   3. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
   4. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

B. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

ii. *Sale of protected health information*:

A. Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

B. For purposes of this paragraph, sale of protected health information means:
   1. Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.
   2. Sale of protected health information does not include a disclosure of protected health information:

   iii. For public health purposes pursuant to § 164.512(b) or § 164.514(e)

   iv. For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

   v. For treatment and payment purposes pursuant to § 164.506(a);

   vi. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

vii. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

viii. To an individual, when requested under § 164.524 or § 164.528;

ix. Required by law as permitted under § 164.512(a); and

x. For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: General Rules - § 164.306

a. *General requirements*. Covered entities and business associates must do the following:
   1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
   2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
   4. Ensure compliance with this subpart by its workforce.

b. *Flexibility of approach*.
   1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
   2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
      i. The size, complexity, and capabilities of the covered entity or business associate.
      ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
      iii. The costs of security measures.
      iv. The probability and criticality of potential risks to electronic protected health information.

c. *Standards*. A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

d. *Implementation specifications*. In this subpart:
   1. Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

2. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.
3. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must--
    - i. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
    - ii. As applicable to the covered entity or business associate--
        - A. Implement the implementation specification if reasonable and appropriate; or
        - B. If implementing the implementation specification is not reasonable and appropriate--
            1. Document why it would not be reasonable and appropriate to implement the implementation specification; and
            2. Implement an equivalent alternative measure if reasonable and appropriate.

e. *Maintenance*. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii).

Policy Number: 2.1
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Privacy-Official Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ **SoftServe Inc.**, as a Business Associate, recognizes that the designation of a Privacy Official is <u>optional</u> under the HIPAA Rules; and that the designation of a Privacy Official provides numerous benefits to **SoftServe Inc.**

Policy Statement

- It is the Policy of **SoftServe Inc.** to designate and maintain at all times an active HIPAA Privacy-Official.
- The HIPAA Privacy-Official's general responsibilities are to:
  - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
  - Conduct various risk analyses, as needed or required.
  - Manage breach notification investigations, determinations, and responses, including breach notifications.
  - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.

Procedures

SoftServe Inc.'s HIPAA Privacy Official, and his or her designees, shall be responsible for implementing, managing, and maintaining the following procedures:

- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
- Administer patient requests under HIPAA's Patient Rights.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by HIPAA.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Draft and disseminate the Privacy Notice required by the Privacy Rule.
- Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.

- ❑ Oversee employee training in the areas of information privacy and security.
- ❑ Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- ❑ Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of online, web-based applications.
- ❑ Monitor data collected by or posted on our website(s) for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.

HHS Regulations
Personnel Designations - § 164.530(a)

1. *Standard: personnel designations*.
   i. A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
   ii. A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.
2. *Implementation specification: personnel designations*. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

HHS Response to Comments Received
Personnel Designations

Comment: Many of the commenters on this topic objected to the cost of establishing a privacy official, including the need to hire additional staff, which might need to include a lawyer or other highly paid individual.

Response: We believe that designation of a privacy official is essential to ensure a central point of accountability within each covered entity for privacy-related issues. The privacy official is charged with developing and implementing the policies and procedures for the covered entity, as required throughout the regulation, and for compliance with the regulation generally. While the costs for these activities are part of the costs of compliance with this rule, not extra costs associated with the designation of a privacy official, we do anticipate that there will be some cost associated with this requirement. The privacy official role may be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or an information officer or compliance official in a larger institution. Cost estimates for the privacy official are discussed in detail in the overall cost analysis.

Comment: A few commenters argued for more flexibility in meeting the requirement for accountability. One health care provider maintained that covered entities should be able to establish their own system of accountability. For example, most physician offices already have the patient protections incorporated in the proposed administrative requirements – the commenter urged that the regulation should explicitly promote the application of flexibility and scalability. A national physician association noted that, in small offices, in particular, responsibility for the policies and procedures should be allowed to be shared among several people. A major manufacturing corporation asserted that mandating a privacy official is unnecessary and that it would be preferable to ask for the development of policies that are designed to ensure that processes are maintained to assure compliance.

Response: We believe that a single focal point is needed to achieve the necessary accountability. At the same time, we recognize that covered entities are organized differently and have different information systems. We therefore do not prescribe who within a covered entity must serve as the privacy official, nor do we prohibit combining this function with other duties. Duties may be delegated and shared, so long as there is one point of accountability for the covered entity's policies and procedures and compliance with this regulation.

Comment: Some commenters echoed the proposal of a professional information management association that the regulation establish formal qualifications for the privacy official, suggesting that this should be a credentialed information management professional with specified minimum training standards. One commenter emphasized that the privacy official should be sufficiently high in management to have influence.

Response: While there may be some advantages to establishing formal qualifications, we concluded the disadvantages outweigh the advantages. Since the job of privacy official will differ substantially among organizations of varying size and function, specifying a single set of qualifications would sacrifice flexibility and scalability in implementation.

Comment: A few commenters suggested that we provide guidance on the tasks of the privacy official. One noted that this would reduce the burden on covered entities to clearly identify those tasks during the initial HIPAA implementation phase.

Response: The regulation itself outlines the tasks of the privacy official, by specifying the policies and procedures required, and otherwise explaining the duties of covered entities. Given the wide variation in the function and size of covered entities, providing further detail here would unnecessarily reduce flexibility for covered entities. We will, however, provide technical assistance in the form of guidance on the various provisions of the regulation before the compliance date.

Comment: Some comments expressed concern that the regulation would require a company with subsidiaries to appoint a privacy official within each subsidiary. Instead they argued that the corporate entity should have the option of designating a single corporate official rather than one at each subsidiary.

Response: In the final regulation, we give covered entities with multiple subsidiaries that meet the definition of covered entities under this rule the flexibility to designate whether such subsidiaries are each a separate covered entity or are together a single covered entity. (See § 164.504(b) for the rules requiring such designation.) If only one covered entity is designated for the subsidiaries, only one privacy officer is needed. Further, we do not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of this rule are met for each such covered entity.

Policy Number: 2.2
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Policies and Procedures Policy

Assumptions

❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.

❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.

❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.

❑ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.

❑ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.

❑ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

❑ Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

❑ It is the Policy of **SoftServe Inc.** to create and implement appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics.
❑ All policies and procedures shall be updated and amended as needed or as required by law.
❑ All policies and procedures shall be distributed to, or made otherwise available to, the entire workforce.
❑ All policies and procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
❑ All members of the workforce are required to read, understand, and comply with this and all other policies and procedures created and implemented by **SoftServe Inc.**

Procedures

❑ **SoftServe Inc.** shall create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA Rules and Regulations as well as with applicable State laws and statutes.
❑ **SoftServe Inc.** shall designate a qualified individual to assume control of the policies and procedures process. This individual shall report to SoftServe's Compliance Officer and shall execute the creation or revision process in a timely manner, in order to meet the current HIPAA Compliance Deadline of September 23, 2013.
❑ **SoftServe Inc.** shall engage its qualified legal counsel to guide or review the policies and procedures creation/revision process, and to intercede where necessary, to ensure **SoftServe Inc.'s** policies and procedures meet all applicable HIPAA (and other) standards.
❑ **SoftServe Inc.** shall internally publish its HIPAA policies and procedures, when complete, to its workforce members, and shall provide appropriate training to members of its workforce on the interpretation and implementation of its policies and procedures.
❑ **SoftServe, Inc.** has established an Information Security Committee to support the ISMS framework and to periodically review the information security policy (ISMS DOC 6.1 Information Security Committee).
❑ **SoftServe Inc.** has establish a HIPAA Committee in conjunction with the ISM Committee to support and review all securities and HIPPA procedure in accordance with Policies and Procedures and Documentation Requirement - § 164.316

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Policies and Procedures and Documentation Requirements - § 164.316

A covered entity or business associate must, in accordance with § 164.306:

a. *Standard: Policies and procedures*. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

b.

1. *Standard: Documentation*.
   - i. Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
   - ii. If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
2. *Implementation specifications*:
   - i. *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
   - ii. *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
   - iii. *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Policy Number: 2.3
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Privacy Complaints Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- ❑ HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.
- ❑ Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Privacy Officer, or other responsible party (if no Privacy Official has been designated), who shall establish a process and appropriate forms to receive and process complaints.

Procedures

- ❑ All complaints must be submitted in written form, dated and signed by the complainant.
- ❑ **SoftServe Inc.** shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.
- ❑ The designated HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
- ❑ The final resolution or disposition of each complaint shall be documented in accordance with__**SoftServe Inc.’s** Documentation Policy, and shall be retained in accordance with **SoftServe Inc.’s** Documentation Retention Policy.
- ❑ The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
- ❑ In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediation’s may include, but are not limited to:
    - A written apology to the complainant from our organization.
    - Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
    - Financial compensation, if determined to be appropriate by legal counsel and senior management.
    - Sanctions against workforce members, as appropriate to the circumstances.
    - Other unspecified remediation(s), as determined by legal counsel and senior management.
- ❑ For complaints submitted to the federal government, it is the Policy of **SoftServe Inc.** to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in **SoftServe Inc.’s** HHS Investigations Policy.
- ❑ No officer, agent, employee, contractor, temporary worker, or volunteer of **SoftServe Inc.** shall obstruct or impede any investigation in any way, whether internal or federal.

HHS Regulations
The Administrative Requirements: Complaints to the Covered Entity - § 164.530(d)

1. *Standard: complaints to the covered entity*. A covered entity must provide a process for individuals to make complaints concerning the covered entity’s policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.
2. *Implementation specification: documentation of complaints*. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

In the final rule, we retain the requirement for an internal complaint process for compliance with this rule, including the two basic requirements of identifying a contact person and documenting complaints received and their dispositions, if any. We expand the scope of complaints that covered entities must have a means of receiving to include complaints concerning violations of the covered entity’s privacy practices, not just violations of the rule. For example, a covered entity must have a mechanism for receiving a complaint that patient information is used at a nursing station in a way that it can also be viewed by visitors to the hospital, regardless of whether the practices at the nursing stations might constitute a violation of this rule.

HHS Response to Comments Received
The Administrative Requirements: Complaints to the Covered Entity

Comment: Several commenters felt that some form of due process is needed when it comes to internal complaints. Specifically, they wanted to be assured that the covered entity actually hears the complaints made by the individual and that the covered entity resolves the complaint within a reasonable time frame. Without due process the commenters felt that the internal complaint process is open ended. Some commenters wanted the final rule to include an appeals process for individuals if a covered entity's determination in regards to the complaint is unfavorable to the individual.

Response: We do not require covered entities to implement any particular due process or appeals process for complaints, because we are concerned about the burden this could impose on covered entities. We provide individuals with an alternative to take their complaints to the Secretary. We believe that this provides incentives for covered entities to implement a complaint process that resolves complaints to individuals' satisfaction.

Comment: Some commenters felt that the individual making the complaint should exhaust all other avenues to resolve their issues before filing a complaint with the Secretary. A number of commenters felt that any complaint being filed with the Secretary should include documentation of the reviews done by the covered entity.

Response: We reject these suggestions, for two reasons. First, we want to avoid establishing particular process requirements for covered entities' complaint programs. Also, this rule does not require the covered entity to share any information with the complainant, only to document the receipt of the complaint and the resolution, if any. Therefore, we cannot expect the complainant to have this information available to submit to the Secretary. Second, we believe the individual making the complaint should have the right to share the complaint with the Secretary at any point in time. This approach is consistent with existing civil rights enforcement programs for which the Department is responsible. Based on that experience, we believe that most complaints will come first to covered entities for disposition.

Comment: Some commenters wanted the Department to prescribe a minimum amount of time before the covered entity could dispose of the complaints. They felt that storing these complaints indefinitely would be cumbersome and expensive.

Response: We agree, and in the final rule require covered entities to keep all items that must be documented, including complaints, for at least six years from the date of creation.

Comments: Some commenters objected to the need for covered entities to have at least one employee, if not more, to deal with complaints. They felt that this would be costly and is redundant in light of the designation of a contact person to receive complaints.

Response: We do not require assignment of dedicated staff to handle complaints. The covered entity can determine staffing based on its needs and business practices. We believe that consumers need one clear point of contact for complaints, in order that this provision effectively inform consumers how to lodge complaints and so that the compliant will get to someone who knows how to respond. The contact person (or office) is for receipt of complaints, but need not handle the complaints.

SECTION 3

Policy Number: 3.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Business Associates Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to Business Associates, in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.
- ❑ In cooperation with our organization, sub-contractors who are Business Associates work with, use, transmit, and/or receive individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), which is afforded specific protections under HIPAA.
- ❑ **SoftServe Inc.** has the primary responsibility in all Business Associate relationships to ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded.
- ❑ The HIPAA ("Omnibus") Final Rule specifically identifies the following types of entities as Business Associates:
    - Subcontractors.
    - Patient safety organizations.
    - HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
    - E-Prescribing gateways.
    - PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
    - Other firms or persons who "facilitate data transmission" that requires routine access to PHI.
- ❑ The "Minimum Necessary Standard" now applies directly to Business Associates. HIPAA now applies the Minimum Necessary standard directly to Business Associates and their subcontractors. When using, disclosing or requesting PHI, all these entities must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- ❑ Subcontractors of Business Associates are now Business Associates themselves. A subcontractor is defined as a person or entity to whom a Business Associate delegates a function, activity, or service involving Protected Health Information, and who is not a member of the Business Associate's own workforce.

- ❑ As a Business Associate itself, **SoftServe Inc.** is required to enter into a Business Associate contract with any subcontractor who is a Business Associate of ours.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and maintain lawful working relationships with our own Business Associates that are in full compliance with all the requirements of the HIPAA Final "Omnibus" Rule.

Procedures

- ❑ Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
- ❑ With regard to our own Business Associates (sub-contractors), the duties and responsibilities of the designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall include, but are not limited to the following:
  - Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA "Omnibus" Final Rule, and any requirements of State laws in the state(s) where we operate.
  - Ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
  - Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), whether in electronic form ("ePHI") or hardcopy form.
  - Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before entrusting such information to them.
  - Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy and the requirements of HIPAA.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:

S*tandard: Business associate contracts and other arrangements*. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

Business Associate Contracts or Other Arrangements (§ 164.308(b)(1))

In the proposed rule § 142.308(a)(2) "Chain of trust" requirement, we proposed that covered entities be required to enter into a chain of trust partner agreement with their business partners, in which the partners would agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged. This standard has been modified from the proposed requirement to reflect, in § 164.308(b)(1) "Business associate contracts and other arrangements," the business associate structure put in place by the Privacy Rule.

In this final rule, covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see § 164.314(a)(1)).

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Organizational Requirements - § 164.314

1. *Standard: Business associate contracts or other arrangements*. The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.
2. *Implementation specifications (Required)*.
   i. *Business associate contracts*. The contract must provide that the business associate will--
      A. Comply with the applicable requirements of this subpart;
      B. In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
      C. Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.
   ii. *Other arrangements*. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).
   iii. *Business associate contracts with subcontractors*. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

Comment: One commenter suggested that business associate agreements should be an "addressable" requirement under the Security Rule.

Response: The HITECH Act does not remove the requirements for business associate agreements under the HIPAA Rules. Therefore, we decline to make the execution of business associate agreements an "addressable" requirement under the Security Rule.

Comment: One commenter recommended that the Department remove the "addressable" designation from the Security Rule, because such designations lead to ambiguity in the application of the Security Rule in the health care industry.

Response: We decline to adopt this recommendation. The Security Rule is structured to be both scalable and flexible, so that entities of different types and sizes can implement the standards and implementation specifications in a manner that is reasonable and appropriate for their circumstances. We do not mandate the use of specific technologies, or require uniform policies and procedures for compliance, because we recognize the diversity of regulated entities and appreciate the unique characteristics of their environments.

Comment: Two commenters suggested providing subcontractors with additional time to comply with the provisions of the Security Rule.

Response: We decline to delay application of the requirements under the Security Rule to subcontractors beyond the compliance dates provided by this final rule. As we emphasized above, the Security Rule already requires covered entities to establish business associate agreements that require business associates to ensure that their subcontractors implement reasonable and appropriate safeguards to protect the security of electronic protected health information they handle.

Comment: A few commenters proposed alternative ways to apply security requirements to subcontractors, such as exempting subcontractors from compliance with the Security Rule if they have already completed security assessments and met the security requirements under other State and Federal laws or only requiring subcontractors to comply with the minimum necessary standard and to utilize "reasonable" security measures with regard to protected health information.

Response: We decline to adopt an exemption or otherwise limit subcontractors' responsibility to safeguard individuals' electronic protected health information. To ensure appropriate and strong security protections for electronic protected health information, subcontractors are required to comply with the Security Rule to the same extent as business associates with a direct relationship with a covered entity

BA = Business Associate
CE = Covered Entity

The Omnibus Rule expands the definition of a "business associate" to generally include all those entities that create, receive, maintain, or transmit PHI on behalf of a CE.

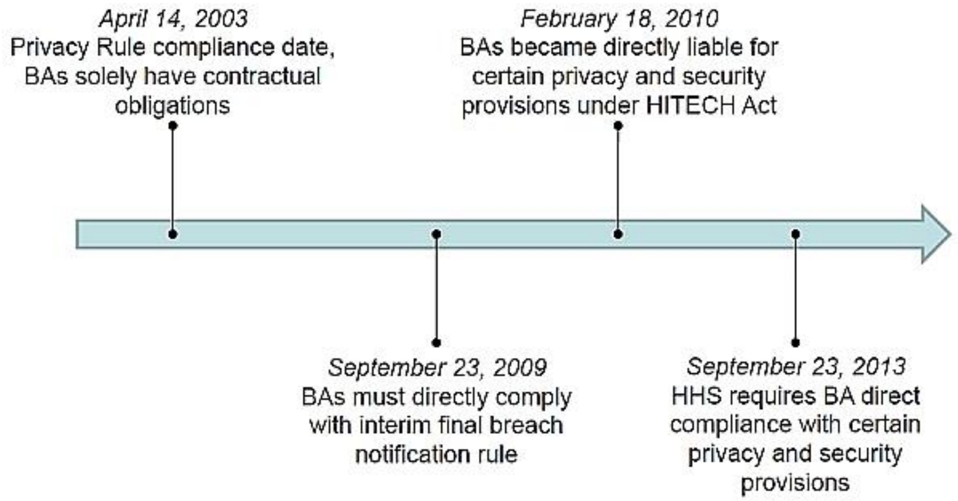
BAs under the Final Rule provide certain identified services *involving PHI* (rather than just IIHI).

The Final Rule also specifically identifies the following types of entities as business associates:

- ❑ Subcontractors.
- ❑ Patient safety organizations.
- ❑ HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
- ❑ E-Prescribing gateways.
- ❑ PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that *do not* offer PHRs on behalf of CEs are *not* BAs.
- ❑ Other firms or persons who "facilitate data transmission" that requires routine access to PHI.

BAs (including their subcontractors) now are subject to civil money penalties and other enforcement actions for noncompliance. Like CEs, BAs may also be liable for violations by their agents.

Timeline of Business Associate Obligations under HIPAA


April 14, 2003
Privacy Rule compliance date, BAs solely have contractual obligations
February 18, 2010
BAs became directly liable for certain privacy and security provisions under HITECH Act
September 23, 2009
BAs must directly comply with interim final breach notification rule
September 23, 2013
HHS requires BA direct compliance with certain privacy and security provisions

Minimum Necessary Standard Now Applies Directly to BAs
The Omnibus Rule applies the "minimum necessary" standard directly to BAs and their subcontractors. When using, disclosing or requesting PHI, all these entities must "make reasonable efforts to limit [the PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

BA Subcontractors

Subcontractors of business associates are now the same category as business associates, in the compliance sense.

Subcontractor + PHI = Business Associate!

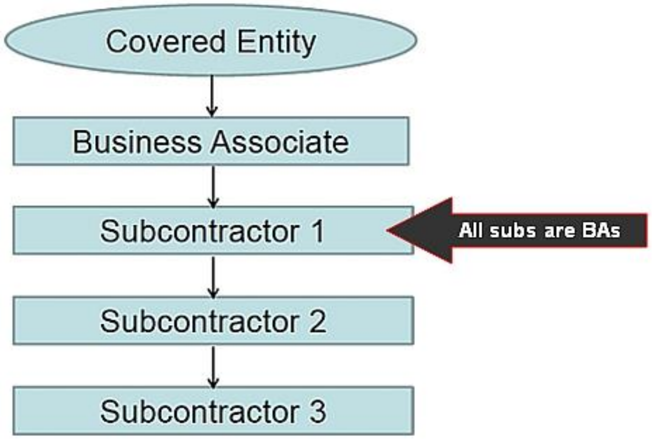
The Omnibus Rule pulls subcontractors into the definition of business associates. Under the Omnibus Rule, a subcontractor is defined as a person or entity to whom a BA delegates a function, activity, or service, and who is *not* a member of the BA's workforce.

This means that a subcontractor of a BA that creates, receives, maintains, or transmits PHI on behalf of the first or primary BA, is now itself a BA and subject to the HIPAA provisions applicable to BAs.

The Omnibus Rule did not change the definition of business associate, but instead simply adds subcontractors to the list of entities that are included as BAs.

Therefore, the business associate who contracts with the covered entity, the business associate's subcontractor, and any subcontractor of a subcontractor—all the way down the chain – are business associates to the extent they create, receive, maintain, or transmit PHI.

The CE-BA Chain



The Omnibus Rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a BA that is a subcontractor—that is the responsibility of the primary or first tier BA.

Q -- When is a Subcontractor *not* a BA?
A -- When a subcontractor is assisting with a BA's *own* management, administration, or legal responsibilities. The BA still must obtain reasonable assurances of confidentiality from the subcontractor, plus assurance of notification from the subcontractor in case of breach, loss, or compromise of data.

Who is *not* a BA?

- ❑ Health Care Providers (for treatment purposes)
- ❑ Health Plan Sponsors (for plan sponsor activities after plan amendments and certifications)
- ❑ Government Agencies (for determining eligibility for or enrollment in a government health plan)
- ❑ Covered Entities that participate in an OHCA (for functions on behalf of the OHCA)
- ❑ External Researchers (for research activities)
- ❑ IRBs (in performing research review, approval, and continuing oversight)
- ❑ Financial institutions (for cashing checks or conducting funds transfer)

Subject to the Section 1179 exemption

- ❑ Onsite Contractors (when treated as workforce)
- ❑ Medical Liability Insurers (when CE purchases a health plan product or other insurance)

The Business Associate Conduit Exception
HHS reiterated that the definition of a BA does not include "conduits" who:

- ❑ Transport PHI; and,
- ❑ Do not access PHI other than on a random or infrequent basis to support transport or as required by law.

<u>The Conduit Exception</u>:

- ❑ Is limited to transmission services (whether digital or hard copy), including temporary storage incident to transmission
- ❑ Does not include an entity that maintains PHI on behalf of a covered entity, e.g., digital or hard copy "document storage companies"

It does not matter whether the entity maintaining the PHI actually views the PHI. And HHS did not address whether entity with only encrypted information (and without key) is a BA.

<u>The Conduit Exception includes</u>:

- ❑ U.S. Postal Service, FedEx, UPS, etc.
- ❑ ISPs who merely provide data transmission services

BA Direct Liability

The Omnibus Rule makes business associates directly liable for compliance with many of the same standards and implementation specifications under the security rule and applies the same penalties to business associates that apply to covered entities.

Under the privacy rule, business associates may use or disclose PHI only in accordance with their business associate contracts or as required by law. Moreover, a business associate may not use or disclose PHI in a manner prohibited by the privacy rule if done by a covered entity (unless HIPAA specifically permits such use and disclosure for business associates). A BA may only use or disclose information in the same manner as the CE. Therefore, any Privacy Rule limitations on how a CE uses or discloses PHI automatically extend to a business associate, and create direct liability for the BA.

The Final Rule adopted the proposal to apply the Minimum Necessary standard directly to BAs when using or disclosing PHI, or when requesting PHI from another CE. It is up to the discretion of the contracting parties to determine to what extent the BA Agreement will include specific Minimum Necessary provisions. HHS intends to issue further guidance on the Minimum Necessary standard with respect to BAs.

<u>Not all of the requirements of the Privacy Rule apply to business associates</u>.
For example, business associates do not need to provide a notice of privacy practices or designate a privacy official (unless the covered entity has chosen to delegate such a responsibility to the business associate, which then would make it a contractual requirement for which contractual liability would attach).

Furthermore, BAs must obtain "satisfactory assurances" in the form of business associate contracts from their subcontractor business associates. Finally, business associates must furnish any information that HHS requires to investigate whether the business associate is in compliance with the regulations.

BAs are Directly Liable under HIPAA for the Following:

1. Impermissible uses and disclosures;
2. Failure to provide breach notification to the CE;
3. Failure to provide access to a copy of electronic PHI to either the CE, the individual, or the individual's designee (whichever is specified in the BAA);
4. Failure to disclose PHI where required by HHS to investigate or determine the business
5. BA's general, overall compliance with HIPAA, as required;
6. Failure to provide an accounting of disclosures; and
7. Failure to comply with the applicable requirements of the Security Rule.

BA Duties under HIPAA Fall into Four General Categories....

1. **Required by HIPAA (penalties for noncompliance)**
    - ❑ Limit uses and disclosures of PHI
        - i. Pursuant to HIPAA
        - ii. Pursuant to BAA
    - ❑ Notify CE or upstream BA of breach of unsecured PHI.
    - ❑ Provide electronic copy of designated record set to CE, upstream BA, or individual (as set forth in BAA) to respond to request for access.
    - ❑ Disclose records (including PHI) to HHS for HHS HIPAA investigation.
    - ❑ Provide an accounting of disclosures.
    - ❑ Comply with the Security Rule
        - i. General requirements
        - ii. Administrative safeguards
        - iii. Physical safeguards
        - iv. Technical safeguards
        - v. Organizational requirements
        - vi. Policies and documentation

2. **Required Only by BA Agreement (Non-compliance = Breach of Contract)**
    - ❑ Safeguards for hard copy and verbal PHI
    - ❑ Report impermissible uses and disclosures that do not qualify as a breach of unsecured PHI
    - ❑ Report security incidents
    - ❑ Provide designated record set maintained in hard copy to respond to request for access
    - ❑ Ensure that appropriate agreement is in place with subcontractors (potentially punishable impermissible disclosure)
    - ❑ Make available PHI for amendments and incorporate amendments
    - ❑ Return or destroy PHI at termination

3. **Potential "Best Practices"**
    - ❑ Designate a privacy official
    - ❑ Policies and procedures governing privacy (use, disclosure, access, amendment, accounting)
    - ❑ Training on privacy
    - ❑ Sanctions policy for privacy noncompliance
    - ❑ Document retention policy for privacy

- ❑ Encrypt all data received, used, stored or transmitted

4. **Not Required Unless Delegated (in writing, in the BAA)**
   - ❑ HIPAA-compliant Notice of Privacy Practices
   - ❑ Complaint process

BA Agreements

The Omnibus Rule includes up to a one-year extension for CEs and BAs to revise their BA Agreements, if such agreements were entered into and compliant with HIPAA as of Jan. 25, 2013 (the date of the Omnibus Rule publication in the Federal Register).

<u>BA Agreements (BAAs) must establish uses and disclosures of PHI</u>:

- ❑ As Required by HIPAA.
- ❑ As Permitted by HIPAA.

New and Renewed BA Agreements - Timing Options

If the parties to a BAA had a HIPAA-compliant Agreement in place before January 25, 2013, and the BAA is *not renewed* between March 26, 2013 and September 2013, then they can continue to lawfully use that BAA until September 23, 2014.

If the parties to a BAA *did not* have a HIPAA-compliant Agreement in place by January 25, 2013, then they must enter into a compliant BAA by September 23, 2013 – one year earlier than for grandfathered BAAs.

No matter what, if a BAA is renewed between September 23, 2013 and September 23, 2014, the new BAA must comply with the HIPAA Final (Omnibus) Rule.

The Omnibus Rule makes BA contracts applicable to arrangements involving a business associate and a subcontractor of that business associate in the same manner that business associate contracts apply to arrangements between a covered entity and its direct business associate. If a subcontractor creates, receives, maintains, or transmits PHI, then a BA must have a BAA with the subcontractor.

HHS emphasizes the continued need for BA contracts even though BAs now are held directly accountable for many provisions of HIPAA. HHS notes that BAA are necessary to clarify and limit permissible uses and disclosures of PHI, ensure business associates are contractually responsible for activities for which they are not directly liable under HIPAA, and clarify respective responsibilities related to patient rights, such as access to PHI.

Each agreement in the BA contract chain must be as or more stringent than the one above it regarding the uses and disclosures of PHI.

"Patterns of Activity" and HIPAA BA Compliance Status
A CE or BA is not in compliance with Business Associate obligations:

- ❑ If it knew of a pattern of activity, or practice of its business associate or subcontractor that constituted a material breach or violation of BA's or subcontractor's obligation(s);
- ❑ Unless it takes reasonable steps to cure the breach or end the violation; and if unsuccessful, terminates the arrangement, if feasible (No requirement to notify HHS).

BAs of Health Plans and Limited Data Sets
If *only* a limited data set is disclosed to a BA of a health plan for health care operations, only a data use agreement is required and a BA Agreement is *not* required.

Policy Number: 3.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Workforce Clearance Policy Procedure

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce clearance, in accordance with the requirements at § 164.308(a)(3).
- ❑ Providing for appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
- ❑ The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members shall have access to all of the individually identifiable health information that they need to do their jobs, but no more access than that.
- ❑ No member of the workforce shall have access to a higher level of individually identifiable health information than the level for which they have been cleared.
- ❑ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall develop specific procedures to ensure that the intent of this policy is executed in fact.
- ❑ Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to individually identifiable health information.
- ❑ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all workforce clearance-related activities and efforts.

Procedures

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Employee user accounts can only be requested by Linear Managers. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. Password issuing will be managed by the IT Service Desk. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to 'Confidential', 'Restricted', 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to 'Public' information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
   1.
      i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
      ii. *Implementation specifications*:
         A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
         B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
         C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
         D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
   2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
   3.
      i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
      ii. *Implementation specifications*:
         A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
         B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Workforce Security (§ 164.308(a)(3))

Comment: The majority of comments concerned the supervision of maintenance personnel by an authorized knowledgeable person. Commenters stated this would not be feasible in smaller settings. For example, the availability of technically knowledgeable persons to ensure this supervision would be an issue. We were asked to either reword this implementation feature or delete it.

Response: We agree that a "knowledgeable" person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, "Authorization and/or supervision," requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis.

Comment: The second largest group of comments requested assurance that, with regard to the proposed "Personnel clearance procedure" implementation feature, having appropriate clearances does not mean performing background checks on everyone. We were asked to delete references to "clearance" and use the term "authorization" in its place.

Response: We agree with the commenters concerning background checks. This feature was not intended to be interpreted as an absolute requirement for background checks. We retain the use of the term "clearance," however, because we believe that it more accurately conveys the screening process intended than does the term "authorization." We have attempted to clarify our intent in the language of § 164.308(a)(3)(ii)(B), which now reads, "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards. To clarify the intent of this provision, we retitle the implementation specification "Workforce clearance procedure."

Comment: One commenter asked that we expand the implementation features to include the identification of the restrictions that should be placed on members of the workforce and others.

Response: We have not adopted this comment in the interest of maintaining flexibility as discussed in § 164.306. Restrictions would be dependent upon job responsibilities, the amount and type of supervision required and other factors. We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule (see, for example, § 164.514(d)(2) (relating to minimum necessary requirements), and § 164.530(c) (relating to safeguards).

Comment: One commenter believes that the proposed "Personnel security" requirement was reasonable, since an administrative determination of trustworthiness is needed before allowing access to sensitive information. Two commenters asked that we delete the requirement entirely. A number of commenters requested that we delete the implementation features. Another commenter stated that all the implementation features may not be applicable or even appropriate to a given entity and should be so qualified.

Response: While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. This final rule has been changed to reflect this approach (see § 164.308(a)(3)(ii)(B)).

Policy Number: 3.2
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA Training Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations concerning the training of workforce members, in accordance with the requirements at § 164.530(b).
- ❑ Clear and complete HIPAA training, in combination with appropriate HIPAA awareness resources, can significantly reduce the likelihood of breaches of confidential health information and the likelihood of HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers, and volunteers.
- ❑ HIPAA training provided by **SoftServe Inc.** shall include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to **SoftServe Inc.'s** operations and to the duties and responsibilities of specific individuals, workgroups, departments, and divisions.

Procedures

- ❑ HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.
- ❑ HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.

- ❑ HIPAA training shall be conducted periodically for all employees, but no less than every six months.
- ❑ Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated HIPAA Privacy Official shall be responsible for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.
- ❑ The designated HIPAA Privacy Official, or other responsible party (if no Privacy Official has been designated), is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.
- ❑ HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.

Scope

This Information Security Training and Awareness Policy applies to all users of all information systems that are the property of **SoftServe** Specifically, it includes:

- ❑ All employees, whether employed on a full-time or part-time basis by **SoftServe**.
- ❑ All contractors and third parties that work on behalf of and are paid directly by **SoftServe**.
- ❑ All contractors and third parties that work on behalf of **SoftServe** but are paid directly by an alternate employer.
- ❑ All employees of partners and clients of **SoftServe** that access **SoftServe**’s non-public information systems.

Roles and Responsibilities

3.1 The **HR Director** is accountable for ensuring that the Confidentiality Agreements are signed by all employees.

3.2 The **ITSD Manager** is accountable for conducting On-boarding meeting and for signing Individual User Agreement by all employees.

3.3 **CISO** must ensure that high priority is given to effective information security training and awareness for their staff. This includes implementation and support of company initiated programs and the development of additional awareness training programs as they deem appropriate.

CISO should:

- ❑ Ensure that a company-wide Information Security Training and Awareness Program is implemented, is well supported by resources and budget, and is effective;
- ❑ Ensure that each Asset Owner has enough sufficiently trained personnel to protect its information resources.

3.4 **IS Manager** is accountable for developing and implementing adequate Information Security Training and Awareness Program in the company. The IS Manager should work to:

- ❑ Establish a company-wide strategy for the Information Security Training and Awareness Program;
- ❑ Ensure that the managers, system and data owners, and others understand the concepts and strategy of the Information Security Training and Awareness Program;
- ❑ Ensure that the company Information Security Training and Awareness Program is funded;
- ❑ Ensure that all users are sufficiently trained in their security responsibilities;
- ❑ Ensure that an effective Information Security Awareness effort is developed and employed such that all personnel are routinely or continuously exposed to Awareness messages through posters, e-mail messages, logon banners, and other techniques;
- ❑ Ensure that Training and Awareness material developed is appropriate for the intended audiences;
- ❑ Ensure that effective tracking and reporting mechanisms are in place;
- ❑ Ensure that Training and Awareness material is reviewed periodically and updated when necessary;

3.5 The **Certification Center Manager** has tactical level responsibility for the Information Security Training and Awareness Program. In this role, the Certification Center Manager should:

- ❑ Ensure that all employees are informed about and invited to Information Security Training and Awareness Program;
- ❑ Ensure that awareness and training material is effectively deployed;
- ❑ Ensure that users and managers have an effective way to provide feedback on the Training and Awareness material;
- ❑ Ensure that Information Security Training and Awareness Program results are moved to employees SSE profiles;

3.6 **Secondary Asset Owners** have responsibility for complying with the Information Security Training and Awareness requirements established for their users. These AO's should:

- ❑ Work with the IS Manager and the VP HR to meet shared responsibilities;
- ❑ Serve in the role of system owner and/or data owner, where applicable;

- ❑ Ensure that all users (including contractors) of their systems are appropriately trained in how to fulfill their responsibilities before allowing them access;
- ❑ Ensure that users (including contractors) understand specific rules of each system and application they use;
- ❑ Work to reduce errors and omissions by users due to lack of Training and/or Awareness.

3.7 **Users / Employees** are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and information system vulnerabilities. Users may include employees, contractors, other company personnel, visitors, guests. Users must:

- ❑ Understand and comply with organization's security policies and procedures;
- ❑ Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
- ❑ Be aware of actions they can take to better protect the company information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.

HHS Regulations
Training - § 164.530(b)

1. *Standard: training*. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.
2. *Implementation specifications: training*.
   - i. A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
     - A. To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
     - B. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
     - C. To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
   - ii. A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

HHS Description
Training

In § 164.518(b) of the NPRM we proposed to require that covered entities provide training on the entities' policies and procedures to all members of the workforce likely to have access to protected health information. Each entity would be required to provide initial training by the date on which this rule became applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time after joining the entity. In addition, we proposed that when a covered entity made material changes in its privacy policies or procedures, it would be required to retrain those members of the workforce whose duties were related to the change within a reasonable time of making the change.

The NPRM would have required that, upon completion of the training, the trainee would be required to sign a statement certifying that he or she received the privacy training and would honor all of the entity's privacy policies and procedures. Entities would determine the most effective means of achieving this training requirement for their workforce. We also proposed that, at least every three years after the initial training, covered entities would be required to have each member of the workforce sign a new statement certifying that he or she would honor all of the entity's privacy policies and procedures. The covered entity would have been required to document its policies and procedures for complying with the training requirements.

The final regulation requires covered entities to train all members of their workforce on the policies and procedures with respect to protected health information required by this rule, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. We do not change the proposed time lines for training existing and new members of the workforce, or for training due to material changes in the covered entity's policies and procedures. We eliminate both the requirement for employees to sign a certification following training and the triennial re-certification requirement. Covered entities are responsible for implementing policies and procedures to meet these requirements and for documenting that training has been provided.

HHS Response to Comments Received
Training

Comment: A few commenters felt that the proposed provision was too stringent, and that the content of the training program should be left to the reasonable discretion of the covered entity.

Response: We clarify that we do not prescribe the content of the required training; the nature of the training program is left to the discretion of the covered entity. The scenarios in the NPRM preamble of potential approaches to training for different sized covered entities were intended as examples of the flexibility and scalability of this requirement.

Comment: Most commenters on this provision asserted that recertification/retraining every three years is excessive, restrictive, and costly. Commenters felt that retraining intervals should be left to the discretion of the covered entity. Some commenters supported retraining only in the event of a material change. Some commenters supported the training requirement as specified in the NPRM.

Response: For the reasons cited by the commenters, we eliminate the triennial recertification requirements in the final rule. We also clarify that retraining is not required every three years. Retraining is only required in the case of material changes to the privacy policies and procedures of the covered entity.

Comment: Several commenters objected to the burden imposed by required signatures from employees after they are trained. Many commenters suggested that electronic signatures be accepted for various reasons. Some felt that it would be less costly than manually producing, processing, and retaining the hard copies of the forms. Some suggested sending out the notice to the personal workstation via email or some other electronic format and having staff reply via email. One commenter suggested that the covered entity might opt to give web based training instead of classroom or some other type. The commenter indicated that with web based training, the covered entity could record whether or not an employee had received his or her training through the use of a guest book or registration form on the web site. Thus, a physical signature should not be required.

Response: We agree that there are many appropriate mechanisms by which covered entities can implement their training programs, and therefore remove this requirement for signature. We establish only a general requirement that covered entities document compliance with the training requirement.

Comment: Some commenters were concerned that there was no proposed requirement for business associates to receive training and/or to train their employees. The commenters believed that if the business associate violated any privacy requirements, the covered entity would be held accountable. These commenters urged the Secretary to require periodic training for appropriate management personnel assigned outside of the component unit of the covered entity, including business associates. Other commenters felt that it would not be fair to require covered entities to impose training requirements on business associates.

Response: We do not have the statutory authority directly to require business associates to train their employees. We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§ 164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

Comments: Many commenters argued that training, as well as all of the other administrative requirements, are too costly for covered entities and that small practices would not be able to bear the added costs. Commenters also suggested that HHS should provide training materials at little, or no, cost to the covered entity.

Response: For the final regulation, we make several changes to the proposed provisions. We believe that these changes address the issue of administrative cost and burden to the greatest extent possible, consistent with protecting the privacy of health information. In enforcing the privacy rule, we expect to provide general training materials. We also hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups.

We note that, under long-standing legal principles, entities are generally responsible for the actions of their workforce. The requirement to train workforce members to implement the covered entity's privacy policies and procedures, and do such things as pass evidence of potential problems to those responsible, is in line with these principles. For example, the comments and our fact finding indicate that, today, many hospitals require their workforce members to sign a confidentiality agreement, and include confidentiality matters in their employee handbooks.

Policy Number: 3.3
Effective Date: 3/26/2013
Last Revised: 7/28/2014

PHI Uses and Disclosures Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.
- ❑ **SoftServe Inc.** must implement policies and procedures to ensure that all uses and disclosures of PHI are made or denied in accordance with HIPAA law and regulations.
- ❑ For especially sensitive information, such as AIDS/HIV, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be *informed.* That is, made with the patient's or consumer's knowledge of the risks and benefits of the disclosure.
- ❑ Any disclosure of confidential patient information carries with it the potential for an unauthorized re-disclosure that breaches confidentiality.
- ❑ **SoftServe Inc.** incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under HIPAA Regulations and under State law to charge a reasonable fee to offset those costs.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to conduct its operations in full compliance with HIPAA's Rules governing uses and disclosures of Protected Health Information.
- ❑ **SoftServe Inc.** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.

Procedures

- ❑ The following priorities and time frames shall apply to requests for disclosures of PHI:
    - *Emergency requests involving immediate emergency care of patient:* immediate processing.
    - *Priority requests pertaining to current care of patient:* within one workday.
    - *Patient request for access to own record:* within three (3) workdays.
    - *Subpoenas and depositions:* as required.
    - *All other requests:* within five (5) workdays
- ❑ Courtesy Notifications to Practitioners – As a courtesy, records processing personnel shall notify the appropriate healthcare practitioner when any of the following occur:
    - Patient or his or her representative requests information from the medical record.
    - Patient or representative requests direct access to the complete medical record.
    - Patient or representative institutes legal action.
- ❑ Disclosure Monitoring and Logging -- Medical records personnel will maintain a log to track the step-by-step process towards completion of each request for the release of PHI. Health Information Management personnel and/or the designated Privacy Official, or other responsible party (if no Privacy Official has been designated), will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
    - Date department received the request.
    - Name of patient.
    - Name and status (patient, parent, guardian) of person making request.
    - Information released.
    - Date released.
    - Fee charged.
- ❑ Fee Schedule – **SoftServe Inc.** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.
- ❑ **SoftServe Inc.** will charge a reasonable fee to offset the costs associated with specific categories of requests. The designated HIPAA Privacy Official, or other responsible party (if no Privacy Official has been designated), shall develop and implement a Fee Schedule related to disclosures of PHI. Fees shall be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and shall include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.

- ❑ Unless the request specifies release of the complete medical record, **SoftServe Inc.** shall release only selected portions of the record. **SoftServe Inc.** shall prepare an appropriate cover letter detailing the items included.
- ❑ Prohibition of Re-disclosure -- Unless a law or regulation requires a more specific prohibition on re-disclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the facility shall contain the following notice:
  - *The attached medical information pertaining to [Name of patient] is confidential and legally privileged. **SoftServe Inc.** has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*
- ❑ Retention of Disclosure Requests -- The designated Privacy Officer, or other responsible party (if no Privacy Official has been designated), will retain the original request, the authorization for release of information, and a copy of the cover letter in the patient(s) medical record for the appropriate record retention period.
- ❑ Use of Copying Services -- To facilitate the timely processing of release of information requests,__**SoftServe Inc.** may use the services of a commercial copying service on terms that protect the integrity and confidentiality of patient information.
- ❑ Disclosure Quality Control -- The director of the Health Information Management Department and/or the designated Privacy Official, or other responsible party (if no Privacy Official has been designated), shall conduct a routine audit of the release of information at least quarterly, paying particular attention to the following:
  - Validity of authorizations.
  - Appropriateness of information abstracted in response to the request.
  - Retention of authorization, request, and transmitting cover letter.
  - Procedures for telephone, electronic, and in-person requests.
  - Compliance with designated priorities and time frames.
  - Proper processing of fees.
  - Maintenance of confidentiality.
- ❑ In-service Training on Disclosures -- The Director of Health Information Management and/or Privacy Official, or other responsible party (if no Privacy Official has been designated), shall give periodic in-service training to all employees involved in the release of information.
- ❑ Semi-Annual Policy Review - The Director of Health Information Management and/or Privacy Official, or other responsible party (if no Privacy Official has been designated), shall review this policy and associated procedures with risk management and legal counsel at least semiannually.
- ❑ Capacity to Authorize -- **SoftServe Inc.** requires a written, signed, current, valid authorization to release medical information as follows:

Patient Category	**Required Signature**
Adult Patient	The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.

Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult patients above.
Psychiatric, drug, alcohol program patients/clients	Same as adult patients above, but check for special requirements.
AIDS/HIV or other sexually transmitted disease patients	Same as adult patients above, but check for special requirements.

- □ Authorization Forms -- The Director of Health Information Management and/or the designated Privacy Official, or other responsible party (if no Privacy Official has been designated), shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
- □ Revocation of Authorization -- A patient may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
- □ Refusal to Honor Authorization -- Health Information Management Department personnel and/or the designated Privacy Official, or others authorized to release information, will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
  - Identity of the person presenting the authorization.
  - Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
  - Legal age or status as an emancipated minor.
  - Patient capacity to understand the meaning of the authorization.
  - Authenticity of the patient(s) signature.
  - Current validity of the authorization.
  - In such situations, the employee shall refer the matter to the Director of Health Information Management and/or Privacy Officer for review and decision.
- □ Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.

Person and Identity Verification Table

Person to Identify	**In-Person Encounter**	**Telephone Encounter**	**Request in Writing** (Fax, mail, hand-delivered)
Attorney	▪ Presents with business card and photo identification (i.e. driver's license or organization ID badge) and:	▪ It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required	▪ Supplies business card, photo identification (i.e. driver's license or org ID badge), and letterhead. Confirmation call is required.
Facility Directory:	▪ Verify identity	▪ Verify identity	▪ Verify identity
Patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number. Verify patient's signature with that on file or on driver's license.
Personal Representative (Legal Guardian) for the Patient	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with Personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number. Verify the Personal Rep's signature with signature on file or on driver's license.
Persons Involved in the Patient's Immediate Care *(PHI relevant only to the*	▪ Patient actively involves this person in his/her care; or ▪ In your best	▪ Patient actively involves this person in his/her care; or ▪ In your best	▪ N/A

Person to Identify	**In-Person Encounter**	**Telephone Encounter**	**Request in Writing** (Fax, mail, hand-delivered)
patient's current care (164.510(b)). ▪ Blood Relative ▪ Spouse ▪ Domestic Partner ▪ Roommate ▪ Boy/Girl Friend ▪ Neighbor ▪ Colleague	professional judgment, the disclosure is in the patient's best interest.	professional judgment, the disclosure is in the patient's best interest. ▪ Use call-back.	
Power of Attorney For the Patient	▪ Presents with a photo ID and a copy of the POA. Verify patient's signature with one on file. ▪ Acquainted with power of attorney as being such	▪ Previously obtained a copy of the POA and verified the patient's signature with one on file. ▪ Acquainted with power of attorney as being such	▪ Obtain a copy of the POA and verify the patient's signature with one on file
Provider From Another Facility	▪ Acquainted with provider as a treatment provider; ▪ Provider is wearing a photo badge from his/her facility; or, ▪ Patient/personal representative introduces provider to you.	▪ Acquainted with provider as a treatment provider; or; ▪ Call requestor back through main switchboard number (not via a direct number).	▪ Recognize name of facility and address on letterhead as a treatment facility; or ▪ Call requestor back through main switchboard number (not via a direct number).
Public Official ▪ CIA ▪ Court Order ▪ FBI ▪ Law Enforcement Officer ▪ OCR ▪ OIG	▪ Presents an agency I.D. badge; ▪ Presents with a written statement of legal authority; ▪ Presents with a written statement of appointment on approp. govt. letterhead; ▪ Presents with warrant,	▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Written statement of legal authority; ▪ Written statement of appointment on appropriate government; ▪ Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or ▪ Contract for services or purchase order

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
▪ Public Health Agency Official ▪ Other	court order, or legal process issued by a grand jury, or a judicial or admin. tribunal; ▪ Presents with a contract for services or purchase order; or, ▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.		
Vendor Who Helps Assists w Treatment, Payment, or Health Care Operations Examples Include, But Are Not Limited to the Following: ▪ Accreditation Org. ▪ DME Company ▪ Insurance Co. ▪ Pharmacy Vendor We Have Rebate Agreement. with ▪ Software Vendor ▪ Statement Vendor	▪ Recognize requestor/ organization; or ▪ Photo identification with organization	▪ Recognize requestor or organization	▪ Recognize requestor/ organization; or ▪ Call requestor back through main switchboard number (not via a direct number).
1. **Workforce Member of Our Organization**	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is wearing an I.D. badge.	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is calling from an in-house extension.	▪ Request is sent from/through our own computer system; or ▪ Request is on our own letterhead.

PHI Disclosures Table

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Accrediting Agencies (JCAHO, CARF)	No	No	No
Attorney for Resident	Yes	Yes	No
Attorney for Facility/Corporation	No	No	No
Contractors/ Business Associates	No, unless their purpose falls outside of TPO.	No	No
For Deceased Persons ❑ Coroner or Medical Examiner, Funeral Directors ❑ Organ Procurement	No	No	Yes
Employer ❑ PHI specific to work related illness or injury, and ❑ Required for employer's compliance with occupational safety and health laws	No, for the purpose listed. Yes for all others.	No	No
Family Members	No for oral disclosures to family members involved in care; Yes for others.	Yes	No

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Entity Subject to the Food and Drug Administration □ Adverse events, product defects or biological product deviations □ Track products □ Enable product recalls, repairs, or replacements □ Conduct post marketing surveillance	No	No	Yes
Health Oversight □ Government benefits program □ Fraud and abuse compliance □ Civil rights laws □ Trauma/tumor registries □ Vital statistics □ Reporting of abuse or neglect	No	No	Yes
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No
Health Care Practitioners and Providers if not Involved in Care or Treatment (i.e., consultants)	No	No	No
Insurance Companies/Third Party Payers □ Related to Claims Processing	No	No	No
Judicial and Administrative Proceedings □ Court order, or warrant □ Subpoena	No No - See Subpoena Policy	No Yes	Yes Yes

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Law Enforcement ❑ Administrative request ❑ Locating a suspect, fugitive, material witness or missing person ❑ Victims of crime ❑ Crimes on premises ❑ Suspicious deaths ❑ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.
Public Health Authorities ❑ Surveillance ❑ Investigations ❑ Interventions ❑ Foreign governments collaborating with US public health authorities ❑ Recording births/deaths ❑ Child/elder abuse ❑ Prevent serious harm ❑ Communicable disease	No	No	Yes
Research (w/o Authorization)	No, if IRB or Privacy Board approves research study and waives authorization.	No	Yes
Resident/Resident's Personal Representative	No	Yes	No
Specialized Government Functions ❑ Military and Veterans' activities ❑ Protective services for the President ❑ Foreign military personnel ❑ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.
Workers' Compensation	No	See	Yes

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
❑ Comply w/existing laws (see state law)		applicable State Law	

HHS Regulations as Amended January 2013
General Rules for Uses and Disclosures of Protected Health Information: Use and Disclosure for Treatment, Payment and Health Care Operations - § 164.502(a)

Standard. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

1. *Covered entities: Permitted uses and disclosures*. A covered entity is permitted to use or disclose protected health information as follows:
   i. To the individual;
   ii. For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
   iii. Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
   iv. Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;
   v. Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
   vi. As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).
2. *Covered entities: Required disclosures*. A covered entity is required to disclose protected health information:
   i. To an individual, when requested under, and required by § 164.524 or § 164.528; and
   ii. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.
3. *Business associates: Permitted uses and disclosures*. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.
4. *Business associates: Required uses and disclosures*. A business associate is required to disclose protected health information:

- i. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.
- ii. To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

5. *Prohibited uses and disclosures*.
   - i. *Use and disclosure of genetic information for underwriting purposes*:

     Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

     - A. Except as provided in paragraph (a)(5)(i)(B) of this section:
       1. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
       2. The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
       3. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
       4. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
     - B. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.
   - ii. *Sale of protected health information*:
     - A. Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.
     - B. For purposes of this paragraph, sale of protected health information means:
       1. Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.
       2. Sale of protected health information does not include a disclosure of protected health information:

- iii. For public health purposes pursuant to § 164.512(b) or § 164.514(e)
- iv. For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;
- v. For treatment and payment purposes pursuant to § 164.506(a);

vi. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

vii. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

viii. To an individual, when requested under § 164.524 or § 164.528;

ix. Required by law as permitted under § 164.512(a); and

x. For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

HHS Regulations as Amended January 2013
General Rules for Uses and Disclosures of Protected Health Information: Minimum Necessary - § 164.502(b)

Standard: minimum necessary

1. *Minimum necessary applies*. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
2. *Minimum necessary does not apply*. This requirement does not apply to:
    i. Disclosures to or requests by a health care provider for treatment;
    ii. Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
    iii. Uses or disclosures made pursuant to an authorization under § 164.508;
    iv. Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
    v. Uses or disclosures that are required by law, as described by § 164.512(a); and
    vi. Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

HHS Regulations
Uses and Disclosures of Protected Health Information Subject to an Agreed Upon Restriction - § 164.502(c)

Standard: uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

HHS Regulations
Creation of De-identified Information - § 164.502(d)

Standard: uses and disclosures of de-identified protected health information.

1. *Uses and disclosures to create de-identified information*. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.
2. *Uses and disclosures of de-identified information*. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:
   i. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and
   ii. If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

HHS Regulations as Amended January 2013
General Rules for Uses and Disclosures of Protected Health Information: Disclosures to Business Associates - § 164.502(e)

1. *Standard: disclosures to business associates*.
   i. A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
   ii. A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.
2. *Implementation specification: documentation*. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

HHS Regulations as Amended January 2013
General Rules for Uses and Disclosures of Protected Health Information: Deceased Individuals - § 164.502(f)

Standard: deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

HHS Regulations as Amended August 2002
Personal Representatives - § 164.502(g)

1. *Standard: personal representatives*. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.
2. *Implementation specification: adults and emancipated minors*. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
3. *Implementation specification: unemancipated minors*.
    - i. If under applicable law a parent, guardian, or other person acting in *loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:
        - A. The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
        - B. The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or
        - C. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.
    - ii. Notwithstanding the provisions of paragraph (g)(3)(i) of this section:
        - A. If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.
        - B. If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.

        C. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraph (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

4. *Implementation specification: deceased individuals*. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
5. *Implementation specification: abuse, neglect, endangerment situations*. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:
    i. The covered entity has a reasonable belief that:
        A. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
        B. Treating such person as the personal representative could endanger the individual; and
    ii. The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

HHS Regulations
Confidential Communications - § 164.502(h)

Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

HHS Regulations
Uses and Disclosures Consistent With Notice - § 164.502(i)

Standard: uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

HHS Regulations
Disclosures by Whistleblowers and Workforce Member Crime Victims - § 164.502(j)

Standard: disclosures by whistleblowers and workforce member crime victims.

1. *Disclosures by whistleblowers*. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:
    i. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
    ii. The disclosure is to:
        A. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
        B. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.
2. *Disclosures by workforce members who are victims of a crime*. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
    i. The protected health information disclosed is about the suspected perpetrator of the criminal act; and
    ii. The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

Policy Number: 3.4
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA/State Law Preemption Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
- ❑ HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better patient and consumer access to health data than HIPAA, will generally preempt HIPAA regulations.
- ❑ HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, State Laws, or both) must be followed.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to comply, whenever possible, with both state law in the state(s) where we operate, as well as HIPAA law and regulations.

Procedures

- ❑ **SoftServe Inc.'s** designated Privacy Official, or other responsible party (if no Privacy Official has been designated) shall analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
- ❑ **SoftServe Inc.'s** designated Privacy Official, or other responsible party (if no Privacy Official has been designated), shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
- ❑ If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the **SoftServe Inc.'s** designated Privacy Official, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to **SoftServe Inc.** operations.
- ❑ **SoftServe Inc.'s** designated Privacy Official, or other responsible party (if no Privacy Official has been designated), shall conduct ongoing research to monitor legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.

HHS Regulations as Amended January 2013
Preemption of State Law: Definitions - Contrary - § 160.202

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

1. A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or
2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

HHS Regulations as Amended August 2002
Preemption of State Law - General Rule and Exception - § 160.203

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

a. A determination is made by the Secretary under § 160.204 that the provision of State law:
    1. Is necessary:
        i. To prevent fraud and abuse related to the provision of or payment for health care;
        ii. To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
        iii. For State reporting on health care delivery or costs; or
        iv. For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
    2. Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

b. The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

c. The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

d. The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

HHS Regulations
Preemption of State Law: Process for Requesting Exception Determinations - § 160.204

a. A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:
    1. The State law for which the exception is requested;
    2. The particular standard, requirement, or implementation specification for which the exception is requested;
    3. The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
    4. How health care providers, health plans, and other entities would be affected by the exception;
    5. The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
    6. Any other information the Secretary may request in order to make the determination.
b. Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
c. The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

HHS Regulations
Preemption of State Law: Duration of Effectiveness of Exception Determinations - § 160.205

An exception granted under this subpart remains in effect until:

a. Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
b. The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

HHS Regulations as Amended January 2013
Preemption of State Law: Definitions - Contrary - § 160.202

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

1. A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

HHS Regulations as Amended January 2013
Preemption of State Law: Definitions - More Stringent - § 160.202

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

1. With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
   i. Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or
   ii. To the individual who is the subject of the individually identifiable health information.
2. With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment as applicable.
3. With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
4. With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
5. With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

HHS Regulations
Preemption of State Law: Definitions - Relates to the Privacy of Individually Identifiable Health Information - § 160.202

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

HHS Regulations
Preemption of State Law: Definitions - State Law - § 160.202

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

SECTION 4

Policy Number: 4.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Assignment of Security Responsibility Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
- ❑ The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- ❑ The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the (Insert Name) designated HIPAA Official or Officer, or other responsible party (if no Privacy Official has been designated), who shall report directly to__ Name of Direct Report __.

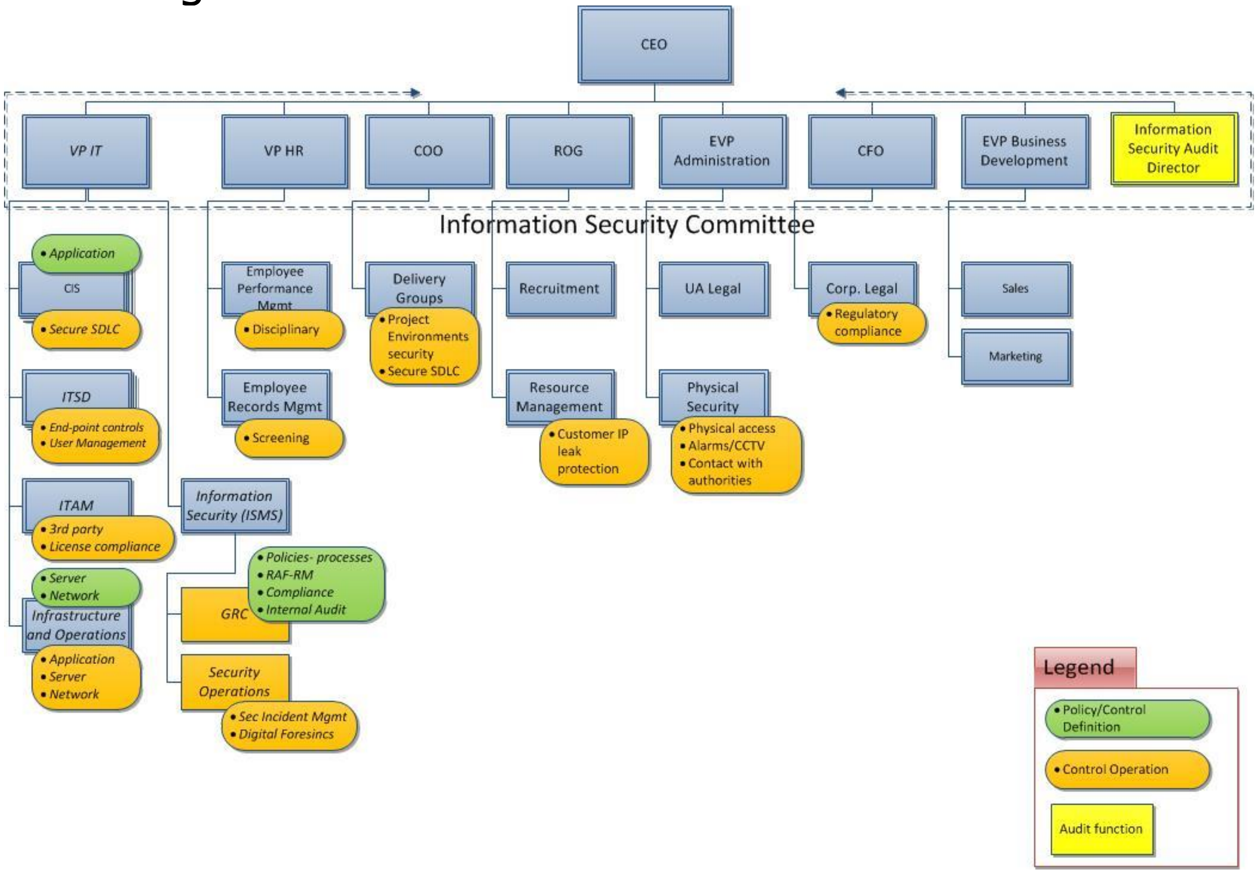
Procedures

The (Insert Name) designated HIPAA Official or Officer or other responsible party (if no Privacy Official has been designated), shall implement the following procedures, as appropriate, in accordance with the Risk Management policies of **SoftServe Inc.**:

- ❑ Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- ❑ Maintain an accurate inventory of (1) all individuals who have access to the Practice's confidential information, including PHI, and (2) all uses and disclosures of the Practice's confidential information by any person or entity.
- ❑ Administer patient requests and processes under HIPAA's patient rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect the Practice's confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by the Privacy Rule.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the privacy notice required by the Privacy Rule.
- ❑ Determine when the Practice might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
- ❑ Ensure that any research efforts conducted or supported by the Practice comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that the Practice's confidential data is adequately protected when such access is granted.
- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future Practice initiatives are structured in such a way to ensure patient privacy.
- ❑ Conduct periodic privacy audits and take remedial action as necessary.
- ❑ Oversee employee training in the area of privacy.
- ❑ Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.

- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice’s policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- ❑ Anticipate members’ concerns and questions about the Practice’s use of their confidential information and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of any future on-line, web-based application procedure.
- ❑ Monitor any data collected by or posted on the Practice’s Web sites for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the Practice’s privacy practices.
- ❑ It is the Policy of **SoftServe Inc.** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements.

ISMS Organizational Structure



Management commitment to information security

The **Board of Directors ("the Board" or "BoD")** is ultimately accountable for information security in corporation. **CEO** is appointed by **BoD** as responsibilities for management and control of information security risks accordingly to CEO Operations Agreement.

The **Executive Management** give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the **Information Security Committee (ISC)**chaired by the **CEO**.

The Executive Management depend heavily on the ISC to coordinate activities throughout Organization, ensuring that suitable policies are in place to support organization security principles and axioms. The Executive Management also rely on feedback from the ISC, CISO, IS Manager, Auditors, Risk Management, Compliance, Legal and other functions to ensure that the principles, axioms and policies are being complied-with in practice.

The Executive Management demonstrate their commitment to information security by:

- ❑ A statement of support from the CEO;
- ❑ Reviewing and re-approving the principles and axioms on regular basis;
- ❑ Approving budgets for controls implementation, operation and related activities in accordance to defined principles and policies;
- ❑ Receiving and acting appropriately on management reports concerning information security performance metrics, information security incidents, investment requests *etc*.

Information security co-ordination

Information security activities should be coordinated throughout **SoftServe** organization to ensure consistent application of the security principles, axioms and policy statements.

The Executive Management have charged the ISC with the task of securing organization's assets. The ISC responsibilities described in ISMS DOC 6.1 Information Security Committee.

Other Responsibilities here

Allocation of information security responsibilities

The Executive Management have appointed **VP IT to act as Chief Information Security Officer** for period of ISMS PLAN phase and until further decisions are made.

Information Security Manager

The IS Manager is responsible for:

- ❑ Policy and Compliance;
- ❑ Defining technical and non-technical information security standards, procedures and guidelines;
- ❑ Supporting IAOs and managers in the definition and implementation of controls, processes and supporting tools to comply with the policy manual and manage information security risks (ISMS DOC 4.1 Risk Management Framework);
- ❑ Identification of gaps between existing controls and customer requirements, providing recommendations to IAOs responsible for meeting particular customer requirements;
- ❑ Monitor and maintain the ISMS, manage operation and resources of ISMS;
- ❑ Defining internal audit principles and process, in particular ISMS audit (ISMS DOC 18.8 Internal Independent Review);
- ❑ Organizing Internal Audit team, developing annual internal audit program schedule (Section 1 Internal Audit);
- ❑ Risk and Contingency Management (ISMS DOC 4.1 Risk Management Framework);
- ❑ Defining Risk Assessment Framework (ISMS DOC 4.1 Risk Management Framework);
- ❑ Coordinating information security risk assessment and analysis (ISMS DOC 4.1 Risk Management Framework);
- ❑ Preparing Risk Assessment Report, Risk Treatment Plan (ISMS DOC 4.3 Risk Treatment Plan) and Risk Treatment Action Plan (ISMS DOC 4.4 Risk Treatment Action Plan);
- ❑ Developing, testing and maintaining measurements, collecting and reporting the measurements data that enable the organization to measure controls effectiveness to produce comparable and reproducible results (ISMS DOC 3.1 Effectiveness Measurement);

- □ Carrying out risk assessments wherever they are required by the ISMS (ISMS DOC 4.1 Risk Management Framework and ISMS DOC 15.1 Supplier Relationship Policy);
- □ Preparing and maintaining Statement of Applicability (SoA) (ISMS DOC 4.6 Statement of Applicability ISO 27001:2013);
- □ Organizing BCP testing (ISMS DOC 17.4 Business Continuity Testing Standard);
- □ Development, review and evaluation of threats and vulnerabilities lists (ISMS DOC 4.7 List of Threats and Vulnerabilities);
- □ Security Administration and approval (ISMS DOC 5.2 Management Review of Information Security);
- □ Security Operations (ISMS DOC 15.1 Supplier Relationship Policy, ISMS DOC 8.4 E-Mail Standard, ISMS DOC 6.3 Teleworker Security Policy, ISMS DOC 13.1 Network Control Policy, ISMS DOC 9.6 Secure Logon Standard, ISMS DOC 8.7 Removable Media Policy, ISMS DOC 8.12 Removal of Assets Standard, ISMS DOC 8.5 Office Equipment Usage Standard etc.);
- □ Reviewing and monitoring compliance with the policy statements and contributing to Internal Audit and Control Self-Assessment (CSA) processes;
- □ Collecting, analyzing and commenting on information security metrics and incidents (ISMS DOC 3.1 Effectiveness Measurement);
- □ Supporting IAOs in the investigation and remediation of information security incidents or other policy violations;
- □ Establishing reasonable security guidelines and measures to protect data and systems based on risk assessment outcomes via Risk Treatment Plan;
- □ Liaising as necessary with related internal functions such as IT Operations, Risk Management, Compliance and Internal Audit, as well as the CISO, ISC and external functions such as the Police when appropriate;
- □ Designing, organizing information security awareness, training and education program (IST&A Program) for personnel to enhance the security culture and develop a broad understanding of the requirements of ISO/IEC 27002 (ISMS DOC 7.5 Information Security Training and Awareness Policy);
- □ Developing IST&A strategy, training materials and tests (ISMS DOC 7.6 Information Security Training and Awareness Guidelines).
- □ Evaluates and approves security of new information processing facilities;
- □ Ensuring that all contacts with authorities are maintained by the relationship Owners (ISMS DOC 6.6 Contact with Authorities);
- □ Maintaining the schedule of required keys in line with the risk assessment, Cryptographic Key Management and evolving security environment;
- □ Ensuring that all information security issues have been included and appropriately treated in business continuity plans;
- □ Managing information security responses and collection and retention of information in respect of information security incidents(ISMS DOC 16.2 Security Incident Reporting Procedure and ISMS DOC 16.1 Handling of InfoSec Incidents Standard and ISMS DOC 16.3 Collection of Evidence Standard);
- □ Ensuring that agendas, documents and minutes are produced and distributed for Information Security Committee meeting (ISMS DOC 6.1 Information Security Committee);

- ❑ Approving Internal Audit team, annual internal audit program schedule (Section 1 Internal Audit).
- ❑ Providing internal audit report to CEO on a regular basis.

Information Security Audit Director

Information Security Audit Director is responsible for:

- ❑ Reviewing internal audit reports.
- ❑ Act as expert for facilitating BoD review and approval of corporate strategic initiatives, treatment plans and audit reports in the area of the information security.
- ❑ Act as expert for facilitating CEO review and approval of technical and methodological practices in physical and personnel security (also referred as economical/commercial security).
- ❑ Monitoring process of handling security incidents with "High" impact level of according to ISMS DOC 16.1 Handling of InfoSec Incidents Standard
- ❑ Overseeing of security controls of BoD workplaces and resources (services, servers).
- ❑ Provide password/authentication token escrow for privileged accounts to Secondary Assets - IT services containing information classified as "secret" and "top secret" according to ISMS DOC 8.8 InfoSec Classification Standard.

Primary Asset Owners

Information (Primary) Asset Owners (IAOs) are **Executive Managers** held accountable for the protection of Information Assets by the ISC. IAOs may delegate information security tasks to their subordinate managers or other individuals but remain accountable for proper implementation of the tasks.

Information Asset Owners are responsible for:

- ❑ Appropriate classification and protection of the information assets;
- ❑ Authorizing access to information assets in accordance with the classification and business needs (ISMS DOC 8.8 InfoSec Classification Standard, ISMS DOC 9.3 Information Systems Administrative Access Standard);
- ❑ Ensuring that their asset is only accessible to **SoftServe** employees or to individuals who have current, signed confidentiality agreements (ISMS DOC 13.2 Confidentiality Agreements Standard);

- □ Carrying our regular review of the related threats and vulnerabilities and update them if necessary (ISMS DOC 4.7 List of Threats and Vulnerabilities). The list of related threats and vulnerabilities must be reviewed at least once per year;
- □ Provide business approvals for establishing new information processing facilities;
- □ Undertaking or commissioning information security risk assessments (for new application system developments) to ensure that the information security requirements are properly defined and documented during the early stages of development;
- □ Ensuring timely completion of regular system/data access reviews;
- □ Monitoring compliance with protection requirements affecting their assets;
- □ Identifying the records that will be generated by the processes or assets for which they are responsible, or which should be generated to indicate conformity with the ISMS, and for ensuring that they are controlled in line with Document Control procedure (ISMS DOC 2.1 Document Control);
- □ Providing IST&A Program company-wide support.

Secondary Asset Owners

Secondary Asset Owners (SAOs) are Department Managers held accountable for ensuring security of Secondary Assets by the ISC. SAOs may delegate information security tasks to their subordinate managers or other individuals but remain accountable for proper implementation of the tasks.

Secondary Asset Owners are responsible for:

- □ Identifying threats, vulnerabilities of their Secondary Assets, suggest controls and implement them.
- □ Classifying their Secondary Assets according to classification of Primary Assets contained, processed or transferred within owned Secondary Assets (see ISMS DOC 8.8 InfoSec Classification Standard).
- □ Changes to their assets. Thus, they usually have to approve and sign off on changes to their assets (e.g., system enhancement, major changes to the software and hardware).
- □ Ensuring that proper controls are in place to address integrity, confidentiality, and availability of information within secondary assets they own.
- □ Measuring the effectiveness of implemented controls and preparing evidences for internal audit.
- □ Processing of non-conformances regarding their Secondary Assets.

VP IT

Vice President IT (VP IT) is responsible for:

- ❑ Design, implementation and maintenance of technical (IT security) controls within organization information systems and networks;
- ❑ Design, implementation and maintenance of controls related to design, development customization of information systems.

Managers

Managers throughout **SoftServe** organization are responsible for:

- ❑ Day-to-day implementation of the information security policy manual;
- ❑ Ensuring that suitable technical, physical and procedural controls are in place in accordance with the manual, and are properly applied and used by all employees. In particular, they should take measures to ensure that employees:
  - are informed of their obligations to fulfill relevant corporate policy statements by means of appropriate awareness, training and education activities;
  - comply with the policy statements and actively support the associated controls; and
  - Are monitored to assess their compliance with the policy statements and the correct operation of the associated controls, and reminded of their obligations as appropriate.
- ❑ Providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within their area of responsibility;
- ❑ Informing IS Manager and/or IAOs of actual or suspected policy violations (information security incidents) affecting their assets; and
- ❑ Evaluating compliance with the policy axioms through the regular CSA process and occasional Internal Audits;
- ❑ Proactive notification of Human Resources and the IT Help Desk of any change in employment status that impacts access requirements;
- ❑ Providing IST&A Program coverage within their departments;
- ❑ Organizing process of managing personnel having appropriate level of security clearance according to Background Check Procedure and corresponding Security Training;

Project Managers

Project Managers are responsible for:

- ❑ Implementing and managing of information security controls within project environment;
- ❑ Identifying, implementing and managing custom security controls required by contractual or legal obligations specific to the project;
- ❑ Ensuring that suitable technical, physical and procedural controls are in place in accordance with the manual, and are properly applied and used by all employees. In particular, they should take measures to ensure that employees:
    - are informed of their obligations to fulfill relevant corporate policy statements by means of appropriate awareness, training and education activities;
    - comply with the policy statements and actively support the associated controls; and
    - Are monitored to assess their compliance with the policy statements and the correct operation of the associated controls, and reminded of their obligations as appropriate.
- ❑ Providing IST&A Program coverage within their projects.

HR Department

Certification Center Manager is responsible for:

- ❑ Organizing the process of involvement of all employees in IST&A Program;
- ❑ Transferring IST&A Program Tests results in employees profiles at SSE.

HR Department Manager is responsible for:

- ❑ Integration of results of IST&A Program Tests to Performance Appraisal Process;
- ❑ Providing reports concerning IST&A Program coverage company-wide.

Employees

All **SoftServe** employees (*i.e.* employees on the payroll and others acting in a similar capacity, such as contractors, consultants, student placements *etc.*) are responsible for complying with the principles, axioms and policies in the information security policy manual where relevant to their jobs. They are responsible for maintaining the security of all information entrusted to them. **SoftServe** employees obliged to report security incidents, weaknesses and concerns immediately to Information Security Manager.

Upon hire, as a condition of employment, each employee undertakes to comply with **SoftServe**'s information security policies.

All **SoftServe** employees are obliged to understand, follow IST&A Program and pass successfully IST&A Program Tests.

Any worker failing to comply with the security policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.

Other Responsibilities here

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
   1.
      i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
      ii. *Implementation specifications*:
         A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
         B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
         C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
         D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

   2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

Assigned Security Responsibility (§ 164.308(a)(2))

We proposed that the responsibility for security be assigned to a specific individual or organization to provide an organizational focus and importance to security, and that the assignment be documented. Responsibilities would include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.

In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy

Policy Number: 4.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Policy on Evaluating the Effectiveness of Security Policies and Procedures

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
- ❑ Security policies and procedures, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to periodically evaluate security policies and procedures, including emergency and contingency plans and procedures, in order to improve their effectiveness.

Procedures

- ❑ It shall be the responsibility of Name of Responsible Party or Person to periodically conduct such technical and nontechnical evaluations.
- ❑ Name of Responsible Party or Person shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- ❑ Such technical and nontechnical evaluations shall be conducted at least every six months (or specify another timeframe).
- ❑ The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.
- ❑ The purpose of such evaluations is to improve the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) that we possess or use.
- ❑ Name of Responsible Party or Person shall fully document our periodic technical and nontechnical evaluations to determine the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, in accordance with our Documentation Policy and the requirements of HIPAA.

Responsibilities

Lead Auditor

- ❑ Prepare Internal Audit program.
- ❑ Leads the ISMS internal audit activities.
- ❑ Conducts the opening and closing meeting.
- ❑ Review and approve audit plan.
- ❑ Review and approve audit report.
- ❑ Reviews the corrective and preventive actions and the follow-up audits done based on the internal audit report submitted.

GRC Analyst

- ❑ Prepares an Audit Plan/Notification as a basis for planning the audit and for disseminating information about the audit.
- ❑ Co-ordinates the audit schedule with concerned department/section heads
- ❑ Plans the audit, prepares the working documents and briefs the audit team.
- ❑ Performs the audit using the consolidated audit checklist.
- ❑ Consolidates all audit findings and observations and prepares internal audit report.
- ❑ Reports critical non-conformances to the audited immediately.
- ❑ Report to the auditee the audit results clearly and without delay.

IS Manager

- ❑ Appoints the Lead Auditor and the Audit Team (note: the Lead Auditor and Information Security Manager may be the same person).
- ❑ Facilitates Internal Audit Team activities
- ❑ Provides up-to-date information on ISMS efficiency measurements and monitoring gathered by GRC team
- ❑ Provides up-to-date information on ISMS controls metrics
- ❑ Receives, considers and discusses the audit report from ISMS design standpoint

Auditee

- ❑ Receives, considers and discusses the audit report.
- ❑ Determines, resources, drives and completes corrective actions as necessary.
- ❑ Is and remains accountable for protecting information assets.

Standard

General

- ❑ Only competent personnel that meet ISMS DOC 1.4 Auditors' Qualifications requirement shall perform audits.
- ❑ An ISMS audit program shall be created that contains all scheduled and potential audits for the whole calendar year. This shall include schedule of internal audits, audits of suppliers, audits to be performed by clients and third-party audits, as appropriate
- ❑ Internal audits shall be scheduled annually or as the need arises.
- ❑ All members of the Internal Audit Team shall be appointed by the Information Security Manager.
- ❑ The Lead Auditor shall supervise the activity of the Audit Team.
- ❑ An Audit Notification Memo is sent to the department/section to be audited at least three working days in advance of the audit.
- ❑ Audit performance will be reviewed as part of the Management Review, (see ISMS DOC 5.2).
- ❑ All audit activities: preparation, execution and reporting shall be provided according to ISMS DOC 1.1A Internal Audit Procedure.

Planning and Preparing the Audit

An annual ISMS internal audit program shall be prepared by the Lead Auditor and approved by the CISO. It should be revised to reflect any changes in the priorities or schedule during the year.

Based on the audit program, the GRC Analyst shall prepare the respective audit plans, reviewed and approved by Lead Auditor. It shall be communicated to the auditors and the auditors. It shall be designed to be flexible in order to permit changes based on the information gathered during the audit.

Opening meeting

One or more pre-audit meetings between the IS Manager, Lead Auditor and auditors shall take place not later than one day prior to the audit proper. Objectives are as follows:

- ❑ To ensure the availability of all the resources needed and other logistics that may be required by the auditor
- ❑ The scope of the audit is verified from the Audit Plan
- ❑ The purpose and scope of the audit.
- ❑ Confirmation of the audit plan
- ❑ Clarification of other matters must be settled before the audit takes place.

Audit Execution

The GRC Analyst conduct audit activities according to ISMS DOC 1.1A Internal Audit Procedure.

In order to avoid interruption of business processes, Internal Audit may be divided into phases. Each phase shall be performed according to ISMS DOC 1.1A Internal Audit Procedure**.**

The auditors will perform the internal audit using audit checklist, which contains:

- ❑ Observation Part – contains specific items that are particular to the organizational unit to be audited. The assigned auditors are responsible for generating questions using this form.
- ❑ Systemic Requirements Part– contain items relating to the requirements of ISO/IEC 27001:2013
- ❑ Control Requirements Part– contain items pertaining to controls outlined in Appendix A of ISO/IEC 27001:2013 and described more fully in ISO/IEC 27002:2013.

Audit findings are collected through interviews, examination of documents and observation of activities and conditions in the areas of concern and will be written on the above-mentioned checklist.

Evidence suggesting other non-conformances should be noted if they seem significant, even though not covered by the checklist. Other objective evidence and/or observations that may reflect positively or negatively on the information security management system shall also be listed on the space provided for on the above-mentioned checklists.

Audit Reporting

The audit team shall review all of their findings whether they are to be reported as non-conformances or as observations. Audit finding should likewise be supported by objective evidence.

Classification of findings shall be:

- ❑ **Major non-conformance** – This pertains to a major deficiency in the ISMS. A non-conformity also pertains to one or more element of the ISO 27001 is not implemented. Non-conformances have a direct effect on information security specifically on the preservation of confidentiality, integrity and availability of information assets.
- ❑ **Minor non-conformance** – A minor deficiency. One or more elements of the ISMS is/are only partially complied. Minor non-conformance has an indirect effect on information security.

Note: Both major and minor non-conformances require appropriate corrective actions to be documented.

- ❑ Improvement potential – A hint for improvement, which may or may not be implemented by the auditors.

Note: Improvement potentials, which pertain to an information security weakness, shall require appropriate preventive actions to be documented.

- ❑ Positive findings – Findings that pertain to processes and/or systems that go beyond what is required by the standard.

The GRC Analyst prepare a formal Audit Report (ISMS DOC 1.6 Audit Report, a number of Non-Conformance Reports in **SoftServe** Incident Management System (ISMS DOC 1.2 Corrective and Preventive Action), one relating to each non-conformance identified (including those closed at the time of the audit), and additional sheets covering observations. The findings of the audit are summarized on the Audit Report, including the number and nature of non-conformances.

Where the audit team use support documentation, this may be inserted into the Audit Report as Observations.

Audit Follow-up and Closure

- □ The Lead Auditor shall preside over the Internal Audit closing meeting attended by the Information Security Manager, audit team and the auditors.
- □ The auditors shall report their findings, observations and recommendations, summarizing the good points before discussing non-conformances supported by the audit evidence.
- □ All parties shall safeguard the confidentiality of the internal audit report
- □ The Information Security Manager will file any working papers that do not form part of the official report separately. On receipt of the completed Audit Report, the Information Security Manager logs the Audit Report, and progresses any Non-Conformance Reports through the Corrective, Preventive Action Procedure (ISMS DOC 1.2 Corrective and Preventive Action), cross-referencing the Non-Conformance Report Log Number in **SoftServe** Incident Management System (ISMS DOC 1.2 Corrective and Preventive Action)on the Audit Lead Sheet.
- □ The Information Security Manager reviews the Observations, with a view to raising a Non-Conformance Report in **SoftServe** Incident Management System (ISMS DOC 1.2 Corrective and Preventive Action) relating to each issue. This then serves to address the findings without a formal non-conformance being raised at audit, and without the Audit Report remaining open for an unnecessarily extended period of time.
- □ An audit will not be considered complete and closed until all corrective actions or measures have been successfully implemented to the satisfaction of the Lead Auditor.
- □ When all the non-conformances associated with an audit have been closed a complete copy of the Audit Report is sent to the auditee for confirmation of the closing of the report.
- □ Where the IS Manager has reason to believe that the cause of the non-conformance may have resulted in similar non-conformances elsewhere, he may require follow-up audits to be carried out on that item, either in the originating area or other affected areas. These are planned in accordance with the process described above.
- □ The results of audits shall be summarized by the Lead Auditor and reviewed at Management Review Meetings in accordance with ISMS DOC 5.2.

Records

As well as miscellaneous audit evidence (such as copies of documents, audit notes, records of interviews, system printouts *etc.*), ISMS internal audits generate the following formal records:

- ❑ Audit plan/Notification (ISMS DOC 1.5 Internal Audit Plan)
- ❑ Internal Audit checklist/Observation sheet
- ❑ ISMS DOC 1.6 Audit Report
- ❑ List of Non-conformances from **SoftServe** Incident Management System (http://sde.softserveinc.com/helpdesk/newlogin.asp)

All information shall be appropriately secured given its often confidential nature.

All information shall be properly filed and indexed.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
   1.
      i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
      ii. *Implementation specifications*:
         A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
         B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
         C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
         D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
   2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
   3.
      i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to

prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. *Implementation specifications*:
   A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
   B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
   C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4.
   i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
   ii. *Implementation specifications*:
      A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
      B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
      C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.
   i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
   ii. *Implementation specifications*. Implement:
      A. *Security reminders* (Addressable). Periodic security updates.
      B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
      C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
      D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.
   i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
   ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.
   i. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
   ii. *Implementation specifications*:
      A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
      B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
      C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
      D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
      E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

8. ***Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**

Evaluation (§ 164.308(a)(8))

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.

Evaluation (§ 164.308(a)(8))

Comment: We received several comments that certification should be performed externally. A larger group of commenters preferred self-certification. The majority of the comments, however, were to the effect that external certification should be encouraged but not mandated. A number of commenters thought that mandating external certification would create an undue financial burden, regardless of the size of the entity being certified. One commenter stated that external certification would not place an undue burden on a small or rural provider.

Response: Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

Comment: Several commenters stated that the certification should cover all components of the proposed rule, not just the information systems.

Response: We agree. We have revised this section to reflect that evaluation would be both technical and nontechnical components of security.

Comment: A number of commenters expressed a desire for the creation of certification guides or models to complement the rule.

Response: We agree that creation of compliance guidelines or models for different business environments would help in the implementation and evaluation of HIPAA security requirements and we encourage professional associations and others to do so. We may develop technical assistance materials, but do not intend to create certification criteria because we do not have the resources to address the large number of different business environments.

Comment: Some commenters asked how certification is possible without specifying the level of risk that is permissible.

Response: The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by § 164.306 is provided.

Comment: Several commenters requested creation of a list of federally "certified" security software and off-the-shelf products. Several others stated that this request was not feasible. Regarding certification of off-the-shelf products, one commenter thought this should be encouraged, but not mandated; several thought this would be an impractical endeavor.

Response: While we will not assume the task of certifying software and off-the-shelf products for the reason described above, we have noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see http://www.niap.nist.gov.).

Comment: One commenter stated, "With HCFA's publishing of these HIPAA standards, and their desire to retain the final responsibility for determining violations and imposing penalties of the statute, it also seems appropriate for HCFA to also provide certifying services to ensure security compliance."

Response: In view of the enormous number and variety of covered entities, we believe that evaluation can best be handled through the marketplace, which can develop more usable and targeted evaluation instruments and processes.

Policy Number: 4.2
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Authorization and Supervision Policy Procedure

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).
- ❑ Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, are essential components of a well-managed risk management system.
- ❑ Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, can help reduce our overall risk, and reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to only permit workforce members who have been appropriately authorized, to have access to individually identifiable health information.

- ❑ It is the Policy of **SoftServe Inc.** to properly and appropriately supervise workforce members who have access to individually identifiable health information.
- ❑ Workforce members of **SoftServe Inc.** shall have access only to the individually identifiable health information that they need in order to perform their work-related duties.
- ❑ It is the Policy of **SoftServe Inc.** to fully document the authorization and supervision of all workforce members who have access to individually identifiable health information.

Procedures

The company confidentiality agreements (NDA for all employees and NDA for subcontractors), which requires the maintenance of confidentiality for a set period, include clauses which:

- ❑ Define the information to be protected, its ownership and its classification.
- ❑ Set out the expected duration of the agreement.
- ❑ Describe the required actions on termination of the agreement.
- ❑ Identify the various responsibilities and actions required of signatories in order to avoid unauthorized information disclosure.
- ❑ Identify the permitted use of the information, and the signatories' rights in respect of that information.
- ❑ Clarify rights to audit and monitor use of that information.
- ❑ Describe the process for notification and reporting of unauthorized disclosure or breaches of confidentiality.
- ❑ Set out the terms for the information to be returned or destroyed at agreement cessation.
- ❑ Describe the actions that are to be taken if the agreement is breached.

The company’s legal counsel reviews the agreement annually and whenever there is a relevant change in the law.

The agreement is also reviewed whenever there are significant changes to contracts of employment and contracts for services with third parties.

This confidentiality agreement is, with effect from the date of first issue of this procedure, incorporated into all new and renewed contracts of employment, all new and renewed contracts for services with third parties or subcontractors, and into Non-Disclosure Agreements ('NDAs').

Third parties are required to sign an NDA prior to being given access to confidential information.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:

1.
   i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
   ii. *Implementation specifications*:
      A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
      B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
      C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
      D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
3.
   i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
   ii. *Implementation specifications*:
      A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Key Activities related to Authorization and Supervision Procedures...

❑ Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
❑ Decide how access will be granted to workforce members within the organization.
❑ Select the basis for restricting access.

- ❑ Select an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access.)
- ❑ Determine if direct access to EPHI will ever be appropriate for individuals external to the organization (e.g., business partners or patients seeking access to their own EPHI).

Questions to Consider...

- ❑ Do the organization's IT systems have the capacity to set access controls?
- ❑ Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?
- ❑ Does the organization grant remote access to EPHI?
- ❑ What method(s) of access control is (are) used (e.g., identity-based, role-based, location-based, or a combination)?
- ❑ Are duties separated such that only the minimum necessary EPHI is made available to each staff member based on their job requirements?

Policy Number: 4.3
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Access Authorization Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to access authorization, in accordance with the requirements at § 164.308(a)(4).
- ❑ The implementation of appropriate processes to grant workforce members access to individually identifiable health information and Protected Health Information can help ensure that our uses and disclosures of individually identifiable health information are lawful and appropriate.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to grant workforce members an appropriate level of access to individually identifiable health information that is based on their work-related duties and responsibilities.
- ❑ The level of access to individually identifiable health information and Protected Health Information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all access authorization-related activities and efforts.

Procedures

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard requestor the IT department, will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to 'Confidential', 'Restricted', 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to 'Public' information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
    1.
        i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
        ii. *Implementation specifications*:
            A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
            B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
3.
   i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

   ii. *Implementation specifications*:

      A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

      B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

      C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
4.
   i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

   ii. *Implementation specifications*:

      A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

      B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

      C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Information Access Management (§ 164.308(a)(4))

Comment: One commenter asked that the requirement be deleted, expressing the opinion that this requirement goes beyond "reasonable boundaries" into regulating common business practices. In contrast, another asked that we expand this requirement to identify participating parties and access privileges relative to specific data elements.

Response: We disagree that this requirement improperly imposes upon business functions. Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained.

Comment: Several commenters asked that we not mandate the implementation features, but leave them as optional, a suggested means of compliance. The commenters noted that this might make the rules more scalable and flexible, since this approach would allow providers to implement safeguards that best addressed their needs. Along this line, one commenter expressed the belief that each organization should implement features deemed necessary based on its own risk assessment.

Response: While the information access management standard in this final rule must be met, we agree that the implementation specifications at § 164.308(a)(4)(ii)(B) and (C) should not be mandated but posed as a suggested means of compliance, which must be addressed. These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications. The final rule has been revised accordingly.

Comment: Clarification was requested concerning the meaning of "formal."

Response: The word "formal" has caused considerable concern among commenters, as it was thought "formal" carried the connotation of a rigidly defined structure similar to what might be found in the Department of Defense instructions. As used in the proposed rule, this word was not intended to convey such a strict structure. Rather, it was meant to convey that documentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad. While documentation is still required (see § 164.316), to alleviate confusion, the word "formal" has been deleted.

Comment: One commenter asked that we clarify that this requirement relates to both the establishment of policies for the access control function and to access control (the implementation of those policies).

Response: "Information access management" does address both the establishment of access control policies and their implementation. We use the term "implement" to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures.

Policy Number: 4.4
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Data Integrity Controls Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
- ❑ The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- ❑ The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with VP of IT, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

Procedures

The Board of Directors and management of **SoftServe**, Inc. all parent, subsidiary and/or affiliated companies, and each of their corporations (further referred as organization or **SoftServe**), which is in the business of providing outsourced software development and IT consulting services, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with the organization's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

The organization's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. IS Manager is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are supported by specific documented policies and procedures.

Security incidents, weaknesses and concerns must be reported immediately to IS Manager, who will be responsible for their management and resolution.

All associates of the organization and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All associates, and certain external parties, will receive appropriate training.

The ISMS is subject to continuous, systematic review and improvement.

The **SoftServe**, Inc. has established an Information Security Committee to support the ISMS framework and to periodically review the information security policy (ISMS DOC 6.1 Information Security Committee).

The **SoftServe**, Inc. is committed to achieving certification of its ISMS to ISO27001:2013.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan. Any exceptions to corporate policies should be documented and approved at appropriate level of the corporate management.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with the Sanction Policies of **SoftServe Inc.**

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
   2. *Implementation specifications*:
      i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
      ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
      iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
      iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

b. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

c.
   1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
   2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

d. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

e.

1. *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
2. *Implementation specifications*:
   - i. *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
   - ii. *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

Transmission Security (§ 164.312(e)(1))

Under "Technical Security Mechanisms to Guard against Unauthorized Access to Data that is Transmitted over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) the alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for "Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) "integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

Comment: The proposed definition of "Integrity controls" generated comments that asked that the word "validity" be changed to "Integrity." Commenters were concerned about the ability of an entity to ensure that information was "valid."

Response: We agree with the commenters about the meaning of the word "validity" in the context of the proposed definition of "Integrity controls." We have named "integrity controls" as an implementation specification in this final rule to require mechanisms to ensure that electronically transmitted information is not improperly modified without detection (see § 164.312(c)(1)).

Policy Number: 4.5
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Sanction Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).
- ❑ Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions; can help prevent breaches of individually identifiable health information and Protected Health Information, and can help prevent, or reduce the severity, of HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established policies and procedures, or who commit various offenses.

- ❑ Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- ❑ Certain offenses can invoke immediate termination, including, but not limited to:
    - Theft
    - Intentional lying or deception
    - Drug or alcohol use while on the job
    - Violence against persons or property
- ❑ Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all workforce sanctions and their dispositions, according to our Documentation Policy and HIPAA requirements.

Procedures

Any employee may be given appropriate disciplinary action when violating **SoftServe** policies, standards, procedures or any other action that can cause information security breach or finance loss.

After information security incident revealed, investigation should be conducted by InfoSec Department and if necessary appropriate decision should be made by Review Board. Decision of Review Board may result in one of mentioned actions:

- ❑ Written Warning (Letter of reprimand)
- ❑ Dismissal (in accordance with Employee Dismissal Procedure)

Review Board consists of representatives of InfoSec Department, HR Department, Linear Manager and in certain cases may be extended by other interested parties.

A written warning shall be the first type of disciplinary action for unsatisfactory job performance or any action that might (but didn't) cause financial loss or security breach. A written warning:

- ❑ Must tell the specific performance or conduct deficiencies, omissions or issues that are the basis for the warning.
- ❑ Must tell the specific performance or conduct improvements that must be made.

An employee may receive **written warning (letter of reprimand)** for a current incident of unacceptable personal conduct or grossly inefficient job performance or any action that caused or might cause security breach or financial loss with **Very Low** or **Low Impact** accordingly to the Risk Impact Levels. Warnings (reprimands) are recorded in employee personal file in SSE.

An employee may be **dismissed** for unsatisfactory job performance, or a current incident of grossly inefficient job performance, unacceptable personal conduct or any action that caused or might cause security breach or financial loss with **Low, Medium, High or Very High Impact** accordingly to the Risk Impact Levels.

An employee may be **dismissed** after receiving two or more **written warnings**.

Prior to a disciplinary dismissal, the employee and Review Board must have a pre-disciplinary conference. InfoSec Department should:

- ❑ Schedule and conduct a pre-disciplinary conference
- ❑ Provide advance written notice of the conference to the employee to include:
  - type of disciplinary action
  - acts or failure to act (reasons) justifying the proposed disciplinary action

A copy of the written warning or dismissal should be provided to the employee and sent to the Human Resources Department, InfoSec Department and other interested parties. Record about disciplinary actions should be made in SSE and personal file of employee.

Penalties based on Impact Levels are recommended types of disciplinary actions but final decision regarding disciplinary action type is always taken by Review Board. Disciplinary process shall follow the steps provided in ISMS DOC 7.9 Disciplinary Procedure. Every employee have right to appeal decision made by Review Board (in accordance with ISMS DOC 7.9.1 Appeal Procedure).

HHS Regulations
The Administrative Requirements: Sanctions - § 164.530(e)

1. *Standard: sanctions*. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.
2. *Implementation specification: documentation*. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

HHS Description
The Administrative Requirements: Sanctions

In § 164.518(e) of the NPRM, we proposed to require all covered entities to develop, and apply when appropriate, sanctions against members of its workforce who failed to comply with privacy policies or procedures of the covered entity or with the requirements of the rule. Covered entities would be required to develop and impose sanctions appropriate to the nature of the violation. The preamble stated that the type of sanction applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination. The NPRM preamble language also stated that covered entities would be required to apply sanctions against business associates that violated the proposed rule.

In the final rule, we retain the requirement for sanctions against members of a covered entity's workforce. We also require a covered entity to have written policies and procedures for the application of appropriate sanctions for violations of this subpart and to document those sanctions. These sanctions do not apply to whistleblower activities that meet the provisions of § 164.502(j) or complaints, investigations, or opposition that meet the provisions of § 164.530(g)(2). We eliminate language regarding business associates from this section. Requirements with respect to business associates are stated in § 164.504.

HHS Response to Comments Received
The Administrative Requirements: Sanctions

Comment: Commenters argued that most covered entities already have strict sanctions in place for violations of a patient's privacy, either due to current laws, contractual obligations, or good operating practices. Requiring covered entities to create a formal sanctioning process would be superfluous.

Response: We believe it is important for the covered entity to have these sanction policies and procedures documented so that employees are aware of what actions are prohibited and punishable. For entities that already have sanctions policies in place, it should not be problematic to document those policies. We do not define the particular sanctions that covered entities must impose.

Comment: Several commenters agreed that training should be provided and expectations should be clear so that individuals are not sanctioned for doing things that they did not know were wrong or inappropriate. A good faith exception should be included in the final rule to protect these individuals.

Response: We agree that employees should be trained to understand the covered entity's expectations and understand the consequences of any violation. This is why we are requiring each covered entity to train its workforce. However, we disagree that a good faith exception is explicitly needed in the final rule. We leave the details of sanctions policies to the discretion of the covered entity. We believe it is more appropriate to leave this judgment to the covered entity that will be familiar with the circumstances of the violation, rather than to specify such requirements in the regulation.

Comment: Some commenters felt that the sanctions need to reach business partners as well, not just employees of the covered entities. These commenters felt all violators should be sanctioned, including government officials and agencies.

Response: All members of a covered entity's workforce are subject to sanctions for violations, including government officials who are part of a covered entity's workforce. Requirements for addressing privacy violations by business associates are discussed in §§ 164.504(e) and 164.530(f).

Comments: Many commenters appreciated the flexibility left to the covered entities to determine sanctions. However, some were concerned that the covered entity would need to predict each type of violation and the associated sanction. They argue that, if the Department could not determine this in the NPRM, then the covered entities should be allowed to come up with sanctions as appropriate at the time of the violation. Some commenters wanted a better explanation and understanding of what HHS' expectation is of when is it appropriate to apply sanctions. Some commenters felt that the sanctioning requirement is nebulous and requires independent judgment of compliance; as a result it is hard to enforce. Offending individuals may use the vagueness of the standard as a defense.

Response: We agree with the commenters that argue that covered entities should be allowed to determine the specific sanctions as appropriate at the time of the violation. We believe it is more appropriate to leave this judgment to the covered entity, because the covered entity will be familiar with the circumstances of the violation and the best way to improve compliance.

Comment: A commenter felt that the self-imposition of this requirement is an inadequate protection, as there is an inherent conflict of interest when an entity must sanction one of its own.

Response: We believe it is in the covered entity's best interests to appropriately sanction those individuals who do not follow the outlined policies and procedures. Allowing violations to go unpunished may lead bigger problems later, and result in complaints being registered with the Department by aggrieved parties and/or an enforcement action.

Comment: This provision should cover all violations, not just repeat violations.

Response: We do not limit this requirement to repeat offenses.

SECTION 5

Policy Number: 5.0
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Breach Notification Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
- ❑ Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Timely notifications to affected Covered Entities about breaches of individually identifiable health information and Protected Health Information can help reduce or prevent identity theft and fraud.
- ❑ Timely notifications to affected Covered Entities about breaches of individually identifiable health information and Protected Health Information can help protect our business and reputation.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

1. Breach excludes:
   i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
   ii. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

    iii. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
    i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
    iii. Whether the protected health information was actually acquired or viewed; and
    iv. The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to provide timely notifications to the affected Covered Entity about all breaches of Protected Health Information.
- □ **SoftServe Inc.** shall notify the affected Covered Entity when any breach of Protected Health Information is discovered. A breach is treated as "discovered" by **SoftServe Inc.** the first day on which such breach is known or should reasonably have been known to any employee or agent of **SoftServe Inc.**, other than the person who committed the breach.

Procedures

- □ Breach Notices must include a brief description of what happened, a description of the types of PHI involved, a brief description of the actions taken in response to the breach, and contact procedures for the Covered Entity to ask questions and obtain further information.
- □ Telephone and email shall be the default methods of notification to the Covered Entity.
- □ Business Associates (subcontractors) of **SoftServe Inc.** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **SoftServe Inc.'s** designated HIPAA Officer or Privacy Officer; or other responsible party (if no Privacy Official has been designated).
- □ Business Associate contracts, whether existing or new, shall have corresponding Breach Notification requirements included in them.
- □ Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **SoftServe Inc.'s** Sanction Policy.
- □ All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **SoftServe Inc.'s** Documentation Policy.

❑ The abbreviation "CE" refers to "Covered Entities".
❑ The abbreviation "BA" refers to "Business Associates".

Under the Omnibus Final Rule
The Omnibus Rule amends the definition of breach to clarify that the impermissible acquisition, access, use, or disclosure of PHI *is presumed to be a breach* and breach notification is necessary unless a covered entity or business associate can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised.

Under the final rule, CEs must determine whether there is a *low probability* that the PHI was compromised – a far different standard than whether there is a significant risk of harm to the individual. As a result, CEs will have to significantly modify their current procedures for conducting a risk assessment, and it is likely that more impermissible uses and disclosures will be reportable breaches under the Final Rule than under the interim final rule.

The new risk assessment requirement for breaches becomes effective September 23, 2013.

Four Factors to Consider in a Breach Risk Assessment
The Omnibus Rule identifies four factors that must be considered in a risk assessment:

1. The nature and extent of the PHI involved -- Was sensitive data, such as Social Security numbers and detailed clinical information, involved in an incident?
2. The unauthorized person who used the PHI or to whom the disclosure was made -- If the disclosures were to another HIPAA-regulated entity or to a federal agency, for example, this may result in a "lower probability that the [PHI] has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity."
3. Whether the PHI actually was acquired or viewed -- This would typically involve a forensic analysis or investigation that could determine whether PHI contained on a lost or stolen laptop or other portable electronic device actually was viewed or accessed.
4. The extent to which the risk to the PHI has been mitigated -- This might involve reaching out to an unauthorized recipient of the PHI to obtain "satisfactory assurances" that any PHI sent to a recipient was not further used or disclosed but instead destroyed.

HHS indicates that covered entities and business associates must evaluate the overall probability that PHI has been compromised by considering all combined factors in a thorough risk assessment. HHS states that it will issue additional guidance in the future to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.

HHS expects risk assessments to be "thorough, completed in good faith, and for the conclusions reached to be reasonable," and noted "additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised."

Breach Notification Only Applies to "Unsecured" PHI
Breach Notification only applies to PHI that *has not* been "secured" (encrypted) according to HHS and NIST standards. PHI that has been secured by these standards, and is subsequently breached, *does not invoke any Breach Notification requirements*.

The current encryption Standard referenced in the Final Rule is: "*Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*".
(74 Federal Register, Pages 42,740-42,742)

This Breach Notification exception *does not apply* to paper, film, and other hardcopy PHI, because these materials cannot be electronically encrypted (protected) in their native forms.

Exceptions to the Definition of "Breach"
The Interim Final Rule (prior to the Omnibus Final Rule) included three exceptions to the definition of "breach." These exceptions were adopted without modification in the Final Omnibus Rule. The exceptions are as follows:

1. Unintentional acquisition, access, or use of PHI by an employee or other person acting under the authority of a CE or BA if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the CE or BA, and such information is not further acquired, accessed, used, or disclosed by any person;
2. Inadvertent disclosure of PHI from one person authorized to access PHI at a facility operated by a CE or BA to another person similarly situated at the same facility, and the information received is not further acquired, accessed, used or disclosed without authorization by any person; and
3. Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Breaches - Limited Data Set Exception Removed
The Omnibus Rule removes the exception for limited data sets that do not contain birth dates or ZIP codes. By removing this exception, the Omnibus Rule requires that the impermissible acquisition, access, use, or disclosure of limited data sets, even those that do not contain birth dates or ZIP codes, be subject to a risk assessment to demonstrate that breach notification is not required.

Under the Final Rule, CEs must perform a risk assessment evaluating the required factors, following the impermissible use or disclosure of any limited data set, even if it *excludes* birth dates and zip codes.

Breaches – Voluntary Notifications without Risk Assessment
A CE or BA has the discretion to *voluntarily* provide the required notifications following an impermissible use or disclosure of Protected Health Information *without* performing a risk assessment.

Breaches -- Notification to HHS

The HITECH Act requires CEs to notify HHS of breaches of unsecured PHI, with the timing of such notification based on the size of the breach. As has been the case, the Omnibus Rule requires notification of breaches affecting 500 or more individuals contemporaneously with notification of the affected individuals.

For breaches affecting fewer than 500 individuals, the Omnibus Rule clarifies that CEs must notify HHS within 60 days after the end of the calendar year in which the breaches were "discovered," not in which the breaches "occurred."

Breaches – Notifications to Individuals and Media

The Omnibus Final Rule adopts almost all of the Interim Final Rule's Breach Notification provisions without modification, including the following:

1. CEs must notify individuals when a reportable breach is discovered. A breach is treated as "discovered" by the CE the first day on which such breach is known or should reasonably have been known to any employee or agent of the CE, other than the person who committed the breach.
2. Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.
3. Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
4. First class mail is the default method of notification. A CE may use e-mail if requested by the individual, or substitute notice via the CE's website or local print or broadcast media if the CE does not have current contact information.
5. CEs must notify major local media outlets of a breach affecting more than 500 individuals.
6. BAs must provide notice of breach to a CE without unreasonable delay and in no event later than 60 days from discovery of the breach by the BA.

Breaches – Duty to Mitigate Harm Remains

The Omnibus Rule retains the need for CEs and BAs to mitigate "harm to individuals." The Final Rule retains the statutory term "mitigate harm to individuals" to make clear that the notification should describe the steps the CE or BA is taking to mitigate potential harm to individuals resulting from the breach and that such harm is not limited to economic loss.

Policy Number: 5.1
Effective Date: 3/26/2013
Last Revised: 4/28/2014

HIPAA Investigations Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ **SoftServe Inc.** recognizes that the U.S. Department of Health and Human Services ("HHS"), its Office for Civil Rights ("OCR") and other designees, as well as State Attorneys General, are all authorized and empowered to investigate Covered Entities and Business Associates in matters of HIPAA compliance and enforcement.
- ❑ **SoftServe Inc.** recognizes that timely and full cooperation with such investigative bodies is mandatory under HIPAA law; and that failure to cooperate with any HIPAA investigation is itself a violation of HIPAA Rules.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS.
- ❑ It is the Policy of **SoftServe Inc.** to not impede or obstruct any HIPAA-related investigations conducted by HHS.
- ❑ It is the Policy of **SoftServe Inc.** to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

Procedures

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

- ❑ Whenever a HHS investigation is discovered, the following persons must be immediately notified:
  - Attorneys (HIPAA counsel and local counsel, if different)
  - Executive Management
  - Privacy Officer
  - Security Officer

  - Compliance Officer
  - Health Information Management Department and/or the Custodian of Records

❑ Cooperate, but do not volunteer information or records that are not requested.

❑ Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. BE SURE that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)

❑ Have at least one, if not two witnesses available to testify as to your requests and their responses.

❑ Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.

❑ Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask.

❑ Permit the investigators to have access to protected health information ("PHI"), in accordance with our notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.

❑ Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.

❑ Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.

❑ Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.

❑ Ask the investigators for documents related to the investigation. For example, request:

  - copies of any search warrants and/or entry and inspection orders
  - copies of any complaints
  - a list of patients they are interested in
  - a list of documents/items seized

❑ Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).

❑ Do not leave the investigators alone, if possible. Assign someone to "assist" each investigator present.

❑ Do not offer food (coffee, if already prepared, and water, if already available, is ok. Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.

- ❑ Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

1. Personnel that may be interviewed
    - President, CEO or Director
    - HIPAA Compliance Officer
    - Lead Systems Manager or Director
    - Systems Security Officer
    - Lead Network Engineer and/or individuals responsible for:
        - o Administration of systems which store, transmit, or access Electronic Protected Health Information (EPHI)
        - o Administration systems networks (wired and wireless)
        - o Monitoring of systems which store, transmit, or access EPHI
        - o Monitoring systems networks (if different from above)
    - Computer Hardware Specialist
    - Disaster Recovery Specialist or person in charge of data backup
    - Facility Access Control Coordinator (physical security)
    - Human Resources Representative
    - Director of Training
    - Incident Response Team Leader
    - Others as identified….
2. Documents and other information that may be requested for investigations/reviews
    - a. Policies and Procedures and other Evidence that Address the Following:
        - Prevention, detection, containment, and correction of security violations
        - Employee background checks and confidentiality agreements
        - Establishing user access for new and existing employees
        - List of authentication methods used to identify users authorized to access EPHI
        - List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
        - List of software used to manage and control access to the Internet
        - Detecting, reporting, and responding to security incidents (if not in the security plan)
        - Physical security
        - Encryption and decryption of EPHI
        - Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)
        - Monitoring systems use - authorized and unauthorized
        - Use of wireless networks
        - Granting, approving, and monitoring systems access (for example, by level, role, and job function)
        - Sanctions for workforce members in violation of policies and procedures governing EPHI access or use

- Termination of systems access
- Session termination policies and procedures for inactive computer systems
- Policies and procedures for emergency access to electronic information systems
- Password management policies and procedures
- Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)
- Disposal of media and devices containing EPHI

b. Other Documents:

- Entity-wide Security Plan
- Risk Analysis (most recent)
- Risk Management Plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
    - o Results from most recent vulnerability scan
- Network penetration testing policy and procedure
    - o Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
- Configuration standards to include patch management for systems which store, transmit, or access EPHI (including workstations)
- Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI
- Organization chart to include staff members responsible for general HIPAA compliance to include the protection of EPHI
- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of EPHI policies and procedures (security awareness training)
- Policies and procedures governing the use of virus protection software
- Data backup procedures
- Disaster recovery plan
- Disaster recovery test plans and results
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain EPHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement media and devices that contain EPHI

Policy Number: 5.2
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Patient Rights Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements pertaining to the rights of patients at § 164.520, to § 164.528, as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- ❑ Patient information related to patient rights includes only that information contained in each patient's Designated Record Set ("DRS"), which is defined in the HIPAA regulations at § 164.501 as:
  - A group of records maintained by or for a covered entity that is:
    - The medical records and billing records about individuals maintained by or for a covered health care provider;
    - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
    - Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- ❑ The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable health information.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to provide all the patient rights to our patients that are called for in the HIPAA regulations.
- ❑ Patient Rights that we provide and support include:
  - The Right to receive a copy of our "Notice of Privacy Practices", which details how individually identifiable health information may be used or disclosed by this organization.

- The Right to review or obtain a copy of medical records about that patient, or about the patient's minor children.
- The Right to request restrictions on the use or disclosure of the patient's medical records.
- The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
- The Right to request amendments to medical records, with certain limitations.
- The Right to an accounting of certain disclosures of individually identifiable health information.
- The Right to file a privacy complaint directly with us, or with the federal government.

❑ No retaliation of any kind is permitted against any person, patient, or workforce member for exercising any Right guaranteed by HIPAA.

HHS Regulations
Notice of Privacy Practices: Right to Notice - § 164.520(a)

Standard: notice of privacy practices.

1. *Right to notice*. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.
2. *Exception for group health plans*.
    i. An individual enrolled in a group health plan has a right to notice:
        A. From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or
        B. From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.
    ii. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has dis-enrolled from a health insurance issuer or HMO offered by the plan, must:
        A. Maintain a notice under this section; and
        B. Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.
    iii. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has dis-enrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

3. *Exception for inmates*. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

HHS Regulations as Amended January 2013
Notice of Privacy Practices: Provision of the Notice - § 164.520(c)

Implementation specifications: provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

1. *Specific requirements for health plans*.
    i. A health plan must provide the notice:
        A. No later than the compliance date for the health plan, to individuals then covered by the plan;
        B. Thereafter, at the time of enrollment, to individuals who are new enrollees.
    ii. No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.
    iii. The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.
    iv. If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.
    v. If there is a material change to the notice:
        A. A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.
        B. A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.
2. *Specific requirements for certain covered health care providers*. A covered health care provider that has a direct treatment relationship with an individual must:
    i. Provide the notice:
        A. No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or
        B. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.
    ii. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reasons why the acknowledgment was not obtained.
    iii. If the covered health care provider maintains a physical service delivery site:

A. Have the notice available at the service delivery site for individuals to request to take with them; and

B. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

iv. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

3. *Specific requirements for electronic notice*.

i. A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

ii. A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

iii. For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

iv. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

HHS Regulations as Amended January 2013

Right of Individual to Request Restriction of Uses and Disclosures of PHI - § 164.522(a)

1. *Standard: right of an individual to request restriction of uses and disclosures*.

i. A covered entity must permit an individual to request that the covered entity restrict:

A. Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

B. Disclosures permitted under § 164.510(b).

ii. Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

iii. A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

iv. If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

v. A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

vi. A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

A. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

B. The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

2. *Implementation specifications: terminating a restriction*. A covered entity may terminate its agreement to a restriction, if:

i. The individual agrees to or requests the termination in writing;

ii. The individual orally agrees to the termination and the oral agreement is documented; or

iii. The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

A. Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

B. Only effective with respect to protected health information created or received after it has so informed the individual.

3. *Implementation specification: documentation*. A covered entity must document a restriction in accordance with Sec. 160.530(j) of this subchapter.

HHS Regulations
Rights to Request Privacy Protection: Confidential Communications - § 164.522(b)

1. *Standard: confidential communications requirements*.

i. A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

ii. A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,

2. *Implementation specifications: conditions on providing confidential communications*.

i. A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

ii. A covered entity may condition the provision of a reasonable accommodation on:

A. When appropriate, information as to how payment, if any, will be handled; and

B. Specification of an alternative address or other method of contact.

iii. A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

- iv. A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

HHS Regulations
Access to Protected Health Information - § 164.524(a)

Standard: access to protected health information.

1. *Right of access*. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:
    - i. Psychotherapy notes;
    - ii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
    - iii. Protected health information maintained by a covered entity that is:
        - A. Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
        - B. Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
2. *Unreviewable grounds for denial*. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.
    - i. The protected health information is exempted from the right of access by paragraph (a)(1) of this section.
    - ii. A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
    - iii. An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
    - iv. An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
    - v. An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
3. *Reviewable grounds for denial*. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

   i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
   ii. The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
   iii. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
4. *Review of a denial of access*. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

HHS Regulations as Amended January 2013
Access of Individuals to Protected Health Information: Requests for Access and Timely Action - § 164.524(b)

Implementation specifications: requests for access and timely action.

1. *Individual's request for access*. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.
2. *Timely action by the covered entity*.
   i. Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.
      A. If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.
      B. If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.
   ii. If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:
      A. The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
      B. The covered entity may have only one such extension of time for action on a request for access.

HHS Regulations as Amended January 2013
Access of Individuals to Protected Health Information: Provision of Access - § 164.524(c)

Implementation specifications: provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. *Providing the access requested*. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.
2. *Form of access requested*.
   i. The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.
   ii. Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.
   iii. The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:
      A. The individual agrees in advance to such a summary or explanation; and
      B. The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
3. *Time and manner of access*.
   i. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual’s request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
   ii. If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.
4. *Fees*. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
   i. Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

ii. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
iii. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
iv. Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

HHS Regulations
Access of Individuals to Protected Health Information: Denial of Access - § 164.524(d)

Implementation specifications: denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. *Making other information accessible*. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.
2. *Denial*. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:
   i. The basis for the denial;
   ii. If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and
   iii. A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).
3. *Other responsibility*. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.
4. *Review of denial requested*. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

HHS Regulations

Right to Amend - § 164.526(a)

Standard: right to amend.

1. *Right to amend*. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.
2. *Denial of amendment*. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:
   i. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
   ii. Is not part of the designated record set;
   iii. Would not be available for inspection under § 164.524; or
   iv. Is accurate and complete.

HHS Regulations as Amended August 2002
Right to an Accounting of Disclosures - § 164.528(a)

Standard: right to an accounting of disclosures of protected health information.

1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:
   i. To carry out treatment, payment and health care operations as provided in § 164.506;
   ii. To individuals of protected health information about them as provided in § 164.502;
   iii. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
   iv. Pursuant to an authorization as provided in § 164.508;
   v. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;
   vi. For national security or intelligence purposes as provided in § 164.512(k)(2);
   vii. To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
   viii. As part of a limited data set in accordance with § 164.514(e); or
   ix. That occurred prior to the compliance date for the covered entity.
2.
   i. The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

ii. If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

A. Document the statement, including the identity of the agency or official making the statement;

B. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

C. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

3. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

HHS Regulations
The Administrative Requirements: Waiver of Rights - § 164.530(h)

Standard: waiver of rights. A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

SECTION 6

Policy Number: 6.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Access Establishment and Modification Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and modification of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(4).
- ❑ Establishing, maintaining, and modifying appropriate levels of workforce member access to individually identifiable health information and Protected Health Information can help reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to provide a lawful and appropriate level of access to individually identifiable health information for each and every workforce member.
- ❑ Such access to individually identifiable health information shall be granted based on the nature and duties of the workforce member's job.
- ❑ Higher levels of access shall be provided only to those who need it.
- ❑ Any workforce member's ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all access establishment and modification-related activities and efforts, according to our Documentation Policy.

Procedures

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department, will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which are located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to ‘Confidential’, ‘Restricted’, 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to ‘Public’ information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
    1.
        i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
        ii. *Implementation specifications*:
            A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
            B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
            C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

    D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
3.
    i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

    ii. *Implementation specifications*:

        A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

        B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

        C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
4.
    i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

    ii. *Implementation specifications*:

        A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

        B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

        C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Information Access Management (§ 164.308(a)(4))

Comment: One commenter asked that the requirement be deleted, expressing the opinion that this requirement goes beyond "reasonable boundaries" into regulating common business practices. In contrast, another asked that we expand this requirement to identify participating parties and access privileges relative to specific data elements.

Response: We disagree that this requirement improperly imposes upon business functions. Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained.

Comment: Several commenters asked that we not mandate the implementation features, but leave them as optional, a suggested means of compliance. The commenters noted that this might make the rules more scalable and flexible, since this approach would allow providers to implement safeguards that best addressed their needs. Along this line, one commenter expressed the belief that each organization should implement features deemed necessary based on its own risk assessment.

Response: While the information access management standard in this final rule must be met, we agree that the implementation specifications at § 164.308(a)(4)(ii)(B) and (C) should not be mandated but posed as a suggested means of compliance, which must be addressed. These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications. The final rule has been revised accordingly.

Comment: Clarification was requested concerning the meaning of "formal."

Response: The word "formal" has caused considerable concern among commenters, as it was thought "formal" carried the connotation of a rigidly defined structure similar to what might be found in the Department of Defense instructions. As used in the proposed rule, this word was not intended to convey such a strict structure. Rather, it was meant to convey that documentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad. While documentation is still required (see § 164.316), to alleviate confusion, the word "formal" has been deleted.

Comment: One commenter asked that we clarify that this requirement relates to both the establishment of policies for the access control function and to access control (the implementation of those policies).

Response: "Information access management" does address both the establishment of access control policies and their implementation. We use the term "implement" to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures.

Policy Number: 6.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Access Termination Policy Procedure

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the termination of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(3).
- ❑ Prompt and appropriate termination of workforce member access to individually identifiable health information and Protected Health Information can greatly reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to terminate any workforce member's access to individually identifiable health information and Protected Health Information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
- ❑ Termination of workforce member access to individually identifiable health information and Protected Health Information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.
- ❑ In no case shall the termination of access to individually identifiable health information and Protected Health Information be delayed more than (Insert Time Period – 30 to 60 minutes is recommended, but 24 hours should be the maximum) from the moment of such a triggering event.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all access termination-related activities, in accordance with our Documentation Policy.

Procedures

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to ‘Confidential’, ‘Restricted’, 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to ‘Public’ information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
    1.
        i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
        ii. *Implementation specifications*:
            A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
3.
   i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
   ii. *Implementation specifications*:
      A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
      B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
      C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

In a...requirement entitled "Termination procedures," we proposed implementation features for the ending of an employee's employment or an internal or external user's access. These features would include things such as changing combination locks, removal from access lists, removal of user account(s), and the turning in of keys, tokens, or cards that allow access.

In this final rule, "Termination procedures" has been made an addressable implementation specification under "Workforce security." This is addressable because in certain circumstances, for example, a solo physician practice whose staff consists only of the physician's spouse, formal procedures may not be necessary.

Comment: The majority of commenters on the "Termination procedures" requirement asked that it be made optional, stating that it may not be applicable or even appropriate in all circumstances and should be so qualified or posed as guidelines. A number of commenters stated that the requirement should be deleted. One commenter stated that much of the material covered under the "Termination procedures" requirement is already covered in "Information access control." A number of commenters stated that this requirement was too detailed and some of the requirements excessive.

Response: Based upon the comments received, we agree that termination procedures should not be a separate standard; however, consideration of termination procedures remains relevant for any covered entity with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain. We further agree with the reasoning of the commenters who asked that these procedures be made optional; therefore, "Termination procedures" is now reflected in this final rule as an addressable implementation specification. We also removed reference to all specific termination activities, for example, changing locks, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others.

Comment: One commenter asked whether human resource employee termination policies and procedures must be documented to show the types of security breaches that would result in termination.

Response: Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below). The purpose of termination procedure documentation under this implementation specification is not to detail when or under which circumstances an employee should be terminated. This information would more appropriately be part of the entity's sanction policy. The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving keys when a termination occurs.

Policy Number: 6.2
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Security Reminders Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to security reminders, in accordance with the requirements at § 164.308(a)(5).

- ❑ The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- ❑ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all information security reminder-related activities and efforts, according to our Documentation Policy.

Procedures

The Information Security Awareness and Training Program is designed to ensure that all individuals are appropriately trained in how to fulfill their duties and responsibilities in view of Information Security while they access to company information systems.

Such trainings shall ensure that employees are versed in the Information Security policies and standards of the company, bring the security awareness of **SoftServe** employee to higher level and decrease likelihood of related informational risks.

All employees of **SoftServe** before allowing them access to company information resources are required to sign documents (see section 3.1 above) provided by HR Department during employment and documents (see section 3.2 above) provided by ITSD Department during On-boarding Awareness meeting.

All employees of **SoftServe** are required to participate in Information Security Training and Awareness Program within 30 days of starting work. All employees are required to pass the IST&A Program Quizzes on a yearly basis (see ISMS DOC 7.6 Information Security Training and Awareness Guidelines). None of the employees should be promoted or their salary raised without successfully passing Information Security Training and Awareness Program Quizzes.

Security Awareness Presentations and Reminders

- ❑ IS Manager shall develop and maintain a communications process to communicate new information security program, security bulletin information, and security items of interest.
- ❑ The VP HR shall organize security awareness trainings within **SoftServe** employee using material developed by IS Manager.
- ❑ Security awareness presentations or messages may be delivered in variety of forms (e.g. e-mail, posters, pop-up messages, web-based sessions or other media depending on the complexity of the message. These messages may also be delivered through "sign-on warning banners" that address information privacy and security issues to all logon/access points to computer information systems where technically practical.)
- ❑ All workforce members shall receive continuing information security awareness updates that focus attention on security issues.

Security Management Training

- ❑ The IS Manager shall provide security management training for the Executives, Managers and Information Asset Owners.
- ❑ The IS Manager shall assist the Executives, Managers and Information Asset Owners in identifying training needs for them.
- ❑ The IS Manager shall ensure that ISMS and ISO skills of related personnel are at an adequate level and yearly, professional security training courses and seminars necessary for this are provided.

System Specific Security Training for Project/Department/SBU staff

- ❑ Department managers/SBU Managers/Project Managers must ensure that all needed members have training and supporting reference materials sufficient to allow them to protect information resources.
- ❑ Department managers/SBU Managers/Project Managers in consultation with affiliate vendor shall provide system- specific security training.
- ❑ When project members' job responsibilities change, their information security needs must be re-assessed by the immediate supervisor. New security training must be provided as necessary for the change in job responsibility.

Professional Security Training

- ❑ Provisions for System/Network administrators and all IT staff training shall include training in information security threats and safeguards, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards. Where IT staff change jobs, their information security needs must be re-assessed and any new training provided as a priority.

Training Evaluation

- ❑ The HR Director shall work with each **SoftServe** Department to monitor training requirements, compliance and effectiveness. Key information to be captured shall include courses, dates, audience members, costs and sources in order to provide enterprise wide analysis and reporting regarding awareness, training, and education initiatives. Captured information shall also include test scores, audience commentary, and suggestions for improving the provided training.
- ❑ All security training and awareness presentations shall provide formal evaluation and feedback mechanisms to address objectives initially established for the training program. Methods for evaluation and feedback may include but are not limited to evaluation forms/questionnaires, focus groups, selective interviews, independent observations, formal status reports and questioners. The IS Manager shall work with the VP HR in evaluating the adequacy and effectiveness of the information security program and seek ways of improving upon the quality of this program.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

A covered entity or business associate must, in accordance with § 164.306:

- ❑ Standard*: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
- ❑ Implementation *specifications*. Implement:
  - *Security reminders* (Addressable). Periodic security updates.
  - *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
  - *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
  - *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

Security Awareness and Training (§ 164.308(a)(5))

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

Comment: Several commenters asked how often training should be conducted and asked for a definition of "periodic," as it appears in the proposed implementation feature "Periodic security reminders." One asked if the training should be tailored to job need.

Response: Amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.

Policy Number: 6.3
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Facility Security Maintenance Records Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security maintenance records, in accordance with the requirements at § 164.310(a)(1-2).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
- ❑ Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.
- ❑ It is the Policy of **SoftServe Inc.** to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- ❑ Responsibility for the creation and updating of facility security maintenance records is hereby assigned to The Head of Physical Security, who shall establish procedures for maintaining such records in appropriate form.

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department, will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user’s **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure.

Users’ access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of user’s access rights should be provided in accordance with formal procedure.

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer’s approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to ‘Confidential’, ‘Restricted’, 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to ‘Public’ information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
2. *Implementation specifications*:
   i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
   ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
   iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
   iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Facility Access Controls (§ 164.310(a)(1))

We proposed, under the "Physical access controls" requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, **maintenance records**, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

In § 164.310(a)(2), we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.

Policy Number: 6.4
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Data Backup Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backups, in accordance with the requirements at § 164.308(a)(7) and elsewhere in the Regulations.
- ❑ The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- ❑ The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- ❑ Timely access to health information is crucial to providing high quality health care, and to our business operations.
- ❑ Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
- ❑ No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- ❑ A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
- ❑ All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times.

Procedures

□ **Name of Responsible Party or Person** is responsible for performing daily backups on __**SoftServe Inc.’s** network, including shared drives containing application data, patient information, financial data, and crucial system information.

□ **SoftServe Inc.** will back up all such data automatically, per **Name of Backup Solution**’s programmed standards, nightly at 2300 hours.

□ **Name of Responsible Party or Person,** or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in **Location of Backup Vault or Facility**.

□ The media vault meets fire and disaster standards for media and will be kept locked at all times. Only the **Name of Responsible Party or Person**, the system administrator, and their designees have access to the media vault.

□ In the event that the secured media vault is not available or properly functioning, the **Name of Responsible Party or Person**, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.

□ **Name of Responsible Party or Person**, the system administrator, or their designees will use__**Name of Backup Solution**’s reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.

□ Individuals so validating the backup will generate daily reports and log them in the network log in the system administrator’s office. The system administrator will maintain such reports for a minimum of 30 days (or specify other number of days, weeks, or months).

□ Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.

□ Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer’s recommended guidelines, currently once per week (or specify other period).

□ A rotation of four, or specify other number weekly data tapes must be maintained at all times.

□ **Name of Responsible Party or Person** will ensure replacement of backup tapes or media according to manufacturer’s recommended guidelines, currently annually (or specify other media replacement timeframe(s)).

□ The **Name of Responsible Party or Person** is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly (or specify other period) and more often if necessary to ensure data integrity, availability, and confidentiality.

□ Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.

□ All personnel who detect or suspect a data backup problem should immediately report the same to the **Name of Responsible Party or Person**. Such personnel should follow up immediate notification with a written memorandum that includes the following information:

- Narrative of the data backup problem.
- How long the problem has existed.
- Suggested solutions.

Standard backup parameters

Full backup — a complete backup which, besides files, incorporates additional information about the time of their last modification. Used in combination with **Incremental backup** or **Differential backup.**

Incremental backup — a partial backup that only incorporates files modified after the last full **backup** or **incremental backup**. Used in combination with Full backup. **Incremental backups** take up less space than differential backup, but first the **full backup** needs to be recovered followed by a recovery of all **incremental backups** as of the relevant date in order to recover information.

Differential Backup — a partial backup that incorporates all files modified after the last **full backup**. Used in combination with **full backup**. **Differential backups** take up more space than **incremental backups**, but only the **full backup** and one **differential backup** need to be recovered as of the relevant date in order to recover information. Differential backups constantly grow in size after the last **full backup**. Therefore, the **full backup** needs to be done more often that in case of **full/incremental.**

Retention time — a parameter defining how long backups should be kept.

The following default parameters are set depending on the significance and type of information:

	Retention time	Backup frequency	Backup method	Notes
Project documentation, financial and administrative data	4 weeks	Daily	Semi-monthly **full backup**, daily **differential backup**	This scheme allows information recovery as of the end of the previous day
Versions of finished project products	4 weeks	Daily	Semi-monthly **full backup**, daily **incremental backup**	-//-
Setups and components necessary for project work	4 weeks	Daily	Semi-monthly **full backup**, daily **incremental backup**	-//-

Interim and final codes of the software product	4 weeks	Daily	Weekly **full backup**, daily **differential backup**	-//-
Mailboxes	1 week	Daily	Weekly **full backup**, daily **differential backup**	-//-
User information	1 week	Daily	Weekly **full backup**, daily **incremental backup**	-//-
System files and server bases	2 weeks	Daily	Weekly **full backup**,	Allows recovery of server operation

Backup methods

Backup is automatically performed by specialized servers. Backup server administrators and owners of resources to be backed up are sent automatic notifications on successful performance of scheduled backup tasks. Access to backup servers and media used to store backups is limited. Backup server administrators are responsible for successful performance of all backup tasks. Backup tasks should be carried out at hours when resources to be backed up are least loaded.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
    1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
    2. *Implementation specifications*:
        - i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
        - ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
        - iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
        - iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

d.
    1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
    2. *Implementation specifications*:
        - i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
        - ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Device and Media Controls (§ 164.310(d)(1))

Comment: One commenter was concerned about the exclusion of removable media devices from examples of physical types of hardware and/or software.

Response: The media examples used were not intended to represent all possible physical types of hardware and/or software. Removable media devices, although not specifically listed, are not intended to be excluded.

Comment: Comments were made that the issue of equipment re-use or recycling of media containing mass storage was not addressed in "Media controls."

Response: We agree that equipment re-use or recycling should be addressed, since this equipment may contain electronic protected health information. The "Device and media controls" standard is accordingly expanded to include a required implementation specification that addresses the re-use of media (see § 164.310(d)(2)(ii)).

Comment: Several commenters asked for a definition of the term "facility," as used in the proposed "Media controls" requirement description. Commenters were unclear whether we were talking about a corporate entity or the physical plant.

Response: The term "facility" refers to the physical premises and the interior and exterior of a building(s). We have added this definition to § 164.304.

Comment: Several commenters believe the "Media controls" implementation features are too onerous and should be deleted.

Response: While the "Device and media controls" standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the "Accountability and data backup" implementation specification as addressable to provide more flexibility in meeting the standard.

Comment: One commenter was concerned about the accountability impact of audit trails on system resources and the pace of system services.

Response: The proposed audit trail implementation feature appears as the addressable "Accountability" implementation specification. The name change better reflects the purpose and intended scope of the implementation specification. This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services.

Comment: A commenter was concerned about the resource expenditure (system and fiscal) for total e-mail backup and wanted a clarification of the extensiveness of data backup.

Response: The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business "as usual" in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.

Policy Number: 6.5
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Facility Security Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a)(1-2).
- ❑ In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.

Procedures

- ❑ Primary responsibility for facility security is hereby assigned to <u>Name of Responsible Party or Person</u>, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- ❑ The analyses of our facility security should include, but are not limited to, the following factors:
  - Windows and doors
  - Roofs and the potential for roof access
  - Locks and keys
  - Electronic access control systems
  - Video cameras and video surveillance systems
  - Electronic alarms and related systems
  - Employee, partner, vendor and guest access
  - Vehicle parking security
  - Routine and non-routine deliveries

Scope

All **SoftServe** offices are subject to controlled access and usage.

Special rooms are rooms with additional security and restricted access.

Responsibilities

Head of Physical Security or DCD is accountable for identification persons that are authorized to access secure area.

Owner of the secure area is an assigned employee who's responsible for performing and approving any activities in the area. The Owner of a secure area is responsible for ensuring that no unsupervised activities take place within the secure area.

Standard

Special rooms (secure areas at **SoftServe**) are:

- ❑ Server
- ❑ Accounting premises
- ❑ IT Department premises
- ❑ Financial premises
- ❑ Legal Departments premises
- ❑ Top-management offices
- ❑ Warehouses
- ❑ Technological rooms (electro panel, ventilation, etc.).
- ❑ Human Resources (rooms with personnel documentation)
- ❑ Healthcare dev. department

The workplaces of duty guards: (only for offices, where a physical guard is present) are located near reception area in offices. Secure areas must be locked at all times. Details of the lock specification described in p.3. "Office Security Policy and Procedure".
Access to secure areas where confidential or internal information is processed (including in conversation) or stored is restricted to authorized persons. Authorization is provided by RFID Card according to p.4. "Regulation of Corporate Rules at **SoftServe**".

Access to secure areas requires authentication and authorized persons are issued with RFID Card. In order to identify an employee, who does not have a RFID Card, a guard, Development Center Director or any responsible person should be guided by the list of employees in SSExplorer (SSE) or procedure Access to IT premises.

The authentication system retains a record of accesses and these are reviewed on call of Head of Physical Security/ Development Center Director to identify any unauthorized accesses.

Third party support personnel only have access to secure areas when required and this access is specifically requested, authorized and monitored (Access to IT premises).

In general, the owner of a secure area and all those who are authorized to work within it, are required only to divulge details of the area and what is done in the area to other employees on a "need-to-know" basis.

Additional security means and the organization of security for the premises of **SoftServe** and its development centers are specified in "Office Security Policy and Procedures in Development Centers" document.

Access to **SoftServe Inc.** IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to 'Confidential', 'Restricted', 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to 'Public' information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
2. *Implementation specifications*:
    i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
    ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
    iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
    iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Comment: Commenters were concerned about having to address in their facility security plan the exterior/interior security of a building when they are one of many occupants rather than the sole occupant. Additional commenters were concerned that the responsibility for physical security of the building could not be delegated to a third party when the covered entity shares the building with other offices.

Response: The facility security plan is an addressable implementation specification. However, the covered entity retains responsibility for considering facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity's facility security plan, when appropriate.

Policy Number: 6.6
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Access Control and Validation Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to access control and validation, in accordance with the requirements at § 164.310(a)(1-2).
- ❑ Access control and validation procedures are designed to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.
- ❑ Strong access control and validation procedures are an essential element of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to implement and support strong and ongoing access control and validation procedures, in full compliance with all the requirements of HIPAA.
- ❑ It is the Policy of **SoftServe Inc.** to fully document access control and validation procedures, in accordance with our Documentation Policy.

Procedures

- ❑ Responsibility for developing, testing, analyzing, and periodically updating access control and validation procedures shall reside with <u>Name of Responsible Party or Person</u>.
- ❑ The development and implementation of specific access control and validation procedures shall be conducted in accordance with guidance and information provided by the National Institute of Standards and Technology ("NIST"), or other information technology "best practices".

Responsibility

- ❑ IS Manager is responsible for establishing access control standards.
- ❑ The VP IT is responsible for administration of allocated and authorized user or user group access rights in conformity with the policy.
- ❑ Linear Managers are responsible for authorizing access requests as being:

  - in line with business and organizational security policies and procedures
  - in conformity to the security requirements of the asset

Policy

SoftServe Inc. implements access control across its networks, IT systems and services. in order to provide authorized, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy. Access control systems are in place to protect the interests of all authorized users of **SoftServe** Inc. IT systems by providing a safe, secure and accessible environment in which to work. Provision of user access rights at **SoftServe** is conducted according to formal procedures.

Standard

Access to **SoftServe Inc**. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user’s **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to 'Confidential', 'Restricted', 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to 'Public' information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
2. *Implementation specifications*:
   i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
   ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
   iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
   iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Facility Access Controls (§ 164.310(a)(1))

We proposed, under the "Physical access controls" requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

In § 164.310(a)(2), we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.

SECTION 7

Policy Number: 7.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Encryption and Decryption Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
- ❑ The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

Procedures

When third-party transports are involved for transferring of information that require encryption according to ISMS DOC 8.8 InfoSec Classification Standard - **Transport level encryption**(e.g. VPN) must be employed. Third-party transports include electronic transmission outside company-owned physical communication lines (e.g. ISPs) and all data movement involving physical media transport processes (e.g. shipments, courier services, postal mail).

All web-based systems and web-services are required to use transport level encryption (SSL/TLS) between browser and web-based system and between consumers and providers of web-services.

On all systems storing information that require encryption according to ISMS DOC 8.8 InfoSec Classification Standard - **Storage encryption** must be used. Systems that are deemed as "high" risk of loss or theft, such as laptops, portable storage devices and personal communication devices must employ full device encryption.

For information that require encryption according to ISMS DOC 8.8 InfoSec Classification Standard and is stored on systems outside company data centers (e.g. employee workstations, laptops, etc.), in situation where Storage Encryption can't be employed - **Object-level encryption** must be used.

Disabling or defeating encryption is prohibited. No one may purposely disable encryption on a Production system without prior approval from the IS Manager. The use of proprietary encryption algorithms is not allowed for any purpose, unless it is reviewed by qualified experts outside of the vendor in question and approved by IS Manager.

Encryption should be used in compliance with all relevant agreements, laws, and regulations.

Standard

Encryption Algorithms

Approved encryption algorithms include:

- ❑ AES (FIPS 197)
- ❑ RSA (FIPS 186-2)

Symmetric cryptosystem key lengths must be at least 256 bits or 128 bits for PDA-like devices (AES-128) and for AES-XTS-128.Asymmetric cryptosystem keys must be of a length that yields equivalent strength.

Encryption protocols and standards

SoftServe information systems should rely on standard encryption protocols and standards

- ❑ File-level encryption: commercial grade encryption tools using approved encryption algorithms listed above
- ❑ Network connections encryption: IPsec, SSL v3 or TLS v1.0
- ❑ Email and IM messages encryption: S/MIME
- ❑ Digital certificates: X.509

All information assets are clearly identified, and an inventory of all-important assets has been drawn up and is maintained in line with the requirements of ISMS DOC 8.2 Asset Inventory & Ownership. The owners review the classifications of information assets annually and if the classification level can be reduced, it will be. The asset owner also is responsible for declassifying information.

Information received from outside the Organization is re-classified by its recipient so that (within the Organization), it complies with this procedure. Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it should be destroyed.

SoftServe's information assets are classified accordingly to five levels of classification (top secret, secret, confidential, internal and public):

Top Secret: this classification applies to information that is specifically restricted by the Board of Directors. Top Secret information may include trade secrets, it may include sales and marketing plans, new product plans, and notes associated with patentable inventions.

- ❑ Information with Top Secret level is available and/or should be distributed only to defined list of people within organization who has been given a top secret security clearance (according to procedure described in section 3.2 in Personnel Screening Standard) and require exceptional security controls.
- ❑ Such information would cause "exceptionally grave damage" to organization in case of disclosure.
- ❑ Top Secret information sent by e-mail must be encrypted and digitally signed, in line with the ISMS DOC 10.1 Encryption Policy, and sent only to the e-mail box of the identified recipient.

❑ Access provisioning requires "need-to-know" basis.

Disclosure, destruction or loss of integrity of such information lead to **Very High** impact level (section 3.6 of Risk Management Framework).

Secret: this classification applies to information that is specifically restricted by EVP.

❑ Such information may include some types of private information, including records of a person's health care, education, and employment may be protected by privacy laws, a person's or organization's financial information that may be considered private if their disclosure might lead to crimes such as identity theft or fraud.
❑ Unauthorized disclosure of private information that can make the perpetrator liable for civil remedies and may in some cases be subject to criminal penalties.
❑ Secret information would cause "serious damage" to organization in case of disclosure.
❑ Secret information sent by e-mail must be encrypted and digitally signed, in line with the ISMS DOC 10.1 Encryption Policy, and sent only to the e-mail box of the identified recipient.
❑ Access provisioning requires "need-to-know" basis.

"Secret" information disclosure, destruction or loss of integrity could cause **High** impact level (section 3.6 of Risk Management Framework).

Confidential: this classification applies to information that is specifically restricted by SBU Manager.

❑ Information that falls into this category must be marked 'Confidential' includes business information or personal data collected by the organization that is subject to special protection and may not be routinely shared with anyone inside or outside of the business.
❑ Confidential material would cause "damage" or be "prejudicial" to organization in case of disclosure.
❑ Access provisioning requires "need-to-know" basis.

Disclosure, destruction or loss of integrity of "Confidential" information could cause **Medium** impact (section 3.6 of Risk Management Framework)**.**

Internal: information of this category is restricted for authorized employees/staff.

- ❑ Internal material would cause "undesirable effects" to organization in case of disclosure.
- ❑ Internal information includes business information that is not subjected to special protection and may be routinely shared with anyone inside the business.

Disclosure, destruction or loss of integrity of information classified as "Internal" could cause **Low** or **Very Low** impact (section 3.6 of Risk Management Framework).

Public: this is information which can be released outside the organization.

- ❑ This refers to information that is already or could be a matter of public record or knowledge. Those without security clearance can view such documents.

Disclosure, destruction or loss of integrity of such kind of information could not cause impact on business.

Labeling

Proper labeling enables all parties to correlate the information with appropriate information handling guidelines. The key of effective labeling is ensuring that a person with access to information is aware of its classification and what restrictions exist in the release or handling of the information.

Electronic information might be stored in Systems and Objects. Electronic information should be labeled in object(s) level. In case it is impossible the whole system should be classified.

Systems include but not limited to: 1C, SSE, SSP, TM, Head Accounter, HRMS (TMS, LMS, WMS, CMS, BMC, CRM, DB's, etc.

Objects include but not limited to: Microsoft Office documents (Word, Excel, etc.), Confluence page, E-mail, etc.

Stored information, both physical and electronic, must be labeled in accordance with Classification above. All the information with no labels is deemed Confidential.

System is deemed classified according to the highest classification of information stored. Warning screens are used during log in into systems.

Predefined templates (ISMS DOC 8.8.1 Templates for classified information) shall be employed.

If predefined templates are not used:

- ❑ The classification level should be included to all pages of the document
- ❑ Label font size should be larger than plain text and be highlighted with colored label title: Dark Red for Top Secret, Red for Secret, Yellow for Internal, Green for Public (where possible)
- ❑ Hardcopy documents that do not have text labels are marked by addition of a physical, stick-on label or marked with either rubber stamps or markers of appropriate content and color (where possible).
- ❑ Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) should be labeled with appropriate classification level mark.

Information is downgraded or upgraded after approve of appropriate Information Asset Owner based on Risk Acceptance Procedure. VP Marketing must also approve all information downgraded to level of classification Public. Classified information that is downgraded or upgraded should be promptly marked to indicate the change with date and signature (hard copy) or electronic message (system, object).

Handling

The Organization’s information assets should be handled in a manner to protect the information assets from unauthorized or accidental disclosure, modification or loss. All information assets should be processed and stored in accordance with information assets classification levels assigned in order to protect the confidentiality, integrity and availability.

- ❑ Information assets can only be handled by individuals that have appropriate authorization or on facilities that shall not be visible to the public when not in use to prevent disclosure and theft, for example leaving a laptop with confidential data visible in a vehicle.

- ❑ Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls specified in ISMS DOC 11.10 Equipment Security Standard, and are protected appropriately while being recorded.
- ❑ Agreements with external organizations (see ISMS DOC 15.1 Supplier Relationship Policy) which include information sharing include a matrix for translating their security classifications into classifications applicable to **SoftServe**.
- ❑ Creator of information ensures that appropriate measures are taken to classified information accordingly to requirements of ISMS DOC 13.3 Information Transfer Policy, ISMS DOC 8.7 Removable media, ISMS DOC 8.10 Information Storage, Disposal and Retention Policy, ISMS DOC 11.19 Clear Screen and Clear Desk Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
2. *Implementation specifications*:
   i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
   ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
   iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
   iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Transmission Security (§ 164.312(e)(1))

Under "Technical Security Mechanisms to Guard against Unauthorized Access to Data that is Transmitted over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Comment: We received comments asking that encryption be deleted as an implementation feature and stating that encryption is not required for "data at rest."

Response: The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule.

Transmission Security (§ 164.312(e)(1))

Comment: We received a number of comments asking for overall clarification as well as a definition of terms used in this section. A definition for the term "open networks" was the most requested action, but there was a general expression of dislike for the manner in which we approached this section, with some comments suggesting that the entire section be rewritten. A significant number of comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet, but rather be considered optional based on individual entity risk assessment/analysis. Many comments noted that there are very few known breaches of security over dial-up lines and that non-judicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Only one commenter suggested that "most" external traffic should be encrypted.

Response: In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines.

We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) the alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for "Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) "integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

Comment: A number of comments were received asking that this final rule establish a specific (or at least a minimum) cryptographic algorithm strength. Others recommended that the rule not specify an encryption strength since technology is changing so rapidly. Several commenters requested guidelines and minimum encryption standards for the Internet. Another stated that, since an example was included (small or rural providers for example), the government should feel free to name a specific encryption package. One commenter stated that the requirement for encryption on the Internet should reference the "CMS Internet Security Policy."

Response: We remain committed to the principle of technology neutrality and agree with the comment that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Consistent with this principle, specification of an algorithm strength or specific products would be inappropriate. Moreover, rapid advances in the success of "brute force" cryptanalysis techniques suggest that any minimum specification would soon be outmoded. We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength. Because

"CMS Internet Security Policy" is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities, we have not referred to it here.

Breach Notification Only Applies to "Unsecured" PHI

Breach Notification only applies to Protected Health Information (PHI) that has not been "secured" (encrypted) according to HHS and NIST standards.

PHI that has been secured by these standards, and is subsequently breached, *does not invoke any Breach Notification requirements*.

<u>The current encryption Standard referenced in the Final Rule is</u>: "*Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*".
(74 Federal Register, Pages 42,740-42,742)

<u>This Breach Notification exception *does not apply* to paper, film, and other hardcopy PHI, because these materials cannot be electronically encrypted (protected) in their native forms</u>.

Policy Number: 7.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Unique User I.D. Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of unique user I.D.'s, in accordance with the requirements at § 164.306, and § 164.312(a)(1).
- ❑ The use of unique user I.D.'s is an essential element in our overall effort to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to exclusively use unique user I.D.'s for all information system access and activities, in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.'s.
- ❑ Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy.

Procedures

General

To ensure secure access to **SoftServe's** Information Systems all company's passwords should met minimal requirements:

- ❑ All passwords, including initial passwords, must be constructed and implemented according to Strong Passwords Standards defined below.
- ❑ All passwords are to be treated as sensitive, Confidential **SoftServe** information. User account passwords must not be divulged to anyone.
- ❑ Whenever there is any indication of its possible password compromise, the password must be changed immediately with appropriate notification sent to IS Department.
- ❑ Administrators must not circumvent the *Password Policy* for the sake of ease of use.
- ❑ Privileged user accounts must have password different from all other passwords for accounts held by this user.
- ❑ All passwords for production servers and network equipment administrative access must be changed at least annually.
- ❑ Only IT Department approved single sign-on applications may be used for simplifying password entry and auto logon into applications. Such application must comply with *Encryption Policy* for storing password information.
- ❑ Passwords must not be stored in any form outside single sign-on application, except for password escrow needs.

- IT Department is responsible for password escrow and must provide adequate level of protection to escrow data including, but not limited to, strong encryption and isolation of escrow storage device.
- Unencrypted passwords must not be transmitted via email messages or other forms of communication.
- Security tokens (i.e. Smartcard) used for multi-factor authentication must be returned on demand or upon termination of the relationship with **SoftServe**.
- Monitoring of networked devices via SNMP protocol should use strongest available authentication mechanism. If plain SNMP v1 community strings have to be used, they must be defined as something else than the standard defaults, such as "public," "private", and "system", and must be different from the passwords used to log in interactively
- Computing devices must not be left unattended without locking console or logging off of the device.
- IT Department password change procedures must include the following:
    - authenticate the user to the IT Department before changing password
    - strong password must be generated
    - the user must change password at first login, whenever possible this policy must be enforced by appropriate authentication mechanisms
- Password cracking or guessing may be performed on a periodic or random basis by IS Department or its delegates. If the password is guessed or cracked during one of these scans, the user will be required to change it.
- The same password shall not be used for business and non-business purposes
- User should avoid keeping a record (e.g. on paper, software file or hand-held device) of password, unless this can be stored securely and the method of storing has been approved (e.g. password vault)

As different **SoftServe** clients provide different requirements for Information Security, additional stricter rules for passwords are provided per each SBU. (Section 2.3)

Companywide Passwords Standards

Workstation Passwords should meet following criteria:

1. Contain both upper and lower case characters (e.g., a-z, A-Z).
2. Have digits and punctuation characters as well as letters (e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
3. Be at least eight alphanumeric characters long (e.g., Ohmy1stubbedmyt0e%).
4. Do not form single word in any language, slang, dialect, jargon, etc.

5. Should not be based on personal information, names of families, or other information which can be easily derived from publicly know information about particular user.

PDA-like Devices Passwords should meet following criteria:

1. Be at least 5 digits long (or longer) and consist of numeric or alphabetical characters.

Passwords Standards per SBU

Infrastructure D

1. User IDs that have been inactive for thirty (30) days must be disabled;
2. User IDs that remain inactive for sixty (60) days must be deleted or blocked;
3. For any password issued by client to company employee, he must immediately change the password upon initial logging into any client's network;
4. Company shall inform client immediately when any Personnel has left company, or otherwise no longer requires access to the client's network.

Healthcare B

1. Passwords should be changed at least every ninety (90) days;
2. The minimum password length for privileged user IDs is twelve (12) characters and sixteen (16) characters for service accounts;
3. Passwords associated with privileged user ids (such as those with administrator/root access privileges) and service accounts (used for machine-to-machine communications with no humans involved in providing the authentication at time of log in or job submission) must expire within three hundred sixty-five (365) days.

Corporate Application Standards

Corporate application deployment should be performed observing following requirements:

- ❑ Applications should support authentication of individual users, but not groups.
- ❑ Applications should support role-based authorization, having security privileges and access rights defined per role, not particular user record.
- ❑ Applications should support Microsoft Active Directory, TACACS+, RADIUS, and/or X.509 with LDAP security retrieve for integration into corporate AAA (Authentication, Authorization and Accounting) service.
- ❑ Applications should support group-based authorization using groups defined in corporate directory services accessed via native Microsoft Active Directory integration or TACACS+, RADIUS or LDAP protocols.
- ❑ Applications should not store passwords in clear text or in any easily reversible form.
- ❑ Applications should provide for some sort of role management, in such a way that one user can take over the functions of another, without having to know the others password.
- ❑ Applications should use secure channel for transferring authentication information through the network. Clear text authentication mechanisms are not allowed in corporate applications.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.

1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
2. *Implementation specifications*:
    - i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
    - ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
    - iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
    - iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

Integrity (§ 164.312(c)(1))

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone call back," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Person or Entity Authentication (§ 164.312(d))

Comment: We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

Response: We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1). "Automatic logoff" has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

Policy Number: 7.2
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Password Management Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to password management, in accordance with the requirements at § 164.308(a)(5).
- ❑ The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.
- ❑ The monitoring of successful and unsuccessful Log-In attempts is a well-established method of detecting malicious intrusions, and intrusion attempts, into information systems by unauthorized persons.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to require the use of strong passwords and pass-phrases by all workforce members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information.
- ❑ The responsibility for implementing this policy and any attendant procedures is hereby assigned to the designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), who shall develop and implement this policy in coordination with the most senior information technology personnel.

Procedures

- ❑ All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of six (6) characters in length, and must or should (select one) include non-alphanumeric characters or symbols in them.
- ❑ Passwords and pass-phrases must or should be changed by users or management (select one) at least every three (3) six (6) (chose one or an alternate timeframe) months.
- ❑ In the event of an information system compromise, as determined by the designated HIPAA Official or HIPAA Officer, some or all workforce-member passwords and pass-phrases may need to be changed. This determination shall be made by the designated HIPAA Official or HIPAA Officer (or insert alternate contact).
- ❑ Under no circumstances shall passwords or pass-phrases be written down and kept at or near computers and workstations where they may be found by others. Passwords and pass-phrases may, however, be written down and stored in a workforce member's wallet or purse, if the password or pass-phrase is thus afforded protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.
- ❑ Any workforce member who loses, misplaces, forgets, or experiences any compromise of their password or pass-phrase shall immediately notify the designated HIPAA Official or HIPAA Officer, or, if they are unavailable, shall notify (specify alternate notification contact). Such notification of password or pass-phrase compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one (1) (Choose or select alternate number) hour(s).
- ❑ Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by this organization.

General

To ensure secure access to **SoftServe's** Information Systems all company's passwords should met minimal requirements:

- ❑ All passwords, including initial passwords, must be constructed and implemented according to Strong Passwords Standards defined below.
- ❑ All passwords are to be treated as sensitive, Confidential **SoftServe** information. User account passwords must not be divulged to anyone.
- ❑ Whenever there is any indication of its possible password compromise, the password must be changed immediately with appropriate notification sent to IS Department.
- ❑ Administrators must not circumvent the *Password Policy* for the sake of ease of use.
- ❑ Privileged user accounts must have password different from all other passwords for accounts held by this user.

- ❑ All passwords for production servers and network equipment administrative access must be changed at least annually.
- ❑ Only IT Department approved single sign-on applications may be used for simplifying password entry and auto logon into applications. Such application must comply with *Encryption Policy* for storing password information.
- ❑ Passwords must not be stored in any form outside single sign-on application, except for password escrow needs.
- ❑ IT Department is responsible for password escrow and must provide adequate level of protection to escrow data including, but not limited to, strong encryption and isolation of escrow storage device.
- ❑ Unencrypted passwords must not be transmitted via email messages or other forms of communication.
- ❑ Security tokens (i.e. Smartcard) used for multi-factor authentication must be returned on demand or upon termination of the relationship with **SoftServe**.
- ❑ Monitoring of networked devices via SNMP protocol should use strongest available authentication mechanism. If plain SNMP v1 community strings have to be used, they must be defined as something else than the standard defaults, such as "public," "private", and "system", and must be different from the passwords used to log in interactively
- ❑ Computing devices must not be left unattended without locking console or logging off of the device.
- ❑ IT Department password change procedures must include the following:
  - authenticate the user to the IT Department before changing password
  - strong password must be generated
  - the user must change password at first login, whenever possible this policy must be enforced by appropriate authentication mechanisms
- ❑ Password cracking or guessing may be performed on a periodic or random basis by IS Department or its delegates. If the password is guessed or cracked during one of these scans, the user will be required to change it.
- ❑ The same password shall not be used for business and non-business purposes
- ❑ User should avoid keeping a record (e.g. on paper, software file or hand-held device) of password, unless this can be stored securely and the method of storing has been approved (e.g. password vault)

As different **SoftServe** clients provide different requirements for Information Security, additional stricter rules for passwords are provided per each SBU. (Section 2.3)

Companywide Passwords Standards

Workstation Passwords should meet following criteria:

1. Contain both upper and lower case characters (e.g., a-z, A-Z).
2. Have digits and punctuation characters as well as letters (e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
3. Be at least eight alphanumeric characters long (e.g., Ohmy1stubbedmyt0e%).
4. Do not form single word in any language, slang, dialect, jargon, etc.
5. Should not be based on personal information, names of families, or other information which can be easily derived from publicly know information about particular user.

PDA-like Devices Passwords should meet following criteria:

1. Be at least 5 digits long (or longer) and consist of numeric or alphabetical characters.

Passwords Standards per SBU

Infrastructure D

1. User IDs that have been inactive for thirty (30) days must be disabled;
2. User IDs that remain inactive for sixty (60) days must be deleted or blocked;
3. For any password issued by client to company employee, he must immediately change the password upon initial logging into any client's network;
4. Company shall inform client immediately when any Personnel has left company, or otherwise no longer requires access to the client's network.

Healthcare B

1. Passwords should be changed at least every ninety (90) days;
2. The minimum password length for privileged user IDs is twelve (12) characters and sixteen (16) characters for service accounts;
3. Passwords associated with privileged user ids (such as those with administrator/root access privileges) and service accounts (used for machine-to-machine communications with no humans involved in providing the authentication at time of log in or job submission) must expire within three hundred sixty-five (365) days.

Corporate Application Standards

Corporate application deployment should be performed observing following requirements:

- ❑ Applications should support authentication of individual users, but not groups.
- ❑ Applications should support role-based authorization, having security privileges and access rights defined per role, not particular user record.
- ❑ Applications should support Microsoft Active Directory, TACACS+, RADIUS, and/or X.509 with LDAP security retrieve for integration into corporate AAA (Authentication, Authorization and Accounting) service.
- ❑ Applications should support group-based authorization using groups defined in corporate directory services accessed via native Microsoft Active Directory integration or TACACS+, RADIUS or LDAP protocols.
- ❑ Applications should not store passwords in clear text or in any easily reversible form.
- ❑ Applications should provide for some sort of role management, in such a way that one user can take over the functions of another, without having to know the others password.
- ❑ Applications should use secure channel for transferring authentication information through the network. Clear text authentication mechanisms are not allowed in corporate applications.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

A covered entity or business associate must, in accordance with § 164.306:

- ❑ Standard*: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
- ❑ Implementation *specifications*. Implement:
  - *Security reminders* (Addressable). Periodic security updates.
  - *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
  - *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
  - *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords**.**

Security Awareness and Training (§ 164.308(a)(5))

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

Policy Number: 7.3
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Person or Entity Authentication Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).
- ❑ The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information (“PHI” and “ePHI”, as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.

- ❑ The establishment and implementation of an effective Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper authentication of persons and entities who request access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations and systems.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Access to **SoftServe Inc**. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer's approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to 'Confidential', 'Restricted', 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to 'Public' information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
   2. *Implementation specifications*:
      - i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
      - ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
      - iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
      - iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

b. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

c.
   1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
   2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

d. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

Integrity (§ 164.312(c)(1))

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone call back," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Integrity (§ 164.312(c)(1))

Comment: We received a large number of comments requesting clarification of the "Data authentication" requirement. Many of these comments suggested that the requirement be called "Data integrity" instead of "Data authentication." Others asked for guidance regarding just what "data" must be authenticated. A significant number of commenters indicated that this requirement would put an extraordinary burden on large segments of the health care industry, particularly when legacy systems are in use. Requests were received to make this an "optional" requirement, based on an entity's risk assessment and analysis.

Response: We adopt the suggested "integrity" terminology because it more clearly describes the intent of the standard. We retain the meaning of the term "Data authentication" under the addressable implementation specification "Mechanism to authenticate data," and provide an example of a potential means to achieve data integrity. Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms that are ubiquitous in hardware and operating systems today. The risk analysis process will address what data must be authenticated and should provide answers appropriate to the different situations faced by the various health care entities implementing this regulation. Further, we believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task.

Comment: We received numerous comments suggesting that "Double keying" be deleted as a viable "Data authentication" mechanism, since this practice was generally associated with the use of punched cards.

Response: We agree that the process of "Double keying" is outdated. This final rule omits any reference to "Double keying."

Person or Entity Authentication (§ 164.312(d))

Comment: We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

Response: We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1). "Automatic logoff" has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) the alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for "Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) "integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

SECTION 8

Policy Number: 8.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Policy on Security Incident Procedures

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- ❑ Appropriate responses to security incidents may include, but are not limited to:
  - Rapid identification and classification of the severity of security incidents.
  - Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
  - Repairing, patching, or otherwise correcting the condition or error that created the security incident.
  - Retrieving or limiting the dissemination of individually identifiable health information, if possible.
  - Making an *immediate* report of a breach, if required, to the affected Covered Entity who supplied the information to us.
  - Mitigating any harmful effects of the security incident.
  - Fully documenting security incidents, along with their causes and our responses.
  - Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
- ❑ Compliance with HIPAA's data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- ❑ Responsibility for responding to and managing security incidents shall reside with the designated HIPAA Official or HIPAA Officer.

- ❑ The designated HIPAA Official or HIPAA Officer shall develop specific forms and procedures that shall be implemented in response to security incidents.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

Procedures

Standard

The Information Security Department logs all information security events and incidents immediately upon receipt. Incident Management System allocates to each incident a unique number and uses this ensure that all incidents are analyzed and closed out. All steps, which are performed during incident response process, shall be saved in appropriate report with RMS (Rights Management System) restricted access.

Restrictions:

- ❑ Stakeholders - Read
- ❑ CISO - Full Control
- ❑ Information Security Manager - Full Control
- ❑ SecOps Team Members - Change

All information security events and weaknesses that are categorized as a IS Incident, immediately upon receipt, assessed and categorized by the Information Security Department.

Initially, there are four categories:

- ❑ Events- are occurrences that, after analysis, have no or very minor importance for information security;
- ❑ Vulnerabilities - are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security;
- ❑ Incidents - are occurrences of events (series of events) that have a significant probability of compromising the organization's information security;
- ❑ Unknowns - are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the three categories.

Incident priority determines response to an incident and is based on impact and urgency. It is a category used to identify the relative importance of the incident and helps determine the timeframe within which action is required.

Impact is a measure of the effect of the incident on business and how service levels will be affected:

- ❑ **Significant/Large/Business**
- ❑ **Moderate/Limited/Project**
- ❑ **Minor/Localized/Employee**

In case of incident with High impact IS Audit Director shall be notified and added as a watcher to the SDE Ticket.

Urgency is a measure of how long it will take until the incident has a significant impact on the business. Urgency may be dependent on time of day, day of the month and certain business activities:

1. **High**
2. **Medium**
3. **Low**

Sample priorities are provided below; some tools have algorithms for computing priority based on impact and urgency:

1. **High** – need immediate and sustained effort by all available resources to resolve (users cannot perform business functions).
2. **Medium** – immediate response by primary support personnel; may require additional personnel to reschedule low or medium priority efforts (users can perform business functions but efficiency is impacted).
3. **Low** – respond using normal procedures (this should be fixed but it can wait).

Priority may be dynamic – the priority may be changed over the lifetime of an incident if the situation changes. Service or Operating Level Agreements with particular parties may include specifics for incident priority.

The 'unknowns' are subject to further analysis to allocate them to one of the other three categories as soon as possible.

The prioritization for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events.

When there are multiple event reports in each category, the Information Security Manager prioritizes the responses and information assets at risk, the danger of further compromise to the organization's information security, and the resources at his/her disposal.

Incidents involving high-value or business critical systems are immediately reported by the Information Security Manager to the Chief Information Security Officer (CISO).

The Information Security Manager seeks additional input from qualified technical staff, as necessary and where he considers the standing instructions to be inadequate, to analyze and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.

The Information Security Manager invokes actions as set out in the standing work instructions plus additional activity that he considers necessary to contain and recover from the incident, and to implement contingency plans. Where necessary, the Information Security Manager coordinates activity with other organizations. The Information Security Manager confirms that the affected business systems have been restored and that the required controls are operational before authorizing a return to normal working.

Once the incident is contained, and the required corrective action is completed, the Information Security Manager reports to the Chief Information Security Officer (CISO) with a summary of the incident, identifying the cause of the incident and analyzing its progress, trying to identify how the organization could have responded earlier or more effectively, or preventive action that might have been taken in advance of the information, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out (see 3.9 below).

The Information Security Manager is responsible for closing out the incident:

- ❑ This includes any reports to external authorities;
- ❑ Initiating disciplinary action by referring the incident to the VP HR;
- ❑ Planning and implementing preventative action to avoid any further recurrence;

- ❑ Collecting and securing audit trails and forensic evidence;
- ❑ Initiating any action for compensation from software, service or outsource suppliers by referring the incident to the Legal department, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.

The Information Security Manager prepares a quarterly report to the Information Security Committee which identifies the number, type, category and severity of information security incidents during the preceding month, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security incidents, improve the organization's ability to respond, and reduce the cost of response.

All the incident reports from the period since the last management review are taken into account at the next one, to ensure that the organization learns from the incidents.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:

6.) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

Security Incident Procedures (§ 164.308(a)(6))

We proposed a requirement for implementation of accurate and current **security incident procedures**: formal, documented report and response procedures so that security violations would be reported and handled promptly. We adopt this standard in the final rule, along with an implementation specification for response and reporting, since documenting and reporting incidents, as well as responding to incidents are an integral part of a security program.

Security Incident Procedures (§ 164.308(a)(6))

Comment: Several commenters asked that we further define the scope of a breach of security. Along this same line, another commenter stated that the proposed security incident procedures were too vague as stated. We were asked to specify what a security incident would be, what the internal chain for reporting procedures would be, and what should be included in the documentation (for example, hardware/software, personnel responses).

Response: We define a security incident in § 164.304. Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

Comment: One commenter asked what types of incidents must be reported to outside entities. Another commented that we clarify that incident reporting is internal.

Response: Internal reporting is an inherent part of security incident procedures. This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations.

Comment: One commenter stated that network activity should be included here.

Response: We see no reason to exclude network activity under this requirement. Improper network activity should be treated as a security incident, because, by definition, it represents an improper instance of access to or use of information.

Comment: One commenter stated that this requirement should address suspected misuse also.

Response: We agree that security incidents include misuse of data; therefore, this requirement is addressed.

Comment: Several commenters asked that this requirement be deleted. One commenter asked that we delete the implementation features.

Response: As indicated above, we have adopted the proposed standard and combined the implementation specifications.

Policy Number: 8.1
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Information Systems Activity Review Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to information systems activity review, in accordance with the requirements at § 164.308(a)(1).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- ❑ The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all information system activity review activities and efforts.
- ❑ This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Procedures

The following must be presented to the management review meeting, as input for the review:

Any formal feedback on the ISMS from interested parties including, but not limited to, the certification body, external parties such as outsourcing suppliers and customers, and special interest groups (ISMS DOC 6.6 Contact with Authorities).

Results and analysis of internal and external ISMS audits and independent reviews (ISMS DOC 18.8 Internal Independent Review , Section 1 Internal Audit).

- ❑ Any documentation relating to preventive and corrective actions carried out (or under way), or vulnerabilities or threats not adequately addressed in previous risk assessments, including the status of those actions.
- ❑ Results from effectiveness measurements.
- ❑ The minutes of previous management reviews, together with information about implementation of decisions and actions.
- ❑ Identified weaknesses or inadequacies in process performance and information about compliance with the Information Security Policy.
- ❑ Information about changes in the organization's environment, the business circumstances, resource availability, contractual regulatory and legal circumstances, or in the technical environment, that might create new risks, or a change in already assessed risks, and have an impact on the organization's information security management.
- ❑ Details of trends related to threats and vulnerabilities and that relate to the organization.
- ❑ Significant information security incidents, recorded in line with ISMS DOC 16.2 Security Incident Reporting Procedure.
- ❑ Approaches that could be used to improve the ISMS.

The management review should focus on:

- ❑ Improving the organization's assessment of the risks to information security and its PDCA approach, including updating the risk assessment and risk treatment plan.
- ❑ Modifying or improving the policies and procedures for managing information security, including improvements to how effectiveness is measured.
- ❑ Modifying or improving its control objectives and controls to ensure that they are adequately focused on the identified risks, and respond to internal and external risks that may impact the ISMS, including changes to contractual obligations.
- ❑ Improving the allocation of resources and responsibilities (ISMS DOC 6.2 Information Security Coordination).
- ❑ Formulating and agreeing any changes to the Information Security Policy which would be necessary to give effect to any improvements identified.

The CISO is responsible for ensuring that the meeting is recorded and required actions identified for follow up.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
    1.
        i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
        ii. *Implementation specifications*:
            A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
            B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
            C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
            D. *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Policy Number: 8.2
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Malware Protection Policy

Assumptions

❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
❑ The use of appropriate techniques, technologies, and methods to protect information systems from malicious software (“malware”) is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
- ❑ Responsibility for malware protection shall reside with the designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from malicious software.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all malware protection-related activities and efforts, in accordance with our Documentation Policy.

Procedures

The **SoftServe** organization acts to protect the integrity of its software and its other information assets against the introduction of malicious code (malware).

The **SoftServe** formally prohibits the use, on any information processing system or device it owns or operates, of any software whose procurement was not carried out through the organization’s procurement procedure. Software that has been obtained and any other files or folders, may not be transferred or downloaded onto the organization’s network via or from external networks, or on any medium (including CD-ROMs, USB sticks), including during maintenance and emergency procedures, unless specific controls have been implemented as detailed in ISMS DOC 12.4 Malware Protection Standard.

The organization formally prohibits the use of mobile code that has not be verified by IS Department.

Monitoring, detecting and deleting unauthorized software is a requirement of the information system, and disciplinary action is to be taken against anyone in breach of the anti-malware policy.

The **SoftServe** acts to identify and patch software and system vulnerabilities in order to reduce the risk of malware attacks. The installation and maintenance of anti-malware software on all organizational information systems and devices is mandatory.

All users are required to accept, in terms of their User Agreements, the Workplace Software Use Policy (ISMS DOC 8.6 User Workplace Software Use Policy), the Internet Acceptable Use Policy (ISMS DOC 8.3 Acceptable Use Policy) and the e-mail rules (ISMS DOC 8.4 E-Mail

Standard) and to receive appropriate training in detecting and responding to malware attacks, and to accept specific anti-malware prevention controls in their User Agreements.

Business continuity plans (Section 17 Information Security Aspects of Business Continuity Management) are required to make specific provision for recovering from malware attacks.

The Information Security Incident Management procedure (see Section 16 Information Security Operations) is required to make specific provision for responding to malware attacks.

Management is required to take adequate steps to ensure that it is aware of and can respond to changes in the malware threat environment.

Requirements

- ❑ All **SoftServe** workstations and servers must use the **SoftServe** IS department approved virus protection software.
- ❑ All workstations have to run anti-virus and anti-malware software installed and configured to perform real-time scanning of accessed files and applications/process running on the system.
- ❑ Real-time anti-virus/anti-malware scanning has to be configured on servers, if they meet one or more of the following conditions:
  - non-IT Department employees have remote access capability;
  - the system is a file server;
  - Microsoft Share access is open to this server from systems used by non-administrative users;
  - HTTP/FTP access is open from the Internet;
  - other "risky" protocols/applications are available to this system from the Internet at the discretion of the **SoftServe** Chief Informational Security Officer (CISO);
  - Outbound Web access is available from the system.
- ❑ The virus protection software must not be disabled or bypassed.
- ❑ The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- ❑ The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- ❑ Mail servers must have either an external or internal anti-virus scanning application that scans all mail leaving or entering the mail system.
- ❑ Administrator may disable real-time file access anti-virus scanners while performing backups, if an external anti-virus application still scans inbound emails while the backup is being performed.

- ❑ Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the **SoftServe** Incident Management System (http://sde.softserveinc.com/helpdesk/newlogin.asp) as high priority incident.
- ❑ Virus-infected computers must be confined or removed from the network until they are verified as virus-free.
- ❑ Any activities with the intention to create and/or distribute malicious programs (malware) inside **SoftServe** networks (e.g., viruses, worms, Trojan horses, e-mail bombs) are prohibited in accordance with the ISMS DOC 8.3 Acceptable Use Policy.

User training

[ISO27002 Clause 8.2.2 (Clause 7.2.2 - ISO 27001:2013)]

All employees of the organization shall receive appropriate awareness training (ISMS DOC 7.5 Information Security Training and Awareness Policy) in respect of malware response.

User training on malware responses includes:

- ❑ The principles and requirements of the anti-malware policy.
- ❑ The requirements of the Acceptable Use Policy (ISMS DOC 8.3 Acceptable Use Policy).
- ❑ Identifying and responding to ‘hoax’ virus warnings, reporting them to the Information Security Director and not passing them on.
- ❑ Restriction for opening attachments to e-mails that are unexpected or where the sender is unknown.
- ❑ Response procedure in case a virus does successfully install itself on their workstation or laptop.
- ❑ Protective steps, that is necessary in respect of portable memory media.
- ❑ Responding to screen and system alerts regarding viruses, spam, and mobile code.
- ❑ Restriction for accepting any file or folder execution requests while on the Internet

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

A covered entity or business associate must, in accordance with § 164.306:

- ❑ Standard*: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
- ❑ Implementation *specifications*. Implement:

- *Security reminders* (Addressable). Periodic security updates.
- *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
- *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
- *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

Security Awareness and Training (§ 164.308(a)(5))

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. **The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.**

Policy Number: 8.3
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Log-In Monitoring Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
- ❑ Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish a program of regular monitoring and review of log-ins and log-in attempts.
- ❑ The designated HIPAA Official or HIPAA Officer, shall assume responsibility for log-in monitoring and analysis, and for ensuring that such activities are executed on a continuous basis.
- ❑ Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Secure Logon

[ISO27002 Clause 11.5.1 | ISO 27001:2013 Clauses 9.4.2]

- ❑ Where possible, no password hinting should be provided during the logon procedure.
- ❑ The system logging failure message should not specify which of user credentials were incorrect.
- ❑ The logon procedure limits the number of unsuccessful attempts allowed to five.
- ❑ Password characters are hidden by symbols and always encrypted before being sent across the network.

Session time-out

- ❑ Users are required to log out of sessions when they are finished.
- ❑ Inactive sessions must be shut down automatically when they have been inactive for a period of:
  - o 15 minutes for PC and laptop;
  - o 3 minutes for PDA-like devices.
- ❑ Exceptions might be for systems that are used in secured or isolated environments and approved by IS Manager.

Sensitive system isolation

[ISO27002 Clause 11.6.2 | ISO 27001:2013 Clauses 14.2.6]

- ❑ The system(s), which require an isolated environment, and their physical, secure areas.
- ❑ Isolation for these systems is achieved by:
  - Network equipment;
  - Physical (separate rooms);
  - Insulation permissions.

HHS Regulations as Amended January 2013

Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

A covered entity or business associate must, in accordance with § 164.306:

- ❑ Standard*: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
- ❑ Implementation *specifications*. Implement:
  - *Security reminders* (Addressable). Periodic security updates.
  - *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
  - *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
  - *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

Last Revised: 7/29/2014

Automatic Log-Off Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of automatic log-off applications, in accordance with the requirements at § 164.306 and § 164.312(a)(1-2).
- ❑ The establishment and implementation of an effective automatic log-off policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to always use automatic log-off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with the InO Director, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document automatic log-off-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Secure Logon

[ISO27002 Clause 11.5.1 | ISO 27001:2013 Clauses 9.4.2]

- ❑ Where possible, no password hinting should be provided during the logon procedure.
- ❑ The system logging failure message should not specify which of user credentials were incorrect.
- ❑ The logon procedure limits the number of unsuccessful attempts allowed to five.
- ❑ Password characters are hidden by symbols and always encrypted before being sent across the network.

Session time-out

- ❑ Users are required to log out of sessions when they are finished.
- ❑ Inactive sessions must be shut down automatically when they have been inactive for a period of:
  - o 15 minutes for PC and laptop;
  - o 3 minutes for PDA-like devices.
- ❑ Exceptions might be for systems that are used in secured or isolated environments and approved by IS Manager.

Sensitive system isolation

[ISO27002 Clause 11.6.2 | ISO 27001:2013 Clauses 14.2.6]

- ❑ The system(s) which require an isolated environment, and their physical secure areas.
- ❑ Isolation for these systems is achieved by:
  - Network equipment;
  - Physical (separate rooms);
  - Insulation permissions.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
2. *Implementation specifications*:
   i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

Integrity (§ 164.312(c)(1))

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone call back," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Comment: A large number of comments were received objecting to the identification of "Automatic logoff" as a mandatory implementation feature. Generally the comments asked that we not be so specific and allow other forms of inactivity lockout, and that this type of feature be made optional, based more on the particular configuration in use and a risk assessment/analysis.

Response: We agree with the comments that mandating an automatic logoff is too specific. This final rule has been written to clarify that the proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification and also permits the use of an equivalent measure.

Comment: We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

Response: We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1). "Automatic logoff" has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

Policy Number: 8.5
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Workstation Security Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- ❑ The establishment and implementation of an effective workstation security policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and maintain this workstation security policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, shall reside with IS Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), to restrict access to authorized users only.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Access to **SoftServe** Inc. IT resources and services is given through the provision of a unique user account and complex password.

By default employees have access to a standard suite of services (email, file server, internet and SharePoint) and software applications (shared to employee's department), the remote desktop and VPN services (RD and VPN are in line with ISMS DOC 13.1 Network Control Policy). If employee requires a separate access to systems not covered in the department, a standard request to the IT department will automatically inform Linear Manager.

Allocation of user's access rights should be provided in accordance with formal procedure [provide link]. Linear Managers can only request employee user accounts. No access to any **SoftServe** Inc. staff IT resources and services shall be provided without prior authentication and authorization of a user's **SoftServe** Inc. account.

User accounts shall be disabled immediately upon termination of employment, contract or agreement, unless a request for an extension is received from the relevant Linear Manager. Removal of user's access rights should be provided in accordance with formal procedure [provide link].

Users' access rights should be reviewed after any changes, such as promotion, demotion or termination of employment, and re-allocated when moving from one role to another within the organization. Changes to privileged accounts should be logged for periodic review. Review of users access rights should be provided in accordance with formal procedure [provide link].

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Access for external user to Internal Corporate Resources is provided via VPN account according to procedure Grant Access to Internal Corporate Resources for external user. VPN access rights may be given to individuals who are not employees of **SoftServe** such as customer representatives, consultants, etc. in order to grant access to project environments, which located in corporate network. Linear Manager should submit a standard ticket to IT department if his project requires remote access to some local resources. Time-limited VPN accounts will be created after ticket evaluation and information security officer’s approval. Access for remote users shall be provided in accordance with the ISMS DOC 6.3 Teleworker Security Policy and the ISMS DOC 5.1 Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk will manage password issuing. The criteria for passwords are given at: ISMS DOC 9.5 Password Policy.

Access to ‘Confidential’, ‘Restricted’, 'Secret' or 'Top Secret' information will be limited to authorized persons whose job responsibilities require it, as determined by law, contractual agreement or the ISMS DOC 5.1 Information Security Policy. The responsibility to implement access restrictions lies with the data and systems owners. Access to data is variously and appropriately controlled according to the data classification levels described in the ISMS DOC 8.8 InfoSec Classification Standard.

Administrative Access to information systems divided to security levels based on possibility to store or transit corporate sensitive information and described in ISMS DOC 9.3 Information Systems Administrative Access Standard.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within **SoftServe** Inc. Active Directory domains. There are no restrictions on the access to ‘Public’ information.

Users are expected to become familiar with and abide by **SoftServe** Inc. policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the ISMS DOC 8.6 User Workplace Software Use Policy at **SoftServe** Inc. and the ISMS DOC 8.3 Acceptable Use Policy.

Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   2. *Implementation specifications*:
      i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Workstation Use (§ 164.310(b))

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

Workstation Security (§ 164.310(c))

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Workstation Use (§ 164.310(b))

Comment: One commenter was concerned most people may be misled by the use of "terminal" as an example in the definition of workstation. The concern was that the standard only addresses "fixed location devices," while in many instances the workstation has become a laptop computer.

Response: For clarity, we have added the definition of "workstation" to § 164.304 and deleted the word "terminal" from the description of workstation use in § 164.310(b).

Workstation Security (§ 164.310(c))

Comment: Comments were directed toward the example profiled in the definition of a secure workstation location. It was believed that what constitutes a secure workstation location must be dependent upon the entity's risk management process.

Response: We agree that what constitutes an appropriate solution to a covered entity's workstation security issues is dependent on the entity's risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title "Secure workstation location" has been changed to "Workstation security" (see also the definition of "Workstation" at § 164.304).

Policy Number: 8.6
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Workstation Use Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- ❑ The establishment and implementation of an effective workstation use policy is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to configure, operate, and maintain our information workstations in full compliance with all the requirements of HIPAA.
- ❑ Our objective in these efforts is to providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- ❑ Responsibility for the development and implementation of this workstation use policy, and any procedures associated with it, shall reside with Asset Owners, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.

Acceptable Use

Corporate User IDs, websites, e-mail and social network accounts may only be used for organizationally sanctioned communications. Any postings by users using **SoftServe** User ID, email address, or in any other means referenced to **SoftServe**, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of **SoftServe**, unless posting is in the course of business duties.

Users should refer to ISMS DOC 8.4 E-Mail Standard for guidance on email service usage and to ISMS DOC 8.5 Office Equipment Usage Standard - for office equipment usage

Employees assume any and all risk associated with public communications. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent themselves as an employee or representative of **SoftServe**.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, **SoftServe** trademarks, logos, and any other **SoftServe** intellectual property may be used in connection with any social activity, only if this is in the course of business duties.

Use of Internet/intranet/e-mail/instant messaging may be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations by the organization.

The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinized by the organization and the organization reserves the right to determine the suitability of the information.

Users should send e-mails containing classified information with the appropriate level of protection required in ISMS DOC 8.8 InfoSec Classification Standard.

Users will not seek to avoid and will uphold the organization’s anti-malware policy (ISMS DOC 12.3 Policy Against Malware), will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person's files or any other information asset for which they don't have the owner's explicit permission.

The use of organizational computer resources is subject to local and international laws and any abuse will be dealt with appropriately. Under no circumstances, a **SoftServe** employee is authorized to engage in any activity that is illegal under local or international law while utilizing **SoftServe**-owned resources.

Limited Use for Development and Testing

Having large portfolio of software development projects under development requires **SoftServe** to impose certain limitations on using generic corporate systems and networks for development and testing purposes.

Specifically, no project environments should use corporate information systems and IT infrastructure services, including authentication services and Active Directory, as part of development, testing or staging infrastructure.

Projects requiring IT infrastructure services, should use services described in IT Business Portfolio Projects Test Lab (see https://confluence.softserveinc.com/display/ITBP/Projects+Test+Lab), or request deployment of separate infrastructure.

Users will not send emails from test environments via corporate email service or perform any sort of network tests/scans against corporate network devices without prior approval from Director of Infrastructure and Operations Team.

Users shall not deploy any kind of services on corporate network, without IT Department permission. Except in isolated desktop/workstation, Virtual Machine or project environments.

Personal Use of Computing Resources

Moderate use for personal purposes of individually assigned computing resources (workstations, phones, printing facilities) and corporate Internet access is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate **SoftServe** policy, is not detrimental to **SoftServe** best interests, and does not interfere with an employee's regular work duties. In particular it should not violate local or international laws, including, but not limited to laws on intellectual property (copyright) protection.

Mobile devices usage is regulated by ISMS DOC 8.15 Mobile Devices Usage Policy.

Users are responsible for exercising good judgment regarding the reasonableness of personal use, if there is any uncertainty, users should consult their supervisor or manager.

Limited and occasional use of **SoftServe** systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate **SoftServe** policy, is not detrimental to **SoftServe** best interests, and does not interfere with an employee's regular work duties. Blogging from **SoftServe** systems is also subject for monitoring.

Resource usage is subject to monitoring, abuse leading to function degradation or increase of company expenses may lead to disciplinary actions or financial sanctions.

Privacy

While configuration of **SoftServe** information assets provides reasonable level of privacy, users should be aware that all data they create on the corporate systems remains the property of **SoftServe** and may be subject to monitoring for compliance or used for valid business purposes.

SoftServe reserves the right to audit networks and systems on a periodic basis to ensure compliance and security of information assets. Authorized individuals within **SoftServe** may monitor equipment, systems, and network traffic at any time per *Availability Tracking*.

Unacceptable Use

The following activities are, in general, prohibited. The lists below are by no means exhaustive, but an attempt to provide a framework for activities, which fall into the category of unacceptable use.

Network

- ❑ Introduction of malicious software into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- ❑ Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- ❑ Port scanning or security scanning is expressly prohibited, unless prior notification is made.
- ❑ Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- ❑ Circumventing user authentication or security of any host, network, or account.

- ❑ Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- ❑ Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- ❑ Use the corporate network services for any types of testing, which can cause unstable work of the services, decrease their efficiency and performance.

Messaging

- ❑ To solicit e-mails that are unrelated to business activity or which are for personal gain, shall not send or receive any material, which is obscene or defamatory, or which is intended to annoy, harass, or intimidate another person.
- ❑ Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam).
- ❑ Unauthorized use or forging of email header information.
- ❑ Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- ❑ Automatic forwarding of business e-mail to external mail addresses.
- ❑ Using E-Mail Service for:
  - Exchange of files (especially executable);
  - Exchange/storage of sources.
- ❑ Use corporate SMTP server smtp.softserveinc.com (smtp.softservecom.com) for projects environments (there is special SMTP server for projects environments mail.projects.softservecom.com).

User workplace software

- ❑ To download software from the Internet or execute or accept any software programs or other code on the Internet unless it is in accordance with User Workplace Software Use Policy (see ISMS DOC 8.6 User Workplace Software Use Policy).
- ❑ To install and/or use operational systems different from Windows and Mac OS on corporate workstation(s).
- ❑ Change the configuration of the workstation OS, namely:
  - Create, remove, relocate, and change the disks size or type.
  - Change the network configuration of the OS.
  - Delete, block the users accounting records (user and security groups).

- Change basic rights of the access for accounts or groups.
- Remove basic software.
- Intervene in the standard service processes.

Organization's Assets

- ❑ Using a **SoftServe** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- ❑ Use the Company`s computers or corporate resources for swindling or other sorts of illegal activities (including storing and sharing information which is forbidden according to the laws of the **SoftServe** employee country; installing, saving, or sharing illegal software; creating or spreading computer viruses, etc.)
- ❑ Use the hardware purpose it was not designed or in violation of respective vendor recommendations, instructions.
- ❑ Change the hardware configuration and connection unless unless this activity is a part of the employee's normal job/duty.
- ❑ Relocate hardware without IT Department representative permission.
- ❑ Connect any network devices to the corporate network without IT Department representative permission, except the Wi-Fi devices connection to SS-Mobile network.

Access

- ❑ Make attempts to bypass any Internet access limitations imposed by the company to receive illegal access (for example, deciphering of the users' passwords, usage of the programs for searching such information in the network traffic).

Public communication

- ❑ To attribute employee's personal statements, opinions, or beliefs to **SoftServe**
- ❑ To engage in any communications that may harm or tarnish the image, reputation, and/or goodwill of **SoftServe** and/or any of **SoftServe** employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments.
- ❑ Making fraudulent offers of products, items, or services originating from any **SoftServe** account.
- ❑ Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Passwords

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Copyrights

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by **SoftServe**.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software, for which **SoftServe** or the end user does not have an active license, is strictly prohibited.
- To upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties.
- To use non-organizational version control services for copyrighted materials belonging to the company or any third parties.

Information handling

- Change the information, which does not belong to the user without tentative coordination with the information owner, except cases discussed with the IT Department. In case of the project resources, the data owner is the project manager.
- To reveal or publicize classified information.
- Store information on workstations, mobile devices or BYOD that is not backed up or synchronized with corporate resources.

Acceptable use of company's assets

To guarantee the security and quality of the network, services and facilities functioning, the user is obliged to follow the Company`s policies, standards and rules, regarding acceptable use of assets:

- Policy of assets acceptable usage and standards of acceptable use of companies network - Acceptable Use Policy;

- ❑ Standard of using mail services - Mailing Use Standard;
- ❑ Standard of using office facilities - Office Equipment Usage Standard;
- ❑ Policy of proper handling of removable media - Removable Media Policy;
- ❑ Secure usage of company's mobile devices - Mobile Devices Security Standard;
- ❑ Policy on use of personal mobile devices - BYOD Policy;
- ❑ Policy of acceptable use of workplace software - User Workplace Software Use Policy.

Security training and awareness

Each employee should get acquainted with Information Security Training and Awareness Policy and pass security awareness training to ensure, that they understand the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as Social Engineering).

Secure access

Accessing to company's network and resources employee should follow next policies and standards:

- ❑ Standards of logging on - Secure Logon Standard;
- ❑ Policy and standards of password management - Password Policy;
- ❑ Policy, which outlines the clear desk and clear screen standards at **SoftServe** - Clear desk and clear screen Policy.

Security incidents reporting

InfoSec Department provides Security Incidents Management. Each employee should report any security incident using Security Incident Reporting Procedure

Additional responsibilities

Additional policies, standards and procedures might be provided to employees depending on employee's responsibilities.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with the Sanction Policies of **SoftServe Inc.**

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   2. *Implementation specifications*:
      - i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      - ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      - iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      - iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Workstation Use (§ 164.310(b))

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

Workstation Security (§ 164.310(c))

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Workstation Use (§ 164.310(b))

Comment: One commenter was concerned most people may be misled by the use of "terminal" as an example in the definition of workstation. The concern was that the standard only addresses "fixed location devices," while in many instances the workstation has become a laptop computer.

Response: For clarity, we have added the definition of "workstation" to § 164.304 and deleted the word "terminal" from the description of workstation use in § 164.310(b).

Workstation Security (§ 164.310(c))

Comment: Comments were directed toward the example profiled in the definition of a secure workstation location. It was believed that what constitutes a secure workstation location must be dependent upon the entity's risk management process.

Response: We agree that what constitutes an appropriate solution to a covered entity's workstation security issues is dependent on the entity’s risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title "Secure workstation location" has been changed to "Workstation security" (see also the definition of "Workstation" at § 164.304).

SECTION 9

Policy Number: 9.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Media Re-Use Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- ❑ Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased or sanitized ("wiped") before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to properly erase and or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used.
- ❑ Responsibility for proper media re-use shall reside with IS Manager, who shall develop procedures to ensure the proper disposition of all such media before any re-use.
- ❑ It is the Policy of **SoftServe Inc.** to fully document media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Hardcopy information

Storage

Hardcopy information that is deemed confidential, secret or top secret (classification is described in ISMS DOC 8.8 InfoSec Classification Standard) shall be stored in an area secured by lock and out of plain view. Access to that information shall be logged limited to parties deemed appropriate by the department "owning" the information. Storage of the information shall be in a facility that is:

- ❑ Not readily accessible by window
- ❑ Has limited door access
- ❑ Is protected from environmental threats

Disposal

Hardcopy information that is deemed confidential, secret or top secret (classification is described in ISMS DOC 8.8 InfoSec Classification Standard) may be destroyed in accordance with applicable document retention laws. Such documents must be shredded prior to disposal. Third parties may be contracted to dispose of documents, but an agent of **SoftServe** must witness the destruction of all documents.

Digital information

Storage

Organization's digital information shall be stored on workstations, media, drives, disks, corporate resources etc. that are approved or owned by the organization. Each user provided access to that information shall be given a unique account and all access attempts shall be logged. The organization's resource storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.

Disposal

The Asset Owner shall destroy digital information that is deemed confidential, secret or top secret, or ITSD Representative using a secure wipe program or hardware device. Applications that remove data to a degree meeting or surpassing regulatory or customer requirements are required if a hardware wipe device is not used. All storage devices shall be cleaned using an approved mechanism. CD's, DVD, tapes, disk, etc. shall be destroyed prior to disposal. CD's and DVD's containing confidential, secret or top secret information shall be shredded or broken in multiple pieces by InfoSec representative. USB keys and memory sticks shall be crushed prior to disposal.

Loss of information resources

The loss of control or custody of organization information shall reported to the IS Manager immediately upon realization of the loss in accordance to ISMS DOC 16.2 Security Incident Reporting Procedure.

Retention

SoftServe requires that different types of records be retained for a specific period of time to comply with US, UK and Ukrainian legislation, customer requirements and organization's practice. Legislation and contractual requirements can be found in ISMS DOC 18.4 Retention Standard.

Retention Standard applies to all records, regardless of format.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.

1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
2. *Implementation specifications*:

        i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
        ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
        iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
        iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

d.

    1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
    2. *Implementation specifications*:
        i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
        ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
        iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
        iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included "Access control," "Accountability" (tracking mechanism), "Data backup," "Data storage," and "Disposal."

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from "Media controls" to "Device and media controls" to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed "Access control" implementation feature has been removed, as it is addressed as part of other standards (see section III.C.12.c of this preamble).

Policy Number: 9.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Media Disposal Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- ❑ Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA.

- ❑ Responsibility for proper media disposal and disposition shall reside with IS Manager, who shall develop procedures to ensure the proper disposition of all such media.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Hardcopy information

Storage

Hardcopy information that is deemed confidential, secret or top secret (classification is described in ISMS DOC 8.8 InfoSec Classification Standard) shall be stored in an area secured by lock and out of plain view. Access to that information shall be logged limited to parties deemed appropriate by the department "owning" the information. Storage of the information shall be in a facility that is:

- ❑ Not readily accessible by window
- ❑ Has limited door access
- ❑ Is protected from environmental threats

Disposal

Hardcopy information that is deemed confidential, secret or top secret (classification is described in ISMS DOC 8.8 InfoSec Classification Standard) may be destroyed in accordance with applicable document retention laws. Such documents must be shredded prior to disposal. Third parties may be contracted to dispose of documents, but an agent of **SoftServe** must witness the destruction of all documents.

Digital information

Storage

Organization's digital information shall be stored on workstations, media, drives, disks, corporate resources etc. that are approved or owned by the organization. Each user provided access to that information shall be given a unique account and all access attempts shall be logged. The organization's resource storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.

Disposal

The Asset Owner shall destroy digital information that is deemed confidential, secret or top secret, or ITSD Representative using a secure wipe program or hardware device. Applications that remove data to a degree meeting or surpassing regulatory or customer requirements are required if a hardware wipe device is not used. All storage devices shall be cleaned using an approved mechanism. CD's, DVD, tapes, disk, etc. shall be destroyed prior to disposal. CD's and DVD's containing confidential, secret or top secret information shall be shredded or broken in multiple pieces by InfoSec representative. USB keys and memory sticks shall be crushed prior to disposal.

Loss of information resources

The loss of control or custody of organization information shall reported to the IS Manager immediately upon realization of the loss in accordance to ISMS DOC 16.2 Security Incident Reporting Procedure.

Retention

SoftServe requires that different types of records be retained for a specific period of time to comply with US, UK and Ukrainian legislation, customer requirements and organization's practice. Legislation and contractual requirements can be found in ISMS DOC 18.4 Retention Standard.

Retention Standard applies to all records, regardless of format.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   2. *Implementation specifications*:
      - i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      - ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      - iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      - iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

d.
   1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
   2. *Implementation specifications*:
      - i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
      - ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included "Access control," "Accountability" (tracking mechanism), "Data backup," "Data storage," and "Disposal."

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from

"Media controls" to "Device and media controls" to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed "Access control" implementation feature has been removed, as it is addressed as part of other standards (see section III.C.12.c of this preamble).

Policy Number: 9.2
Effective Date: 3/26/13
Last Revised: 7/29/2014

Hardware and Media Accountability Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at § 164.310(d)(1-2).
- ❑ Proper protection of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), requires that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with InO Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to ensure that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all hardware and media accountability-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Standard

The **SoftServe** maintains a single inventory of assets, which is subdivided into a categories: hardware, software, personnel, site, network and services. Asset registers are stored and processed in Configuration Management Database (CMDB) - as part of **SoftServe** overall IT Service Management solution build on BMC SDE software (as CMDB is now in process of fulfillment, table below shows actual state of SA inventorying).

The organization groups some assets together into composite asset group, in which case it identifies the assets what affected by same threats and vulnerabilities. (ISMS DOC 8.1 Organization Assets Groups).

In addition, the organization maintains lists of key information-related services (which includes designated secure areas), and management is aware of those individuals whose skills, knowledge and experience are considered essential.

The list of asset groups (ISMS DOC 8.1 Organization Assets Groups) is used in the risk assessment process (see ISMS DOC 4.1 Risk Management Framework).

For each asset, the organization documents sufficient information to identify the asset (if require: type or category of asset, make or manufacturer, model, serial number), identifies the physical (or logical) location of the asset, information security classification of each asset, and the security processes or controls (including access controls, backups, etc.).

For each asset, the organization identifies the business unit or business role that 'owns' the asset. The owner is responsible for ensuring that the asset is correctly classified, for the day to day maintenance of the identified controls, that access controls (see ISMS DOC 9.1 Access Control Policy) are defined and periodically reviewed, and that vulnerabilities are identified.

Owners may delegate routine tasks, in respect of their assets or systems to the subordinates with appropriate knowledge level and experience.

All new information assets are added to the next iteration of Risk Assessment, together with details of the required security processes/controls.

Table, which shows progress of inserting Secondary Assets into CMDB:

Group of assets	Secondary Asset	Inventory location
Hardware	PC	CMDB
	Mobile Devices	CMDB
	Laptop	Inventory on portal
	Network equipment	CMDB
	Telephony user equipment	CMDB
	Server Hardware	Inventory on portal
	Legal Documents	-
	Legal Media	-
	Finance Documents	-
	Finance Media	-
Software	User Workplace Software	-

Group of assets	Secondary Asset	Inventory location
	Customized/In House Developed Software	-
	Server Software	-
Personnel	**SoftServe** Employees	SSE
	SoftServe Project Team Members	SSE
Site	Lviv1	-
	Lviv2	-
	Lviv3	-
	Lviv4	-
	Chernivtsi	-
	I.Frankivsk	-
	Dnipropetrovsk1	-
	Dnipropetrovsk2	-
	Rivne	-
	Fort Myers, FL	-
	Sevastopol	-
	Security Areas Lviv1	-
	Security Areas Lviv2	-
	Security Areas Lviv3	-
	Security Areas Lviv4	-

Group of assets	Secondary Asset	Inventory location
	Security Areas Chernivtsi	-
	Security Areas I.Frankivsk	-
	Security Areas Dnipropetrovsk1	-
	Security Areas Dnipropetrovsk2	-
	Security Areas Rivne	-
	Security Areas Fort Myers, FL	-
	Security Areas Sevastopol	-
Network	Intranet	-
	LAN	CMDB
	Extranet	-
	Internet Access	-
	Telephony	-
	Wireless Network	-
Services	Printing (Equipment and Software)	-
	Software as a Service	-
	Internet Service Provision	-
	Air-conditioning and heating services	-
	Office Renting	-

SoftServe Inc. information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by government agencies. Removable media (portable storage devices) must be encrypted in accordance with the **SoftServe** ISMS DOC 10.1 Encryption Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   2. *Implementation specifications*:
      i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

d.
   1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
   2. *Implementation specifications*:
      i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
      ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included "Access control," "Accountability" (tracking mechanism), "Data backup," "Data storage," and "Disposal."

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from

"Media controls" to "Device and media controls" to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed "Access control" implementation feature has been removed, as it is addressed as part of other standards

Comment: Several commenters believe the "Media controls" implementation features are too onerous and should be deleted. **SoftServe Inc.**

Response: While the "Device and media controls" standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the "Accountability and data backup" implementation specification as addressable to provide more flexibility in meeting the standard.

Comment: One commenter was concerned about the accountability impact of audit trails on system resources and the pace of system services.

Response: The proposed audit trail implementation feature appears as the addressable "Accountability" implementation specification. The name change better reflects the purpose and intended scope of the implementation specification. This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services.

Policy Number: 9.3
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Mobile Device Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- ❑ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- ❑ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to extend all the privacy and security protections required by HIPAA to Protected Health Information accessed, used, transmitted, and stored on mobile devices operated by members of our workforce.
- ❑ It is the Policy of **SoftServe Inc.** to include privacy and security issues related to mobile devices in our Risk Management process and analyses, to better understand risks inherent in the use of such devices.

- ❑ This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and are capable of receiving, processing, or transmitting Protected Health Information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Mobile Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile Devices include, but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).
- ❑ This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased by, and provided by **SoftServe Inc.**
- ❑ Mobile Devices which cannot be or have not been configured to comply with this Policy are prohibited.
- ❑ It is the Policy of **SoftServe Inc.** to limit the access, use, transmittal, and storage of Protected Health Information exclusively to those mobile devices that can be configured and operated to deliver privacy and security comparable to the non-mobile data processing systems and devices that we operate.
- ❑ It is the Policy of **SoftServe Inc.** to limit the access, use, transmittal and storage of Protected Health Information on mobile devices to the Minimum Necessary, as that term is defined in the HIPAA Regulations.
- ❑ It is the Policy of **SoftServe Inc.** to train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit, or store Protected Health Information
- ❑ It is the Policy of **SoftServe Inc.** to fully document all mobile device-related activities, which involve Protected Health Information, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- ❑ No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by the IT Department/Security Office/etc. Authorization will be given only for uses of Mobile Devices confirmed to have been configured to be compliant with this Policy.
- ❑ Any access, use, transmittal or storage of Protected Health Information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any **SoftServe Inc.** facility or office, including an authorized home office or remote site, must be in compliance with all **SoftServe Inc.** policies at all times.
- ❑ Authorization to use a Mobile Device may be suspended at any time:
  - If the User fails or refuses to comply with this Policy;
  - In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
  - In connection with the investigation of a possible or proven security breach, security incident, or violation of **SoftServe Inc.'s** policies;
  - In order to protect life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of **SoftServe Inc.**;
  - Upon request of a supervisor or department head in which the User works; or
  - Upon the direction of Ino Manager.
- ❑ Authorization to use a Mobile Device terminates:
  - Automatically upon the termination of a User's status as a member of **SoftServe Inc.'s** workforce;

- Upon a change in the User’s role as a member of **SoftServe Inc.’s** Workforce, unless continued authorization is authorized in writing.
- If it is determined that the User violated this or any other **SoftServe Inc.** policy, in accordance with **SoftServe Inc.’s** Sanction policy.

❑ The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.

❑ At any time, any Mobile Device may be subject to audit to ensure compliance with this and other **SoftServe Inc.** policies. Any User receiving such a request shall transfer possession of the Mobile Device to IT Department/Security Office/etc. at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.

Mobile devices taken outside secure **SoftServe** environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorized access or tampering. Mobile devices taken abroad may also be at risk, for example confiscated by police or customs officials.

Mobile device's loss will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of sensitive information. Loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset.

This procedure describes security measures required to protect mobile computing and communicating devices such as notebook or tablet computers, personal digital assistants (PDA’s), cell phones or other similar equipment from theft, loss or damage.

General measures

❑ An employee who was allocated by mobile computing or communicating device is responsible for its safety and custodianship in the office and outside the office.

❑ While connecting to a local area network (LAN) or Internet, mobile device, which was without connection, shall be automatically updated with the latest antivirus signature.

❑ Only licensed software may be loaded on **SoftServe's** mobile devices (ISMS DOC 12.8 Software Licensing Policy).

❑ A notebook PC shall always be carried in a padded carry bag.

❑ If mobile device or any of its accessories were lost due to outright negligence, a staff member shall compensate the loss financially.

❑ Lost or stolen devices must be reported to the company within 24 hours trough ISMS DOC 16.2 Security Incident Reporting Procedure.

Access control

- ❑ Users must not grant access to their mobile devices to unauthorized individuals.
- ❑ Users must use strong passwords (according to ISMS DOC 9.5 Password Policy).
- ❑ If the user's mobile computing device is equipped with a biometric device, such as a fingerprint reader, it should be enabled and used with a strong password.
- ❑ All mobile devices must have a password protected keyboard/screen lock that is automatically activated by a period of inactivity (according to ISMS DOC 9.6 Secure Logon Standard).
- ❑ Device should lock in case of reaching limit of incorrect logon attempts (according to ISMS DOC 9.6 Secure Logon Standard).
- ❑ Users must use the **SoftServe** virtual private network to access **SoftServe** resources from insecure networks, such as wireless and public Internet service providers.
- ❑ Remote access from a mobile computing device to **SoftServe** information systems must be achieved in accordance with the ISMS DOC 13.1 Network Control Policy, and any defined requirements for the protection or use of the **SoftServe** information service(s) should be met.
- ❑ All peer-to-peer wireless communication technologies, i.e., ad-hoc Wi-Fi, Bluetooth, infrared, etc., must be disabled when not in use.

Data storage and use

- ❑ Sensitive data should be kept to the minimum required for its effective business use in order to minimize the risks and impacts should a breach occur.
- ❑ If sensitive data are stored on a Mobile Device, the Device should be equipped with data encryption software so that if the device is stolen or accessed, the data cannot be recovered.
- ❑ Mobile Devices require the use of a password/PIN to gain access to the data stored on it
- ❑ If functionality is provided, Mobile Devices must erase all data stored on them after not more than 10 invalid log-in attempts.
- ❑ All Corporate information stored on a Mobile Device must be securely erased prior to disposal, reuse, resale or return to a vendor at end of a lease.
- ❑ The employee's device may be remotely wiped if:
    - The device is lost

- the employee terminates his or her employment
- IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure

Referring to security in business trips

- □ User should never leave device in public or insecure areas and should be especially alert in hotels, airports, restaurants, conference centers, meeting places, at railway stations and bus stops.
- □ Users should always carry the mobile device as hand baggage onto the aircraft and should not allow it to be sent with luggage under no circumstances.
- □ If using BYOD, users should keep a record mobile device's model, serial number and IMEI number (if applicable) - this information could be useful for police in the case of theft.
- □ A standard configuration is installed and maintained by the ITSD. Mobile device user may not install own software or change configuration settings without the prior knowledge and consent of the ITSD User Support Engineer.
- □ If leaving device behind in secure locations, user should still log off or lock the screen before leaving, to prevent access to stored data by other persons.

Off-Premises Equipment Usage

- □ Users of mobile devices in public areas outside the company should take proper safeguards in line with ISMS DOC 8.9 Mobile Devices Security Standard to ensure that unauthorized viewing of sensitive data is avoided, such as ensuring that their device is not left unattended, screens are locked whenever they are not used, and sensitive data is not displayed on screens in widely public areas.
- □ Users of Mobile devices accessing the Internet from public places should ensure that proper security measures are maintained. Users should ensure the antivirus is always active to maintain the protection of their devices.
- □ As much as possible, store sensitive company data only on approved network storage drives rather than on any mobile device or laptop.
- □ In case the user faces an operational or security incident while using his portable device, he should immediately report it to the IT Department for proper handling and support.

General mobile device manufacturer rules (MDMR)

Device safety

- ❑ Switch the device off when mobile phone use is not allowed or when it may cause interference or danger, for example, in aircraft, in hospitals or near medical equipment, fuel, chemicals, or blasting areas. Obey all instructions in restricted areas.
- ❑ Obey all local laws. Always keep your hands free to operate the vehicle while driving. Your first consideration while driving should be road safety.
- ❑ The device screen is made of glass. This glass can break if the device is dropped on a hard surface or receives a substantial impact. If the glass breaks, do not touch the glass parts of the device or attempt to remove the broken glass from the device. Stop using the device until the glass is replaced by qualified service personnel. Inform IT Department

Proper care

- ❑ Keep the device dry. Precipitation, humidity, and all types of liquids or moisture can contain minerals that corrode electronic circuits. If your device gets wet, remove the battery, and allow the device to dry.
- ❑ Do not use or store the device in dusty or dirty areas. Moving parts and electronic components can be damaged.
- ❑ Equipment should be protected from power failures and other electrical anomalies. The electrical supply to all force equipment should conform to the equipment manufacturers' specifications.
- ❑ Mustn't turn on immediately HW in the cold temperature after warm room and conversely
- ❑ Save device from drop, knock, or shake. Rough handling can break internal circuit boards and mechanics.
- ❑ Do not paint the device. Paint can clog moving parts and prevent proper operation.
- ❑ Keep your device away from magnets or magnetic fields.

Lost/Stolen Equipment Off-premises

SoftServe and all of its employees are legally obliged to protect sensitive company data. If this data or the network and computer resources that contain it become compromised or threatened due to the loss or theft of information technology equipment, for example a device such as a laptop or smart phone, company and its employees must immediately take steps to prevent or minimize the harm or damage that could result. In the event of a loss, these procedures anticipate the rapid execution of each step in order to minimize the impact of the loss.

- ❑ When device (laptop, desktop, smart phone, iPad, other) is lost or stolen, immediately call local Police to report the incident at any time of day or night or in case when issue is caused in company premises inform Guard in appropriate offices
- ❑ Equipment missing or stolen is reported immediately to IT Department. Employee should provide copy of police report in case of device being stolen.
- ❑ The IT department will, among other things, reset your password and block all access to network resources, including e-mail, until such a time that you can change your password.
- ❑ IT will contact you to determine the nature and scope of any compromised sensitive data.
- ❑ If there was a potential compromise of sensitive information or exposure of network resources, the Chief Information Security Officer may confer with appropriate company officials and/or legal counsel, coordinate notification to affected individuals, and report the incident to state agencies and the media as required

HIPAA Group recommends the following materials to help you gain a better understanding of mobile device risks, and how to configure and utilize mobile devices for maximum security:

- ❑ ***Security Guidance for Remote Users*** **– Centers for Medicaid and Medicare Services**
  www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

- ❑ ***An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*** **– National Institute of Standards and Technology (Publication No. SP800-66)**
  ...as well as other NIST I.T. Security papers and reports available from:
  http://csrc.nist.gov/publications/PubsSPs.html

Policy Number: 9.4
Effective Date: 3/26/2013
Last Revised: 7/26/2014

Data Backup and Storage Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backup and storage, in accordance with the requirements at § 164.310(d)(1-2) and § 164.308(a)(7).
- ❑ The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and electronic protected health information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- ❑ The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- ❑ Timely access to health information is crucial to providing high quality health care, and to our business operations.
- ❑ Physicians and others must have immediate, around-the-clock access to patient information.
- ❑ No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- ❑ A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to create retrievable, exact copies of electronic protected health information, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.
- ❑ The <u>Asset Owner</u> is responsible for performing appropriate backups on **SoftServe Inc.'s** network, including shared drives containing application data, patient information, financial data, and crucial system information.

Procedures

- ❑ <u>Asset Owners</u> will back up all such data as necessary, ISMS programmed standards, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.

- ❑ The Asset Owner or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in Lviv.
- ❑ The media vault meets fire and disaster standards for media and will be kept locked at all times. Only ISMS team, the system administrator, and their designees have access to the media vault.
- ❑ In the event that the secured media vault is not available or properly functioning, a member of the ISMS team, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
- ❑ Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer's recommended guidelines, currently once per week, or specify other period.
- ❑ The ISMS Manager will ensure replacement of backup tapes or media according to manufacturer's recommended guidelines, currently annually (or specify other media replacement timeframe(s)).
- ❑ The ISMS Manager is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly (or specify other timeframe), and more often if necessary to ensure data integrity, availability, and confidentiality.
- ❑ Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ All personnel who detect or suspect a data backup problem should immediately report the same to the InO. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
  - Narrative of the data backup problem.
  - How long the problem has existed.
  - Suggested solutions.

Data classification

The following default parameters are set depending on the information classification level:

				Corporate Backup Policy					
				Standard services		**Critical services**		**Low-end services**	
№	**Corporate Data Type**	**Windows based systems**	**Linux based systems**	**Retention range**	**Backup/Synchronization frequency**	**Retention range**	**Backup/Synchronization frequency**	**Retention range**	**Backup/Synchronization frequency**
1	**System files and System partition**	Bare-Metal type of data which using for Bare Metal Recovery	System files, partition of Operation Systems, ext.	14 days	Daily	30 days	Daily	14 days	Weekly
2	**Microsoft Databases**	SQL Server type of data which related to Microsoft SQL products (included WID)	Not Using	14 days	Daily	30 days	15 minutes	7 days	Daily
3	**Linux Databases**	Not Using	Corporate Databases of PostgreSQL, MySQL, ext.	14 days	Hourly (exclude Night)	14 days	Hourly (exclude Night)	7 days	Daily

4	**Setups and components necessary for project works**	File Server - type of data which related to files and folders, SharePoint Server - type of data which related to Microsoft Share Point products.	Setups and components necessary of Corporate Sites, ext.	14 days	Daily	30 days	2 times per day or Hourly	7 days	Daily
		Not Using	Setups and components necessary of FTP, Monitoring systems, ext.	30 days	Daily	Not Using	Not Using	7 days	Daily
		Not Using	Interim and final codes of the software product of SVN(Subversion), ext.	Not Using	Not Using	30 days	Hourly (exclude Night)	Not Using	Not Using
5	**Documentation, financial and administrative data**	File Server - type of data which related to files and folders, SharePoint Server type of data which related to Microsoft Share Point products	Documentation, financial and administrative data of Attachments, Atlasian, ext.	30 days	Daily	30 days	3 times per day or Hourly	14 days	Daily

6	**Mailing Service**	Exchange Server type of data which related to Microsoft Exchange Server products	Not Using	7 days	Daily	14 days	Every 4 hours	Not Using	Not Using
7	**Integrity Check of Critical Files**	Not Using	Integrity Check of Operation Systems, ext.	1 Day	Daily	1 Day	Daily	1 Day	Daily
8	**Virtual Machines (VMware VDR/VDP)**	Backup your Virtual Machines of VMware Data Recovery	Backup your Virtual Machines of VMware Data Recovery	14 Day	Daily	Not Using	Not Using	30 days	Weekly

Backup parameters

- ❑ Specialized servers automatically perform backup: for Windows based systems - Microsoft DPM; for Linux based systems - Network Backup Solution Bacula.
- ❑ Backup server administrators (backup operators) and owners of resources to be backed up are sent automatic notifications on successful performance of scheduled backup tasks.
- ❑ Access to backup servers and media, which store backups, is limited.
- ❑ Backup tasks should be carried out at hours when resources to be backed up are least loaded.
- ❑ Backup testing is provided periodically by asking backup's owners to restore data and to write feedback about successful or unsuccessful results.

Backup methodology

Depending on retention time and synchronization frequency, different backup methods are provided:

- ❑ **Full backup** — a complete backup which besides files incorporates additional information about the time of their last modification. Used in combination with **Incremental backup** or **Differential backup.**
- ❑ **Incremental backup** — a partial backup that incorporates only files modified after the last full **backup** or **incremental backup**. Used in combination with Full backup. **Incremental backups** take up less storage space than differential backup, but first the **full backup** needs to be recovered followed by a recovery of all **incremental backups** as of the relevant date in order to recover information.
- ❑ **Differential Backup** — a partial backup that incorporates all files modified after the last **full backup**. Used in combination with **full backup**. **Differential backups** take up more space than **incremental backups**, but only the **full backup** and one **differential backup** need to be recovered as of the relevant date in order to recover information. Differential backups constantly grow in size after the last **full backup**. Therefore, the **full backup** needs to be done more often that in case of **full/incremental.**
- ❑ **Non-disruptive backups** – At the time of backup, a snapshot is taken of the virtual machine, and the snapshot is presented to the backup application. This simplifies management by eliminating the need to have an agent running inside the virtual machine. It also avoids consuming resources within the virtual machine for backup jobs.
- ❑ **Encapsulation** – VMware virtualization encapsulates a complete system—including operating system, applications and data—into a small set of files. As a result, the entire system is backed up and can be recovered in a single operation, eliminating the complexity of traditional data protection solutions.

- □ **Short-term protection**. Short-term backup can be performed to disk, to disk and Windows Azure, or to tape. Short-term tape backup can’t be used for client protection groups, or for workload data. It can only be used for server file data (such as volume, shares, and folders).
- □ **Long-term protection**. Only tape is supported for long-term backup. If tape is used for long-term protection, there is possibility to compress or encrypt the data. Encrypted data might result in taking up more space than unencrypted data. Data encryption will require a certificate for authentication.
- □ **Synchronization frequency**. Synchronization frequency specifies how often the data you want to protect will be synchronized with the DPM replica. Synchronization frequency interval could be from 15 minutes to 24 hours, or it’s possible to selected synchronization only before a recovery point is created (in accordance with recovery point settings). The default setting is 15 minutes, which means that DPM server version of the data won’t be more than 15 minutes behind the version on the protected computer.
- □ **Recovery points**. A recovery point (snapshot) is a point-in-time copy of a replica stored on the DPM server. DPM creates recovery points of each replica in a protection group according to recovery point settings. The recovery points could be accessed to recover previous versions of files in the event of data loss or corruption. Data could be recovered from recovery points, and the end-user recovery could be configured to let users to recover their own data from recovery points.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   2. *Implementation specifications*:
      i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

        iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
d.
    1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
    2. *Implementation specifications*:
        i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
        ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
        iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
        iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Comment: Several commenters believe the "Media controls" implementation features are too onerous and should be deleted.

Response: While the "Device and media controls" standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the "Accountability and data backup" implementation specification as addressable to provide more flexibility in

SECTION 10

Policy Number: 10.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Policy on Data and Applications Criticality Analysis

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
- ❑ A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies and during normal business operations.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

Procedures

- ❑ Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ Criticality analysis shall be the responsibility of InO, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- ❑ Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that **SoftServe Inc.** possesses and/or uses to the continuity and success of our operations.
- ❑ The most critical data and applications shall be given the given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- ❑ In conducting data and applications analyses, InO shall employ the technical guidance and recommendations of the National Institute of Standards and Technology ("NIST"), and/or other information technology "best practices", as appropriate.
- ❑ ISMS team shall fully document all analyses of the relative criticality of both data and applications, in accordance with our Documentation Policy and the requirements of HIPAA.

Strategy

If the event occurs at **SoftServe** office(s), which may interrupt critical business functions, primarily delivery of services to the **SoftServe** customers, for period longer than 7 days, designated business functions will need to be performed from alternate location(s) or by alternate personnel.

Scope

Business Continuity/Disaster Recovery Plan covers (BCP) restoration of company business operations in following **Interruption Events**:

- □ **Loss of one or several corporate sites**. Such events might occur via severe structural damage of the buildings, where they reside. This covers partial or full destruction of company assets located within these buildings. Alternatively, Development Center might be considered lost by actions preventing company staff from entering the premises, e.g.: hostile takeover of facilities, legal action resulting in office seizure, etc.
- □ **Unavailability of one or several corporate sites.** This may be caused by extended unavailability of critical utility or communication services, like electrical power, water and plumbing, heating, telecommunications, etc. It is assumed that such event do not damage company assets and they can be used for immediate recovery actions
- □ **Loss of Data Center**
- □ **Unavailability of Data Center.**
- □ **Loss of personnel.** Such event may occur together with loss of site and results in death, injuries or extended sickness of company personnel.

Assumptions

- □ Business Continuity/Disaster Recovery Plan is prepared to address high impact residual risks. BCP does not describe risk mitigation actions introduced into daily company operations, like backup Internet channels for Development and Data Center, redundant power supply for the buildings, deployed emergency power generators, that is risk controls continuously operated by the company.
- □ Business Continuity/Disaster Recovery Plan does not address country-level events.
- □ Corporate representative offices and U.S. headquarters do not constitute critical assets in terms of business continuity. In the event of loss or unavailability of our US offices, phone and email connectivity will be rerouted to European headquarters and handled by Ukraine-based personnel.
- □ Climate in Ukraine is mostly temperate continental, with low risks of major natural disasters, such as hurricanes, floods or tornadoes that cause serious damages to the facilities. Known climate events in the cities affected power supply lines, which have recovery time within 1-2 days.
- □ Ukraine is not on a major fault line, and therefore does not experience earthquakes or volcano eruptions.

Organization

BCP Documentation

SoftServe Business Continuity/Disaster Recovery Plan consists of following standalone documents, which are executed if Interruption Event(s) occur:

- □ **Emergency Response Team Organization**
- □ **Business Continuity Plan** for each **Interruption Event (IE BCP)**, like loss of Lviv4 or Dnipro2 office or unavailability of Data Center at Lviv1.
- □ **Building Evacuation Plans (BEPs)** for each of **SoftServe** offices. Evacuation plans include floor plans provided by respective building owner.

BCP Phases

Initial Response Phase

The Initial Response phase begins as soon as an **Initial Response Team (IRT)** member is informed of an interruption event that has occurred, or is about to occur. It ends when the IRT:

- □ Determines that the event does not pose a threat to critical functions, or
- □ Decides to notify the **Emergency Response Team (ERT)**.

Assessment Phase

The Assessment Phase begins as soon as the ERT is notified of an event. It ends when the predetermined threshold of a disaster situation has been met or the Executive Emergency Management Teams (EEMT) agrees to declare a disaster and begin the **Emergency Declaration Phase**.

Emergency Declaration Phase

The **Emergency Declaration Phase** begins when the ERT determines that the event will impact critical function processing and that it is necessary to activate emergency action plans. When the ERT decides to declare an Emergency, it must also establish the Level of the Emergency. There are three levels:

Level 1: Maintain operations at primary site, alert teams, continue to monitor event impact and prepare for possible relocation.

Level 2: Relocate Level 2 Critical functions to Alternate Site, continue other operations at primary site, continue to monitor event impact and prepare for possible Level 3 declaration.

Level 3: Relocate all Critical functions to Alternate Site.

During the Emergency Declaration Phase all parties involved in the emergency action plans are contacted and mobilized, and begin to activate the emergency procedures in their respective plans. The Emergency Declaration Phase is complete when the interruption event has either been terminated by the ERT or all critical functions have been relocated to their Alternate Site.

Recovery Site Preparation and Systems Restoration Phase

The **Recovery Site Preparation Phase** activities include:

- All activities required to prepare the Alternate Site(s) for the mission critical functions that are being relocated from their primary site(s).
- All activities required to restore all designated data processing systems, functions and facilities that are required to support mission critical business functions.

The phase begins when the Recovery Site Support Teams and Data Center Recovery Teams arrive at the recovery site and ends when:

- All designated recovery site preparations have been completed
- All designated critical systems have been restored, restarted and turned over to the business functions they support.

Relocation Phase

The **Relocation Phase** begins as soon as all recovery site preparations have been completed. It ends as soon as all mission critical business function teams have been transported and have arrived at the recovery site. Relocation Phase activities Include:

- Communicating and coordinating transportation arrangements for the critical business functions teams
- Meeting the teams as they arrive and directing them to the designated recovery work spaces

Business Functions Start-up Phase

The **Business Functions Start-up Phase** begins when critical systems have been recovered and there are enough critical business function team employees at the recovery site(s) to begin the highest priority operations. It ends when the recovery site(s) are adequately staffed to support the all mission critical business functions. Activities include:

- Validation of restored systems' functionality and data integrity
- Evaluation of data recovery point and determining any data loss
- Controlled restart of business function operations

Remain at the Recovery Site(s) Phase

In the event that a multiple-day stay at the recovery site(s) is required, there are actions that must be taken due to this extended stay. This phase begins at the beginning of the second day of operations at the recovery site(s). It ends as soon as the ERT declares that the primary site is ready to be reoccupied and the decision to return to the primary site has been made.

Return to Primary Site Phase

This phase begins when the ERT makes the decision to return to the primary site. It ends as soon as full operations have been re-established at the primary site.

Testing

SoftServe BCP testing and validation is performed for each IE BCP independently. Each IE BCP should be tested/revised on annual basis.

BCP testing is performed using following methodologies:

- □ **Table-top** (structured walk-through) test for Emergency Response Team, validating organizational readiness and identifying potential gaps or show-stoppers;
- □ **Technical test** (only for Data Center IE BCP), performed by IT to validate critical system recovery procedures;
- □ **Evacuation drill** (orientation test) for building loss related IEs to verify personnel awareness.

BCP testing is scheduled year ahead in the way to create minimal disruption for company business operations.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:

    1.

        i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

        ii. *Implementation specifications*:

            A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

            B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

            C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

            D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

    2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

3.

i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. *Implementation specifications*:

A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4.

i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. *Implementation specifications*:

A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

ii. *Implementation specifications*. Implement:

A. *Security reminders* (Addressable). Periodic security updates.

B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

   i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

   ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

   i. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

   ii. *Implementation specifications*:

      A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

      B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

      C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

      D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

      E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Contingency Plan (§ 164.308(a)(7)

We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

Contingency Plan (§ 164.308(a)(7)

Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption. The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Policy Number: 10.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Audit Controls Policy

Assumptions

- □ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- □ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).
- □ The establishment and implementation of an effective audit controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to establish and maintain appropriate and effective audit controls in full compliance with the requirements of HIPAA.
- □ Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with GRC Analyst who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- □ Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- □ It is the Policy of **SoftServe Inc.** to fully document all audit control-related activities and efforts, in accordance with our Documentation Policy.

Procedures

Preparation

Lead Auditor initiates internal Audit.

Controls for Audit are chosen and filled in document ISMS DOC 1.1A Audit Control Readiness by Auditors.

- □ GRC Analyst send opening e-mail to all Auditors to inform about start of Internal Audit (or next Phase of Internal Audit).

- □ GRC Analyst plan Internal Audit actions and prepare expected Audit Plan.
- □ GRC Analyst contacts Auditors to agree a mutually convenient date(s) for the audit and to discuss the scope of the audit.
- □ GRC Analyst generates questions regarding chosen controls and forms Audit Checklist.

Audit Plan is created by GRC Analyst approved by Lead Auditor and communicated to all Auditors.

GRC Analyst creates audit Checklist.

Execution

- □ GRC Analyst addresses all questions defined in Audit Checklist and makes appropriate comments.
- □ GRC Analyst collects findings through interviews, examination of documents and observation of activities and conditions in the areas of concern. Evidence suggesting other non-conformances are noted if they seem significant, even though not covered by the checklist. Other objective evidence and/or observations that may reflect positively or negatively on the information security management system are also listed on the space provided for on the above-mentioned checklists.

GRC Analyst updates checklist regarding comments, evidences and findings.

Reporting

- □ GRC Analyst reviews and analyses all findings and evidences.
- □ GRC Analyst creates Non-conformances in SDE system and address them to appropriate responsible persons (according to ISMS DOC 1.2 Corrective and Preventive Action).
- □ GRC Analyst prepares an Audit Report.
- □ GRC Analyst send closing e-mail to all Auditors to inform about finalization of Internal Audit (or current Phase of Internal Audit).

Audit Report (ISMS DOC 1.6 Audit Report) is set on DMS by GRC Analyst.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
   2. *Implementation specifications*:
      - i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
      - ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
      - iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
      - iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

b. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

We proposed five technical security services requirements with supporting implementation features: Access control; **Audit controls**; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; **Audit trails**; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, **audit controls**, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity.

We adopt this requirement in this final rule.

Access Control (§ 164.312(a)(1))

Comment: We received a comment stating that "Audit controls" should be an implementation feature rather than the standard, and suggesting that we change the title of the standard to "Accountability," and provide additional detail to the audit control implementation feature.

Response: We do not adopt the term "Accountability" in this final rule because it is not descriptive of the requirement, which is to have the capability to record and examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security

Comment: One commenter recommended that this final rule state that audit control mechanisms should be implemented based on the findings of an entity's risk assessment and risk analysis. The commenter asserted that audit control mechanisms should be utilized only when appropriate and necessary and should not adversely affect system performance.

Response: We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care.

Comment: One commenter was concerned about the interplay of State and Federal requirements for auditing of privacy data and requested additional guidance on the interplay of privacy rights, laws, and the expectation for audits under the rule.

Response: In general, the security standards will super cede any contrary provision of State law. Security standards in this final rule establish a minimum level of security that covered entities must meet. We note that other Federal law to adhere to additional, or more stringent security measures may require covered entities. Section 1178(a)(2) of the statute provides several exceptions to this general rule. With regard to protected health information, the preemption of State laws and the relationship of the Privacy Rule to other Federal laws is discussed in the Privacy Rule beginning at 65 FR 82480; the preemption provisions of the rule are set out at 45 CFR part 160, subpart B.

It should be noted that although the Privacy Rule does not incorporate a requirement for an "audit trail" function, it does call for providing an accounting of certain disclosures of protected health information to an individual upon request. There has been a tendency to assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule's requirement for an audit capability will satisfy the Privacy Rule's requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).

Policy Number: 10.2

Effective Date: 3/26/2013

Last Revised: 7/29/2014

Data Transmission Security Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to data transmission security, in accordance with the requirements at § 164.312(e)(1) and § 164.312(e)(2).
- ❑ The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- ❑ The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to establish and implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of these Data Transmission Security Procedures shall reside with GRC Analyst, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific Data Transmission Security Procedures shall be developed to protect individually identifiable health information, including Electronic Protected Health Information ("EPHI", as defined by HIPAA).
- ❑ It is the Policy of **SoftServe Inc.** to fully document all Data Transmission Security Procedures, activities, and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

Classification

All information assets are clearly identified, and an inventory of all important assets has been drawn up and is maintained in line with the requirements of ISMS DOC 8.2 Asset Inventory & Ownership. Their owners review the classifications of information assets annually and if the classification level can be reduced, it will be. The asset owner also is responsible for declassifying information.

Information received from outside the Organization is re-classified by its recipient so that (within the Organization), it complies with this procedure. Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it should be destroyed.

SoftServe's information assets are classified accordingly to five levels of classification (top secret, secret, confidential, internal and public):

Top Secret: this classification applies to information that is specifically restricted by the Board of Directors. Top Secret information may include trade secrets, it may include sales and marketing plans, new product plans, and notes associated with patentable inventions.

- ❑ Information with Top Secret level is available and/or should be distributed only to defined list of people within organization who has been given a top secret security clearance (according to procedure described in section 3.2 in Personnel Screening Standard) and require exceptional security controls.
- ❑ Such information would cause "exceptionally grave damage" to organization in case of disclosure.
- ❑ Top Secret information sent by e-mail must be encrypted and digitally signed, in line with the ISMS DOC 10.1 Encryption Policy, and sent only to the e-mail box of the identified recipient.
- ❑ Access provisioning requires "need-to-know" basis.

Disclosure, destruction or loss of integrity of such information lead to **Very High** impact level (section 3.6 of Risk Management Framework).

Secret: this classification applies to information that is specifically restricted by EVP.

- ❑ Such information may include some types of private information, including records of a person's health care, education, and employment may be protected by privacy laws, a person's or organization's financial information that may be considered private if their disclosure might lead to crimes such as identity theft or fraud.
- ❑ Unauthorized disclosure of private information that can make the perpetrator liable for civil remedies and may in some cases be subject to criminal penalties.
- ❑ Secret information would cause "serious damage" to organization in case of disclosure.

- ❑ Secret information sent by e-mail must be encrypted and digitally signed, in line with the ISMS DOC 10.1 Encryption Policy, and sent only to the e-mail box of the identified recipient.
- ❑ Access provisioning requires "need-to-know" basis.

"Secret" information disclosure, destruction or loss of integrity could cause **High** impact level (section 3.6 of Risk Management Framework).

Confidential: this classification applies to information that is specifically restricted by SBU Manager.

- ❑ Information that falls into this category must be marked 'Confidential' includes business information or personal data collected by the organization that is subject to special protection and may not be routinely shared with anyone inside or outside of the business.
- ❑ Confidential material would cause "damage" or be "prejudicial" to organization in case of disclosure.
- ❑ Access provisioning requires "need-to-know" basis.

Disclosure, destruction or loss of integrity of "Confidential" information could cause **Medium** impact (section 3.6 of Risk Management Framework)**.**

Internal: information of this category is restricted for authorized employees/staff.

- ❑ Internal material would cause "undesirable effects" to organization in case of disclosure.
- ❑ Internal information includes business information that is not subjected to special protection and may be routinely shared with anyone inside the business.

Disclosure, destruction or loss of integrity of information classified as "Internal" could cause **Low** or **Very Low** impact (section 3.6 of Risk Management Framework).

Public: this is information which can be released outside the organization.

- This refers to information that is already or could be a matter of public record or knowledge. Those without security clearance can view such documents.

Disclosure, destruction or loss of integrity of such kind of information could not cause impact on business.

Labeling

Proper labeling enables all parties to correlate the information with appropriate information handling guidelines. The key of effective labeling is ensuring that a person with access to information is aware of its classification and what restrictions exist in the release or handling of the information.

Electronic information might be stored in Systems and Objects. Electronic information should be labeled in object(s) level. In case it is impossible the whole system should be classified.

Systems include but not limited to: 1C, SSE, SSP, TM, Head Accountant, HRMS (TMS, LMS, WMS, CMS, BMC, CRM, DB's, etc.

Objects include but not limited to: Microsoft Office documents (Word, Excel, etc.), Confluence page, E-mail, etc.

Stored information, both physical and electronic, must be labeled in accordance with Classification above. All the information with no labels is deemed Confidential.

System is deemed classified according to the highest classification of information stored. Warning screens are used during log in into systems.

Predefined templates (ISMS DOC 8.8.1 Templates for classified information) shall be employed.

If predefined templates are not used:

- ❑ The classification level should be included to all pages of the document
- ❑ Label font size should be larger than plain text and be highlighted with colored label title: Dark Red for Top Secret, Red for Secret, Yellow for Internal, Green for Public (where possible)
- ❑ Hardcopy documents that do not have text labels are marked by addition of a physical, stick-on label or marked with either rubber stamps or markers of appropriate content and color (where possible).
- ❑ Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) should be labelled with appropriate classification level mark.

Information is downgraded or upgraded after approve of appropriate Information Asset Owner based on Risk Acceptance Procedure. VP Marketing must also approve all information downgraded to level of classification Public. Classified information that is downgraded or upgraded should be promptly marked to indicate the change with date and signature (hard copy) or electronic message (system, object).

Handling

The Organization’s information assets should be handled in a manner to protect the information assets from unauthorized or accidental disclosure, modification or loss. All information assets should be processed and stored in accordance with information assets classification levels assigned in order to protect the confidentiality, integrity and availability.

- ❑ Information assets can only be handled by individuals that have appropriate authorization or on facilities that shall not be visible to the public when not in use to prevent disclosure and theft, for example leaving a laptop with confidential data visible in a vehicle.
- ❑ Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls specified in ISMS DOC 11.10 Equipment Security Standard, and are protected appropriately while being recorded.
- ❑ Agreements with external organizations (see ISMS DOC 15.1 Supplier Relationship Policy), which include information sharing, include a matrix for translating their security classifications into classifications applicable to **SoftServe**.
- ❑ Creator of information ensures that appropriate measures are taken to classified information accordingly to requirements of ISMS DOC 13.3 Information Transfer Policy, ISMS DOC 8.7 Removable media, ISMS DOC 8.10 Information Storage, Disposal and Retention Policy, ISMS DOC 11.19 Clear Screen and Clear Desk Policy.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
    1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
    2. *Implementation specifications*:
        - i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
        - ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
        - iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

        iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

b. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

c.

    1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
    2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

d. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

e.

    1. *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
    2. *Implementation specifications*:
        i. *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
        ii. *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

Transmission Security (§ 164.312(e)(1))

Under "Technical Security Mechanisms to Guard against Unauthorized Access to Data that is Transmitted over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Transmission Security (§ 164.312(e)(1))

Comment: We received a number of comments asking for overall clarification as well as a definition of terms used in this section. A definition for the term "open networks" was the most requested action, but there was a general expression of dislike for the manner in which we approached this section, with some comments suggesting that the entire section be rewritten. A significant number of comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet, but rather be considered optional based on individual entity risk assessment/analysis. Many comments noted that there are very few known breaches of security over dial-up lines and that non-judicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Only one commenter suggested that "most" external traffic should be encrypted.

Response: In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines.

We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) the alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for

"Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) "integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

Comment: A number of comments were received asking that this final rule establish a specific (or at least a minimum) cryptographic algorithm strength. Others recommended that the rule not specify encryption strength since technology is changing so rapidly. Several commenters requested guidelines and minimum encryption standards for the Internet. Another stated that, since an example was included (small or rural providers for example), the government should feel free to name a specific encryption package. One commenter stated that the requirement for encryption on the Internet should reference the "CMS Internet Security Policy."

Response: We remain committed to the principle of technology neutrality and agree with the comment that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Consistent with this principle, specification of algorithm strength or specific products would be inappropriate. Moreover, rapid advances in the success of "brute force" cryptanalysis techniques suggest that any minimum specification would soon be outmoded. We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength. Because "CMS Internet Security Policy" is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities, we have not referred to it here.

Policy Number: 10.3
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA Documentation Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.

- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for **SoftServe Inc.** must document all HIPAA-related activities that require documentation.
- All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.
- Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by **SoftServe Inc.**
- All HIPAA-related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by **SoftServe Inc.**
- All required HIPAA documentation shall be securely and appropriately maintained and stored in accordance with HIPAA Regulations and with the policies on document retention of **SoftServe Inc.**
- HIPAA documentation shall be made available, as needed, to all workforce members who are authorized to access it, and shall be made available to appropriate authorities for audits, investigations, and other purposes authorized or required by law.

Procedures

Principles

General principles for ISMS documentation:

- Labels must identify the classification of the information contained in the record, the owner of the information and the date it was generated (for hard copy version) how it described in **Section 5: Document Labeling Scheme**.
- The referential documentation should be added to the reference section of the document.
- Where necessary, document can be given serial numbers in respect to the specific process to which they relate.
- The retention period for the record is determined by the organization’s overall approach to document and record retention, as set out in ISMS DOC 15.2.

- Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the ISMS.

  - ISMS Documentation consists of several classes of information entities:

- Actual documents, used to keep and disseminate knowledge in form of policies, standards, regulations, practices, guides, how-to's, etc.
- Item registers, used for storing inventory information about assets (hardware, software, people, processes, locations, configuration items, etc.)
- Event records, used for recording incidents, requests, feedbacks, etc.

Each of above classes requires different process of creation, updating, dissemination, which may need automation for improving efficiency and accuracy in handling information. Considering existing company practices and infrastructure for automating information handling, ISMS documentation will be split between several systems:

- Documents will be managed using corporate Confluence Content Management System (CMS)

Training records will be managed using corporate Training Management System **(Link TBD)**

Document Structure

All ISMS documents contain following mandatory sections:

- Change history (shown only in PDF/print form)
- Contents (Scope, Responsibilities, Procedure)
- Document Owner and Approval section. The owner and approval of the document who issued and is responsible for keeping it up to date, needs to be identified – by role, not by name.
- References - containing list of external references or attachments
- Distribution - listing all people that must be informed about this document

Using Confluence mechanisms all these sections are maintained automatically, where **References** section lists other Confluence pages referenced by current and files attached, **Distribution** - showing people "watching" this page.

Document Labeling Scheme

> ✓ We should define what labels will be used and to what exact purpose within ISMS Document Management System. E.g. we might mark all policies with "policy" label to be able to process all such pages

ISMS Documentation toolkit defines following document classes:

- ❑ Policy
- ❑ Procedure
- ❑ Instruction
- ❑ Record

We used **policy**, **procedure**, **instruction, record** labels to mark document as belonging to appropriate category.

Additional labels are used throughout ISMS space to mark following information:

- ❑ Labels in form **a_<X>_<Y>** mark document related to appropriate ISO27001 control. This labels aggregated in ISMS DOC 4.6 Statement of Applicability
- ❑ Labels in form "resp_isd" mark documents describing respective corporate role responsibility in Information Security implementation.
- ❑ Labels in form "raci_isd_a" mark role that approves respective document, "raci_ismsm_o" mark role owning respective document. This labels aggregated in ISMS DOC 2.4 Approvers and Responsible person's document and duplicates information presented in ***Document Owner and Approval*** section of document and reflects ISMS RACI Matrix.
- ❑ Labels **Top Secret (TS),** Secret**,** Confidential, Restricted and **Public** were used to mark document as belonging to appropriate Level of(ISMS DOC 7.6)

ISMS labels should be seeded using technique described here.

Authorization levels

The organization has clearly defined authorization levels, which cannot be delegated.

The board of directors has ultimate authority over the information security policy and ISMS and approves and authorizes all changes to the information security policy (ISMS DOC 5.1 Information Security Policy) and any separate policy statements (ISMS DOC 6.2 Information Security Coordination and ISMS DOC 18.6 Data Protection and Privacy Policy).

The CISO (see section 5.1 of ISMS DOC 6.2) has lead executive authority for information security to approve, authorize and issue all documents according to ISMS DOC 2.4 Approvers and Responsible persons.

The Information Security Director and all Heads of Department/Divisional/Function approve and authorize documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by Heads of Department/Divisional/Function have to be approved and authorized by the CISO.

Owners of information assets (see section 5.4 of ISMS DOC 6.2 and ISMS DOC 7.1 Asset Inventory & Ownership) are responsible for the security classification of their asset(s), the day-to-day protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

- The individual has the necessary skill, competence and resources to carry out the processes or task(s) and
- The Owner retains accountability for ensuring that the process or task is carried out correctly.

Access rights are specified in ISMS DOC 11.1 Access Control and ISMS DOC 11.2 Access Control Rules & Rights and ISMS DOC 11.3 User Access Management. Access rights are personal, are set out in individual User Agreements (ISMS DOC 8.11 Individual User Agreement and ISMS DOC 11.19 Clear Desk and Clear Screen Policy , DOC 11.13) and cannot be delegated.

Document approval workflows

Ad hoc Workflows plugin is used to automate page approval process.

Reporting plugin is used together with Ad hoc Workflows Supplier to include workflow state/approval information inside the page and make typical Approval section fully automated and therefore maintainable.

DMS instance is used for preparation and modification of documents requiring formal approval by ISC or company management (Executive, BoD,). After documents are ready, they are published on corporate confluence "large Confluence" as official documents to be followed by entire company. Publishing of finalized documents is automated by Ad hoc Workflows and Remote Publishing plugins.

Using Ad hoc Workflows there are three page states:

- **Draft** - if document is in redaction and is not ready for review;
- **For Review** - when document is ready and should be reviewed by ISMS Manager;
- **CISO review (BOD Review, VP Review)** - when document is approved by ISMS Manager and should be reviewed by CISO (BoD, VP);
- **Published** - this state mean that document is approved by company management and is published on corporate confluence to be followed by entire company.

Reference workflow report (ISMS DOC 2.3 Documents List by State) provides a list of documentation that should be approved by responsible persons. It allows to simplify whole document approval process.

DMS allows tracking of all changes on each page. To view all page activities user should pick "Page Activity" from "Tools" drop down menu. This activity list shows additions and edits done by appropriate person and activities with statuses done by approvers or redactors.

Terms

Important terms used in ISMS documents should be defined using Glossary page. It creates hidden separate pages. This way, hierarchy of pages containing terms definitions does not "pollute" actual document space and does not show in built-in page hierarchy view on the left.

All Important terms used in ISMS documents have appropriate references on Glossary.

Technical details

- □ If we use macros insert _in the ISMS document, we should note last date of modification near the title of this insertion: **Insertion NAME** (Last modified: 03 January 2013 - 01:06 PM)
- □ All tables and pictures contained in the ISMS documents must indicate their name, according to this template: **Table: NAME** and **Picture: NAME**

ISMS Documents Change Management

- □ Changes to ISMS policies and procedures (including updating, withdrawal or replacement) must be authorized in line with the requirements of section 6 of this document.
- □ All changes are subject to, and a consequence of, a change in the risk assessment.
- □ Where possible, records should be stored electronically and be readily accessible. Records are to be stored securely according to the relevant classification.
- □ Storage areas shall minimize unauthorized access. Only personnel responsible for these records may remove records from the storage area.
- □ Removal of ISMS records from the vicinity of the storage area shall be documented on log.
- □ Records should be destroyed at the end of their retention period. A ISMS document destruction shall be authorized by ISMS Manager

HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:

- □ Maintain written or electronic copies of communications that the Rules require to be in writing.
- □ Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.
- □ Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.
- □ Note: The six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

HIPAA Documentation includes the following:

- □ HIPAA Policies and Procedures.
- □ HIPAA Risk Analysis and related notes and research materials
- □ Policies and Procedures for minimum necessary uses by your work force.
- □ Accounting documentation which includes…
  - Information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures; description, etc.);
  - the written accounting that is provided to the individual; and

- the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals

❑ Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.

❑ All complaints received and their disposition, if any.

❑ All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.

❑ The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.

❑ Training provided (i.e., topics, dates, and, ideally, participants).

❑ Sanctions imposed against non-complying work force members.

❑ All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.

❑ The methods and results of analyses that justify release of de-identified information.

❑ Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.

❑ Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.

❑ The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.

❑ All signed authorizations and revocations.

❑ All approved confidential communication requests and terminations or revocations.

Policy Number: 10.4
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA Documentation Availability Policy

Assumptions

❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations concerned with the availability of HIPAA-related documentation, in accordance with the HIPAA requirements at § 164.310, § 164.316, and § 164.530(j), among others.

❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.

❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.

❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.

- □ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- □ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- □ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- □ Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to make all HIPAA-related documentation available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains.
- □ All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation, or who require such documentation in the performance of their work-related duties.
- □ Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
- □ No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

Procedures

Principles

General principles for ISMS documentation:

- □ Labels must identify the classification of the information contained in the record, the owner of the information and the date it was generated (for hard copy version) how it described in **Section 5: Document Labeling Scheme**.
- □ The referential documentation should be added to the reference section of the document.
- □ Where necessary, document can be given serial numbers in respect to the specific process to which they relate.
- □ The retention period for the record is determined by the organization's overall approach to document and record retention, as set out in ISMS DOC 15.2.
- □ Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or

the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the ISMS.

ISMS Documentation consists of several classes of information entities:

- Actual documents, used to keep and disseminate knowledge in form of policies, standards, regulations, practices, guides, how-to's, etc.
- Item registers, used for storing inventory information about assets (hardware, software, people, processes, locations, configuration items, etc.)
- Event records, used for recording incidents, requests, feedbacks, etc.

Each of above classes requires different process of creation, updating, dissemination, which may need automation for improving efficiency and accuracy in handling information. Considering existing company practices and infrastructure for automating information handling, ISMS documentation will be split between several systems:

- Documents will be managed using corporate Confluence Content Management System (CMS)

Training records will be managed using corporate Training Management System.

Document Structure

All ISMS documents contain following mandatory sections:

- Change history (shown only in PDF/print form)
- Contents (Scope, Responsibilities, Procedure)
- Document Owner and Approval section. The owner and approval of the document who issued and is responsible for keeping it up to date, needs to be identified – by role, not by name.
- References - containing list of external references or attachments
- Distribution - listing all people that must be informed about this document

Using Confluence mechanisms all these sections are maintained automatically, where **References** section lists other Confluence pages referenced by current and files attached, **Distribution** - showing people "watching" this page.

Document Labeling Scheme

✓ We should define what labels will be used and to what exact purpose within ISMS Document Management System. E.g. we might mark all policies with "policy" label to be able to process all such pages

ISMS Documentation toolkit defines following document classes:

- □ Policy
- □ Procedure
- □ Instruction
- □ Record

We used **policy**, **procedure**, **instruction, record** labels to mark document as belonging to appropriate category.

Additional labels are used throughout ISMS space to mark following information:

- □ Labels in form **a_<X>_<Y>** mark document related to appropriate ISO27001 control. This labels aggregated in ISMS DOC 4.6 Statement of Applicability
- □ Labels in form "resp_isd" mark documents describing respective corporate role responsibility in Information Security implementation.
- □ Labels in form "raci_isd_a" mark role that approves respective document, "raci_ismsm_o" mark role owning respective document. This labels aggregated in ISMS DOC 2.4 Approvers and Responsible person's document and duplicates information presented in ***Document Owner and Approval*** section of document and reflects ISMS RACI Matrix.
- □ Labels **Top Secret (TS),** Secret**,** Confidential, Restricted and **Public** were used to mark document as belonging to appropriate Level of(ISMS DOC 7.6)

ISMS labels should be seeded using technique described here.

Authorization levels

The organization has clearly defined authorization levels, which cannot be delegated.

The board of directors has ultimate authority over the information security policy and ISMS and approves and authorizes all changes to the information security policy (ISMS DOC 5.1 Information Security Policy) and any separate policy statements (ISMS DOC 6.2 Information Security Coordination and ISMS DOC 18.6 Data Protection and Privacy Policy).

The CISO (see section 5.1 of ISMS DOC 6.2) has lead executive authority for information security to approve, authorize and issue all documents according to ISMS DOC 2.4 Approvers and Responsible persons.

The Information Security Director and all Heads of Department/Divisional/Function approve and authorize documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by Heads of Department/Divisional/Function have to be approved and authorized by the CISO.

Owners of information assets (see section 5.4 of ISMS DOC 6.2 and ISMS DOC 7.1 Asset Inventory & Ownership) are responsible for the security classification of their asset(s), the day-to-day protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

- □ The individual has the necessary skill, competence and resources to carry out the processes or task(s) and
- □ The Owner retains accountability for ensuring that the process or task is carried out correctly.

Access rights are specified in ISMS DOC 11.1 Access Control and ISMS DOC 11.2 Access Control Rules & Rights and ISMS DOC 11.3 User Access Management. Access rights are personal, are set out in individual User Agreements (ISMS DOC 8.11 Individual User Agreement and ISMS DOC 11.19 Clear Desk and Clear Screen Policy , DOC 11.13) and cannot be delegated.

Document approval workflows

Ad hoc Workflows plugin is used to automate page approval process.

Reporting plugin is used together with Ad hoc Workflows Supplier to include workflow state/approval information inside the page and make typical Approval section fully automated and therefore maintainable.

DMS instance is used for preparation and modification of documents requiring formal approval by ISC or company management (Executive, BoD,). After documents are ready, they are published on corporate confluence "large Confluence" as official documents to be followed by entire company. Publishing of finalized documents is automated by Ad hoc Workflows and Remote Publishing plugins.

Using Ad hoc Workflows there are three page states:

- □ **Draft** - if document is in redaction and is not ready for review;
- □ **For Review** - when document is ready and should be reviewed by ISMS Manager;
- □ **CISO review (BOD Review, VP Review)** - when document is approved by ISMS Manager and should be reviewed by CISO (BoD, VP);
- □ **Published** - this state mean that document is approved by company management and is published on corporate confluence to be followed by entire company.

Reference workflow report (ISMS DOC 2.3 Documents List by State) provides a list of documentation that should be approved by responsible persons. It allows to simplify whole document approval process.

DMS allows tracking of all changes on each page. To view all page activities user should pick "Page Activity" from "Tools" drop down menu. This activity list shows additions and edits done by appropriate person and activities with statuses done by approvers or redactors.

Terms

Important terms used in ISMS documents should be defined using Glossary page. It creates hidden separate pages. This way, hierarchy of pages containing terms definitions does not "pollute" actual document space and does not show in built-in page hierarchy view on the left.

All Important terms used in ISMS documents have appropriate references on Glossary.

Technical details

- □ If we use macros insert _in the ISMS document, we should note last date of modification near the title of this insertion: **Insertion NAME** (Last modified: 03 January 2013 - 01:06 PM)
- □ All tables and pictures contained in the ISMS documents must indicate their name, according to this template: **Table: NAME** and **Picture: NAME**

ISMS Documents Change Management

- □ Changes to ISMS policies and procedures (including updating, withdrawal or replacement) must be authorized in line with the requirements of section 6 of this document.
- □ All changes are subject to, and a consequence of, a change in the risk assessment.
- □ Where possible, records should be stored electronically and be readily accessible. Records are to be stored securely according to the relevant classification.
- □ Storage areas shall minimize unauthorized access. Only personnel responsible for these records may remove records from the storage area.
- □ Removal of ISMS records from the vicinity of the storage area shall be documented on log.
- □ Records should be destroyed at the end of their retention period. A ISMS document destruction shall be authorized by ISMS Manager

HIPAA Rules require that Covered Entities and Business Associates maintain their policies and procedures in written or electronic form, as well as the following:

- □ Maintain written or electronic copies of communications that the Rules require to be in writing.
- □ Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.
- □ Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.
- □ Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

HIPAA Documentation includes the following:

- □ HIPAA Policies and Procedures.
- □ HIPAA Risk Analysis and related notes and research materials
- □ Policies and Procedures for minimum necessary uses by your work force.
- □ Accounting documentation which includes…
  - Information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures; description, etc.);
  - the written accounting that is provided to the individual; and
  - the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals

- □ Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
- □ All complaints received and their disposition, if any.
- □ All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.
- □ The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
- □ Training provided (i.e., topics, dates, and, ideally, participants).
- □ Sanctions imposed against non-complying work force members.
- □ All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
- □ The methods and results of analyses that justify release of de-identified information.
- □ Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.
- □ Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
- □ The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
- □ All signed authorizations and revocations.
- □ All approved confidential communication requests and terminations or revocations.

Policy Number: 10.5
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA Documentation Retention Policy

Assumptions

- □ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- □ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- □ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- □ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- □ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- □ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-

191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

- ❑ Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.
- ❑ HIPAA documentation shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
- ❑ HIPAA documentation shall be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards.

Procedures

Principles

General principles for ISMS documentation:

- ❑ Labels must identify the classification of the information contained in the record, the owner of the information and the date it was generated (for hard copy version) how it described in **Section 5: Document Labeling Scheme**.
- ❑ The referential documentation should be added to the reference section of the document.
- ❑ Where necessary, document can be given serial numbers in respect to the specific process to which they relate.
- ❑ The retention period for the record is determined by the organization’s overall approach to document and record retention, as set out in ISMS DOC 15.2.
- ❑ Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the ISMS.

ISMS Documentation consists of several classes of information entities:

- ❑ Actual documents, used to keep and disseminate knowledge in form of policies, standards, regulations, practices, guides, how-to's, etc.
- ❑ Item registers, used for storing inventory information about assets (hardware, software, people, processes, locations, configuration items, etc.)
- ❑ Event records, used for recording incidents, requests, feedbacks, etc.

- ❑ Each of above classes requires different process of creation, updating, dissemination, which may need automation for improving efficiency and accuracy in handling information. Considering existing company practices and infrastructure for automating information handling, ISMS documentation will be split between several systems:

- □ Documents will be managed using corporate Confluence Content Management System (CMS)

Training records will be managed using corporate Training Management System **(Link TBD)**

Document Structure

All ISMS documents contain following mandatory sections:

- □ Change history (shown only in PDF/print form)
- □ Contents (Scope, Responsibilities, Procedure)
- □ Document Owner and Approval section. The owner and approval of the document who issued and is responsible for keeping it up to date, needs to be identified – by role, not by name.
- □ References - containing list of external references or attachments
- □ Distribution - listing all people that must be informed about this document

Using Confluence mechanisms all these sections are maintained automatically, where **References** section lists other Confluence pages referenced by current and files attached, **Distribution** - showing people "watching" this page.

Document Labeling Scheme

✓ We should define what labels will be used and to what exact purpose within ISMS Document Management System. E.g. we might mark all policies with "policy" label to be able to process all such pages

ISMS Documentation toolkit defines following document classes:

- □ Policy
- □ Procedure
- □ Instruction
- □ Record

We used **policy**, **procedure**, **instruction, record** labels to mark document as belonging to appropriate category.

Additional labels are used throughout ISMS space to mark following information:

- □ Labels in form **a_<X>_<Y>** mark document related to appropriate ISO27001 control. This labels aggregated in ISMS DOC 4.6 Statement of Applicability
- □ Labels in form "resp_isd" mark documents describing respective corporate role responsibility in Information Security implementation.

- Labels in form "raci_isd_a" mark role that approves respective document, "raci_ismsm_o" mark role owning respective document. This labels aggregated in ISMS DOC 2.4 Approvers and Responsible person's document and duplicates information presented in ***Document Owner and Approval*** section of document and reflects ISMS RACI Matrix.
- Labels **Top Secret (TS), Secret, Confidential, Restricted and Public** were used to mark document as belonging to appropriate Level of(ISMS DOC 7.6)

ISMS labels should be seeded using technique described here.

Authorization levels

The organization has clearly defined authorization levels, which cannot be delegated.

The board of directors has ultimate authority over the information security policy and ISMS and approves and authorizes all changes to the information security policy (ISMS DOC 5.1 Information Security Policy) and any separate policy statements (ISMS DOC 6.2 Information Security Coordination and ISMS DOC 18.6 Data Protection and Privacy Policy).

The CISO (see section 5.1 of ISMS DOC 6.2) has lead executive authority for information security to approve, authorize and issue all documents according to ISMS DOC 2.4 Approvers and Responsible persons.

The Information Security Director and all Heads of Department/Divisional/Function approve and authorize documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by Heads of Department/Divisional/Function have to be approved and authorized by the CISO.

Owners of information assets (see section 5.4 of ISMS DOC 6.2 and ISMS DOC 7.1 Asset Inventory & Ownership) are responsible for the security classification of their asset(s), the day-to-day protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

- The individual has the necessary skill, competence and resources to carry out the processes or task(s) and
- The Owner retains accountability for ensuring that the process or task is carried out correctly.

Access rights are specified in ISMS DOC 11.1 Access Control and ISMS DOC 11.2 Access Control Rules & Rights and ISMS DOC 11.3 User Access Management. Access rights are personal, are set out in individual User Agreements (ISMS DOC 8.11 Individual User Agreement and ISMS DOC 11.19 Clear Desk and Clear Screen Policy , DOC 11.13) and cannot be delegated.

Document approval workflows

Ad hoc Workflows plugin is used to automate page approval process.

Reporting plugin is used together with Ad hoc Workflows Supplier to include workflow state/approval information inside the page and make typical Approval section fully automated and therefore maintainable.

DMS instance is used for preparation and modification of documents requiring formal approval by ISC or company management (Executive, BoD,). After documents are ready, they are published on corporate confluence "large Confluence" as official documents to be followed by entire company. Publishing of finalized documents is automated by Ad hoc Workflows and Remote Publishing plugins.

Using Ad hoc Workflows there are three page states:

- ❑ **Draft** - if document is in redaction and is not ready for review;
- ❑ **For Review** - when document is ready and should be reviewed by ISMS Manager;
- ❑ **CISO review (BOD Review, VP Review)** - when document is approved by ISMS Manager and should be reviewed by CISO (BoD, VP);
- ❑ **Published** - this state mean that document is approved by company management and is published on corporate confluence to be followed by entire company.

Reference workflow report (ISMS DOC 2.3 Documents List by State) provides a list of documentation that should be approved by responsible persons. It allows to simplify whole document approval process.

DMS allows tracking of all changes on each page. To view all page activities user should pick "Page Activity" from "Tools" drop down menu. This activity list shows additions and edits done by appropriate person and activities with statuses done by approvers or redactors.

Terms

Important terms used in ISMS documents should be defined using Glossary page. It creates hidden separate pages. This way, hierarchy of pages containing terms definitions does not "pollute" actual document space and does not show in built-in page hierarchy view on the left.

All Important terms used in ISMS documents have appropriate references on Glossary.

Technical details

- ❑ If we use macros insert _in the ISMS document, we should note last date of modification near the title of this insertion: **Insertion NAME** (Last modified: 03 January 2013 - 01:06 PM)
- ❑ All tables and pictures contained in the ISMS documents must indicate their name, according to this template: **Table: NAME** and **Picture: NAME**

ISMS Documents Change Management

- Changes to ISMS policies and procedures (including updating, withdrawal or replacement) must be authorized in line with the requirements of section 6 of this document.

- □ All changes are subject to, and a consequence of, a change in the risk assessment.
- □ Where possible, records should be stored electronically and be readily accessible. Records are to be stored securely according to the relevant classification.
- □ Storage areas shall minimize unauthorized access. Only personnel responsible for these records may remove records from the storage area.
- □ Removal of ISMS records from the vicinity of the storage area shall be documented on log.
- □ Records should be destroyed at the end of their retention period. A ISMS document destruction shall be authorized by ISMS Manager

HIPAA Rules require that Covered Entities and Business Associates maintain their policies and procedures in written or electronic form, as well as the following:

- □ Maintain written or electronic copies of communications that the Rules require to be in writing.
- □ Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.
- □ Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.
- □ Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

HIPAA Documentation includes the following:

- □ HIPAA Policies and Procedures.
- □ HIPAA Risk Analysis and related notes and research materials
- □ Policies and Procedures for minimum necessary uses by your work force.
- □ Accounting documentation which includes…
  - Information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures, description, etc.);
  - the written accounting that is provided to the individual; and
  - The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
- □ Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
- □ All complaints received and their disposition, if any.
- □ All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.
- □ The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
- □ Training provided (i.e., topics, dates, and, ideally, participants).
- □ Sanctions imposed against non-complying work force members.
- □ All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
- □ The methods and results of analyses that justify release of de-identified information.
- □ Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.

- □ Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
- □ The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
- □ All signed authorizations and revocations.
- □ All approved confidential communication requests and terminations or revocations.

Policy Number: 10.6
Effective Date: 3/26/2013
Last Revised: 7/28/2014

HIPAA Documentation Updating Policy

Assumptions

- □ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- □ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- □ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- □ Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- □ Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- □ The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- □ Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- It is the Policy of **SoftServe Inc.** to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.
- Reviews of HIPAA-related documentation shall be made periodically, but at least every 12 months for the purposes of this policy.
- Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be made by **SoftServe Inc.'s** designated Privacy Officer or HIPAA Officer.
- Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be documented according to **SoftServe Inc.'s** Documentation Policy.

Procedures

Principles

General principles for ISMS documentation:

- Labels must identify the classification of the information contained in the record, the owner of the information and the date it was generated (for hard copy version) how it described in **Section 5: Document Labeling Scheme**.
- The referential documentation should be added to the reference section of the document.
- Where necessary, document can be given serial numbers in respect to the specific process to which they relate.
- The retention period for the record is determined by the organization's overall approach to document and record retention, as set out in ISMS DOC 15.2.
- Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the ISMS.

ISMS Documentation consists of several classes of information entities:

- Actual documents, used to keep and disseminate knowledge in form of policies, standards, regulations, practices, guides, how-to's, etc.
- Item registers, used for storing inventory information about assets (hardware, software, people, processes, locations, configuration items, etc.)
- Event records, used for recording incidents, requests, feedbacks, etc.

Each of above classes requires different process of creation, updating, dissemination, which may need automation for improving efficiency and accuracy in handling information. Considering existing company practices and infrastructure for automating information handling, ISMS documentation will be split between several systems:

- Documents will be managed using corporate Confluence Content Management System (CMS)

Training records will be managed using corporate Training Management System **(Link TBD)**

Document Structure

All ISMS documents contain following mandatory sections:

- Change history (shown only in PDF/print form)
- Contents (Scope, Responsibilities, Procedure)
- Document Owner and Approval section. The owner and approval of the document who issued and is responsible for keeping it up to date, needs to be identified – by role, not by name.
- References - containing list of external references or attachments
- Distribution - listing all people that must be informed about this document

Using Confluence mechanisms all these sections are maintained automatically, where **References** section lists other Confluence pages referenced by current and files attached, **Distribution** - showing people "watching" this page.

Document Labeling Scheme

> ✓ We should define what labels will be used and to what exact purpose within ISMS Document Management System. E.g. we might mark all policies with "policy" label to be able to process all such pages

ISMS Documentation toolkit defines following document classes:

- Policy
- Procedure
- Instruction
- Record

We used **policy**, **procedure**, **instruction, record** labels to mark document as belonging to appropriate category.

Additional labels are used throughout ISMS space to mark following information:

- Labels in form **a_<X>_<Y>** mark document related to appropriate ISO27001 control. This labels aggregated in ISMS DOC 4.6 Statement of Applicability

- Labels in form "resp_isd" mark documents describing respective corporate role responsibility in Information Security implementation.
- Labels in form "raci_isd_a" mark role that approves respective document, "raci_ismsm_o" mark role owning respective document. This labels aggregated in ISMS DOC 2.4 Approvers and Responsible person's document and duplicates information presented in ***Document Owner and Approval*** section of document and reflects ISMS RACI Matrix.
- Labels **Top Secret (TS), Secret, Confidential, Restricted and Public** were used to mark document as belonging to appropriate Level of(ISMS DOC 7.6)

ISMS labels should be seeded using technique described here.

Authorization levels

The organization has clearly defined authorization levels, which cannot be delegated.

The board of directors has ultimate authority over the information security policy and ISMS and approves and authorizes all changes to the information security policy (ISMS DOC 5.1 Information Security Policy) and any separate policy statements (ISMS DOC 6.2 Information Security Coordination and ISMS DOC 18.6 Data Protection and Privacy Policy).

The CISO (see section 5.1 of ISMS DOC 6.2) has lead executive authority for information security to approve, authorize and issue all documents according to ISMS DOC 2.4 Approvers and Responsible persons.

The Information Security Director and all Heads of Department/Divisional/Function approve and authorize documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by Heads of Department/Divisional/Function have to be approved and authorized by the CISO.

Owners of information assets (see section 5.4 of ISMS DOC 6.2 and ISMS DOC 7.1 Asset Inventory & Ownership) are responsible for the security classification of their asset(s), the day-to-day protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

- The individual has the necessary skill, competence and resources to carry out the processes or task(s) and
- The Owner retains accountability for ensuring that the process or task is carried out correctly.

Access rights are specified in ISMS DOC 11.1 Access Control and ISMS DOC 11.2 Access Control Rules & Rights and ISMS DOC 11.3 User Access Management. Access rights are personal, are set out in individual User Agreements (ISMS DOC 8.11 Individual User Agreement and ISMS DOC 11.19 Clear Desk and Clear Screen Policy , DOC 11.13) and cannot be delegated.

Document approval workflows

Ad hoc Workflows plugin is used to automate page approval process.

Reporting plugin is used together with Ad hoc Workflows Supplier to include workflow state/approval information inside the page and make typical Approval section fully automated and therefore maintainable.

DMS instance is used for preparation and modification of documents requiring formal approval by ISC or company management (Executive, BoD,). After documents are ready, they are published on corporate confluence "large Confluence" as official documents to be followed by entire company. Publishing of finalized documents is automated by Ad hoc Workflows and Remote Publishing plugins.

Using Ad hoc Workflows there are three page states:

- ❑ **Draft** - if document is in redaction and is not ready for review;
- ❑ **For Review** - when document is ready and should be reviewed by ISMS Manager;
- ❑ **CISO review (BOD Review, VP Review)** - when document is approved by ISMS Manager and should be reviewed by CISO (BoD, VP);
- ❑ **Published** - this state mean that document is approved by company management and is published on corporate confluence to be followed by entire company.

Reference workflow report (ISMS DOC 2.3 Documents List by State) provides a list of documentation that should be approved by responsible persons. It allows to simplify whole document approval process.

DMS allows tracking of all changes on each page. To view all page activities user should pick "Page Activity" from "Tools" drop down menu. This activity list shows additions and edits done by appropriate person and activities with statuses done by approvers or redactors.

Terms

Important terms used in ISMS documents should be defined using Glossary page. It creates hidden separate pages. This way, hierarchy of pages containing terms definitions does not "pollute" actual document space and does not show in built-in page hierarchy view on the left.

All Important terms used in ISMS documents have appropriate references on Glossary.

Technical details

- ❑ If we use macros insert _in the ISMS document, we should note last date of modification near the title of this insertion: **Insertion NAME** (Last modified: 03 January 2013 - 01:06 PM)
- ❑ All tables and pictures contained in the ISMS documents must indicate their name, according to this template: **Table: NAME** and **Picture: NAME**

ISMS Documents Change Management

- ❑ Changes to ISMS policies and procedures (including updating, withdrawal or replacement) must be authorized in line with the requirements of section 6 of this document.

- ❑ All changes are subject to, and a consequence of, a change in the risk assessment.
- ❑ Where possible, records should be stored electronically and be readily accessible. Records are to be stored securely according to the relevant classification.
- ❑ Storage areas shall minimize unauthorized access. Only personnel responsible for these records may remove records from the storage area.
- ❑ Removal of ISMS records from the vicinity of the storage area shall be documented on log.
- ❑ Records should be destroyed at the end of their retention period. A ISMS document destruction shall be authorized by ISMS Manager

HIPAA Rules require that Covered Entities and Business Associates maintain their policies and procedures in written or electronic form, as well as the following:

- ❑ Maintain written or electronic copies of communications that the Rules require to be in writing.
- ❑ Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.
- ❑ Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.
- ❑ Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

HIPAA Documentation includes the following:

- ❑ HIPAA Policies and Procedures.
- ❑ HIPAA Risk Analysis and related notes and research materials
- ❑ Policies and Procedures for minimum necessary uses by your work force.
- ❑ Accounting documentation which includes…
  - Information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures, description, etc.);
  - the written accounting that is provided to the individual; and
  - The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
- ❑ Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
- ❑ All complaints received and their disposition, if any.
- ❑ All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.
- ❑ The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
- ❑ Training provided (i.e., topics, dates, and, ideally, participants).
- ❑ Sanctions imposed against non-complying work force members.
- ❑ All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
- ❑ The methods and results of analyses that justify release of de-identified information.
- ❑ Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.

- ❑ Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
- ❑ The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
- ❑ All signed authorizations and revocations.
- ❑ All approved confidential communication requests and terminations or revocations.

SECTION 11

Policy Number: 11.0
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Disaster Recovery Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).
- ❑ HIPAA requires **SoftServe Inc.** to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information.
- ❑ A disaster may occur at any time, not necessarily during work hours.
- ❑ **SoftServe Inc.** must remain operational with as little disruption of business operations and patient care as possible.
- ❑ Continuity of patient care requires uninterrupted access to patient information.
- ❑ In a dangerous emergency, evacuating personnel has priority over preserving information assets.
- ❑ The following conditions can destroy or disrupt **SoftServe Inc.'s** information systems:
  - Power interruption.
  - Fire.
  - Water.
  - Weather and other natural phenomena, such as earthquakes.
  - Sabotage and vandalism.
  - Terrorism.

Policy Statement

It is the policy of **SoftServe Inc.** to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information.

Procedures

Preventive Measures

- ❑ ISMS and or their designee(s) shall ensure that the following preventive measures, as applicable, are implemented and documented:
  - Retain dictation on disk for three months (or specify other time period).
  - Back up computerized files according to our Data Backup Policy.
  - Store backup media tape in the off-site media vault, according to our Data Backup Policy.
  - Maintain and replace backup tapes according to our Data Backup Policy.

- Test integrity of backup system no less than monthly (or specify other time period), according to our Data Backup Policy.
- Store media properly. For example, laser discs must be stored in sleeves of plastic, paper, or combination of the two, placed in cardboard jackets or boxes, and stored on edge on metal shelving, properly labeled.
- Color-code all media as to priority of evacuation: red is first priority; yellow is second priority; green is third priority.
- Protect by uninterruptible power supplies all servers and other critical equipment from damage in the event of an electrical outage.
- Locate file servers and other critical hardware in rooms with Halon fire protection systems which limit damage to the immediate area of the fire. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
- In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
- In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
- Training in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster.

□ **ISMS team** must implement and document the following:

- Ensure that major hardware is covered under **SoftServe Inc.'s** property and casualty, and or other appropriate insurance policy or policies.
- Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

Priority Tasks during Emergencies

As applicable, and under appropriate circumstances, all workforce members should:

□ Remain calm.
□ Activate the alarm. That is, pull the fire alarm or call 911 as appropriate.
□ Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
□ If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
□ If safe, close all doors as you leave.
□ Obtain portable phone(s) to communicate.
□ Notify concerned fire, police, security, administration, and others as necessary.
□ Notify other departments of situation and emergency protocols.
□ If computers have not automatically powered down, initiate procedures to orderly shutdown systems, when possible.
□ If a fire or flood occurs, disconnect power if possible.
□ If a fire or flood occurs, try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
□ Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
□ Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
□ Respond to requests for records via portable phone rather than computer.
□ Continue to provide patient charts as requested by physicians or other parties.

Priority Disaster Recovery Tasks

As applicable, and under appropriate circumstances, all workforce members should:

- □ Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
- □ Not permit unauthorized personnel to enter the affected area.
- □ Determine the extent of the damage and whether additional equipment/supplies are needed.
- □ Determine how long it will be before service can be restored, and notify departments.
- □ Replace hardware as necessary to restore service.
- □ Work with vendors as necessary to ensure that support is given to restore service.
- □ Notify insurance carriers.
- □ Retrieve and upload backup files if necessary to restore service.
- □ Air-dry floppy disks, if any, using a hair dryer on "air," not "heat." When dry, copy disk.
- □ For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
- □ Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
- □ Wrap paper records to prevent them from sticking together. Label the wrapped records.
- □ Contact fire, water, and storm damage Restoration Company. Contract for services as needed.
- □ Reconstruct/reacquire documents from the following:
  - Dictation system.
  - Word processing system.
  - Computer system.
  - Holders of document copies.
- □ Move records and equipment back to home location.
- □ Catch up on filing.
- □ Ensure that backup procedures are followed.
- □ Document data that cannot be recovered in patient record.
- □ Meet with management and staff to identify opportunities for improvement.

Additional Disaster Recovery Tasks

The following tasks must be assigned to specific persons or positions:

- □ Determine whether additional equipment and supplies are needed.
- □ Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- □ If necessary, check with other vendors to see whether they can provide faster delivery.
- □ Rush order any supplies and equipment necessary.
- □ Notify personnel that an alternate site will be necessary and where it is located.
- □ Coordinate moving equipment and support personnel to the alternate site.
- □ Bring recovery materials from offsite storage to the alternate site.

- ❑ As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- ❑ Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
- ❑ Prepare backup materials and return them to the offsite storage area.
- ❑ Set up operations at the alternate site if necessary.
- ❑ Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- ❑ Ensure that periodic backup procedures are followed according to our Data Backup Policy.
- ❑ Plan to phase in all critical support.
- ❑ Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- ❑ Coordinate with administration and others for continuing support and ultimate restoration of normal operations.

Strategy

If the event occurs at **SoftServe** office(s), which may interrupt critical business functions, primarily delivery of services to the **SoftServe** customers, for period longer than 7 days, designated business functions will need to be performed from alternate location(s) or by alternate personnel.

Scope

Business Continuity/Disaster Recovery Plan covers (BCP) restoration of company business operations in following **Interruption Events**:

- ❑ **Loss of one or several corporate sites**. Such events might occur via severe structural damage of the buildings, where they reside. This covers partial or full destruction of company assets located within these buildings. Alternatively, Development Center might be considered lost by actions preventing company staff from entering the premises, e.g.: hostile takeover of facilities, legal action resulting in office seizure, etc.
- ❑ **Unavailability of one or several corporate sites**. This may be caused by extended unavailability of critical utility or communication services, like electrical power, water and plumbing, heating, telecommunications, etc. It is assumed that such event do not damage company assets and they can be used for immediate recovery actions
- ❑ **Loss of Data Center**
- ❑ **Unavailability of Data Center.**
- ❑ **Loss of personnel.** Such event may occur together with loss of site and results in death, injuries or extended sickness of company personnel.

Assumptions

- ❑ Business Continuity/Disaster Recovery Plan is prepared to address high impact residual risks. BCP does not describe risk mitigation actions introduced into daily company operations, like backup Internet channels for Development and Data Center, redundant power supply for the buildings, deployed emergency power generators, that is risk controls continuously operated by the company.
- ❑ Business Continuity/Disaster Recovery Plan does not address country-level events.

- Corporate representative offices and U.S. headquarters do not constitute critical assets in terms of business continuity. In the event of loss or unavailability of our US offices, phone and email connectivity will be rerouted to European headquarters and handled by Ukraine-based personnel.
- Climate in Ukraine is mostly temperate continental, with low risks of major natural disasters, such as hurricanes, floods or tornadoes that cause serious damages to the facilities. Known climate events in the cities affected power supply lines, which have recovery time within 1-2 days.
- Ukraine is not on a major fault line, and therefore does not experience earthquakes or volcano eruptions.

Organization

BCP Documentation

SoftServe Business Continuity/Disaster Recovery Plan consists of following standalone documents, which are executed if Interruption Event(s) occur:

- **Emergency Response Team Organization**
- **Business Continuity Plan** for each **Interruption Event (IE BCP)**, like loss of Lviv4 or Dnipro2 office or unavailability of Data Center at Lviv1.
- **Building Evacuation Plans (BEPs)** for each of **SoftServe** offices. Evacuation plans include floor plans provided by respective building owner.

BCP Phases

Initial Response Phase

The Initial Response phase begins as soon as an **Initial Response Team (IRT)** member is informed of an interruption event that has occurred, or is about to occur. It ends when the IRT:

- Determines that the event does not pose a threat to critical functions, or
- Decides to notify the **Emergency Response Team (ERT)**.

Assessment Phase

The Assessment Phase begins as soon as the ERT is notified of an event. It ends when the predetermined threshold of a disaster situation has been met or the Executive Emergency Management Teams (EEMT) agrees to declare a disaster and begin the **Emergency Declaration Phase**.

Emergency Declaration Phase

The **Emergency Declaration Phase** begins when the ERT determines that the event will impact critical function processing and that it is necessary to activate emergency action plans. When the ERT decides to declare an Emergency, it must also establish the Level of the Emergency. There are three levels:

Level 1: Maintain operations at primary site, alert teams, continue to monitor event impact and prepare for possible relocation.

Level 2: Relocate Level 2 Critical functions to Alternate Site, continue other operations at primary site, continue to monitor event impact and prepare for possible Level 3 declaration.

Level 3: Relocate all Critical functions to Alternate Site.

During the Emergency Declaration Phase all parties involved in the emergency action plans are contacted and mobilized, and begin to activate the emergency procedures in their respective plans. The Emergency Declaration Phase is complete when the interruption event has either been terminated by the ERT or all critical functions have been relocated to their Alternate Site.

Recovery Site Preparation and Systems Restoration Phase

The **Recovery Site Preparation Phase** activities include:

- □ All activities required to prepare the Alternate Site(s) for the mission critical functions that are being relocated from their primary site(s).
- □ All activities required to restore all designated data processing systems, functions and facilities that are required to support mission critical business functions.

The phase begins when the Recovery Site Support Teams and Data Center Recovery Teams arrive at the recovery site and ends when:

- □ All designated recovery site preparations have been completed
- □ All designated critical systems have been restored, restarted and turned over to the business functions they support.

Relocation Phase

The **Relocation Phase** begins as soon as all recovery site preparations have been completed. It ends as soon as all mission critical business function teams have been transported and have arrived at the recovery site. Relocation Phase activities Include:

- □ Communicating and coordinating transportation arrangements for the critical business functions teams
- □ Meeting the teams as they arrive and directing them to the designated recovery work spaces

Business Functions Start-up Phase

The **Business Functions Start-up Phase** begins when critical systems have been recovered and there are enough critical business function team employees at the recovery site(s) to begin the highest priority operations. It ends when the recovery site(s) are adequately staffed to support the all mission critical business functions. Activities include:

- □ Validation of restored systems' functionality and data integrity
- □ Evaluation of data recovery point and determining any data loss
- □ Controlled restart of business function operations

Remain at the Recovery Site(s) Phase

In the event that a multiple-day stay at the recovery site(s) is required, there are actions that must be taken due to this extended stay. This phase begins at the beginning of the second day of operations at the recovery site(s). It ends as soon as the ERT declares that the primary site is ready to be reoccupied and the decision to return to the primary site has been made.

Return to Primary Site Phase

This phase begins when the ERT makes the decision to return to the primary site. It ends as soon as full operations have been re-established at the primary site.

Testing

SoftServe BCP testing and validation is performed for each IE BCP independently. Each IE BCP should be tested/revised on annual basis.

BCP testing is performed using following methodologies:

- □ **Table-top** (structured walk-through) test for Emergency Response Team, validating organizational readiness and identifying potential gaps or show-stoppers;
- □ **Technical test** (only for Data Center IE BCP), performed by IT to validate critical system recovery procedures;
- □ **Evacuation drill** (orientation test) for building loss related IEs to verify personnel awareness.

BCP testing is scheduled year ahead in the way to create minimal disruption for company business operations.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:
   1.
      i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
      ii. *Implementation specifications*:
         A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
         B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
         C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

3.

i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. *Implementation specifications*:

A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4.

i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. *Implementation specifications*:

A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

ii. *Implementation specifications*. Implement:

A. *Security reminders* (Addressable). Periodic security updates.
B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

i. ***Standard: Contingency plan*.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. *Implementation specifications*:

A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Contingency Plan (§ 164.308(a)(7)

Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption. The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Policy Number: 11.1
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Contingency Operations Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to contingency operations, in accordance with the requirements at § 164.310(a)(1-2).
- ❑ Contingency Operations, for purposes of this policy document, are defined as processes and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- ❑ Contingency operations plans and procedures, in combination with other emergency preparedness plans and procedures, shall be documented, analyzed, revised and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.

Policy Statement

- ❑ It is the Policy of **SoftServe Inc.** to be fully prepared to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), during emergencies and contingency operations.
- ❑ Responsibility for planning and executing contingency operations shall reside with ISMS Team, who shall prepare, analyze, test, and update plans for contingency operations on a periodic basis.
- ❑ The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency.
- ❑ It is the Policy of **SoftServe Inc.** to fully document all contingency operations plans and procedures, in accordance with our Documentation Policy.

Procedures

Strategy

If the event occurs at **SoftServe** office(s), which may interrupt critical business functions, primarily delivery of services to the **SoftServe** customers, for period longer than 7 days, designated business functions will need to be performed from alternate location(s) or by alternate personnel.

Scope

Business Continuity/Disaster Recovery Plan covers (BCP) restoration of company business operations in following **Interruption Events**:

- **Loss of one or several corporate sites**. Such events might occur via severe structural damage of the buildings, where they reside. This covers partial or full destruction of company assets located within these buildings. Alternatively, Development Center might be considered lost by actions preventing company staff from entering the premises, e.g.: hostile takeover of facilities, legal action resulting in office seizure, etc.
- **Unavailability of one or several corporate sites**. This may be caused by extended unavailability of critical utility or communication services, like electrical power, water and plumbing, heating, telecommunications, etc. It is assumed that such event do not damage company assets and they can be used for immediate recovery actions
- **Loss of Data Center**
- **Unavailability of Data Center.**
- **Loss of personnel.** Such event may occur together with loss of site and results in death, injuries or extended sickness of company personnel.

Assumptions

- Business Continuity/Disaster Recovery Plan is prepared to address high impact residual risks. BCP does not describe risk mitigation actions introduced into daily company operations, like backup Internet channels for Development and Data Center, redundant power supply for the buildings, deployed emergency power generators, that is risk controls continuously operated by the company.
- Business Continuity/Disaster Recovery Plan does not address country-level events.
- Corporate representative offices and U.S. headquarters do not constitute critical assets in terms of business continuity. In the event of loss or unavailability of our US offices, phone and email connectivity will be rerouted to European headquarters and handled by Ukraine-based personnel.
- Climate in Ukraine is mostly temperate continental, with low risks of major natural disasters, such as hurricanes, floods or tornadoes that cause serious damages to the facilities. Known climate events in the cities affected power supply lines, which have recovery time within 1-2 days.
- Ukraine is not on a major fault line, and therefore does not experience earthquakes or volcano eruptions.

Organization

BCP Documentation

SoftServe Business Continuity/Disaster Recovery Plan consists of following standalone documents, which are executed if Interruption Event(s) occur:

- **Emergency Response Team Organization**
- **Business Continuity Plan** for each **Interruption Event (IE BCP)**, like loss of Lviv4 or Dnipro2 office or unavailability of Data Center at Lviv1.
- **Building Evacuation Plans (BEPs)** for each of **SoftServe** offices. Evacuation plans include floor plans provided by respective building owner.

BCP Phases

Initial Response Phase

The Initial Response phase begins as soon as an **Initial Response Team (IRT)** member is informed of an interruption event that has occurred, or is about to occur. It ends when the IRT:

- □ Determines that the event does not pose a threat to critical functions, or
- □ Decides to notify the **Emergency Response Team (ERT)**.

Assessment Phase

The Assessment Phase begins as soon as the ERT is notified of an event. It ends when the predetermined threshold of a disaster situation has been met or the Executive Emergency Management Teams (EEMT) agrees to declare a disaster and begin the **Emergency Declaration Phase**.

Emergency Declaration Phase

The **Emergency Declaration Phase** begins when the ERT determines that the event will impact critical function processing and that it is necessary to activate emergency action plans. When the ERT decides to declare an Emergency, it must also establish the Level of the Emergency. There are three levels:

Level 1: Maintain operations at primary site, alert teams, continue to monitor event impact and prepare for possible relocation.

Level 2: Relocate Level 2 Critical functions to Alternate Site, continue other operations at primary site, continue to monitor event impact and prepare for possible Level 3 declaration.

Level 3: Relocate all Critical functions to Alternate Site.

During the Emergency Declaration Phase all parties involved in the emergency action plans are contacted and mobilized, and begin to activate the emergency procedures in their respective plans. The Emergency Declaration Phase is complete when the interruption event has either been terminated by the ERT or all critical functions have been relocated to their Alternate Site.

Recovery Site Preparation and Systems Restoration Phase

The **Recovery Site Preparation Phase** activities include:

- □ All activities required to prepare the Alternate Site(s) for the mission critical functions that are being relocated from their primary site(s).
- □ All activities required to restore all designated data processing systems, functions and facilities that are required to support mission critical business functions.

The phase begins when the Recovery Site Support Teams and Data Center Recovery Teams arrive at the recovery site and ends when:

- □ All designated recovery site preparations have been completed
- □ All designated critical systems have been restored, restarted and turned over to the business functions they support.

Relocation Phase

The **Relocation Phase** begins as soon as all recovery site preparations have been completed. It ends as soon as all mission critical business function teams have been transported and have arrived at the recovery site. Relocation Phase activities Include:

- □ Communicating and coordinating transportation arrangements for the critical business functions teams
- □ Meeting the teams as they arrive and directing them to the designated recovery work spaces

Business Functions Start-up Phase

The **Business Functions Start-up Phase** begins when critical systems have been recovered and there are enough critical business function team employees at the recovery site(s) to begin the highest priority operations. It ends when the recovery site(s) are adequately staffed to support the all mission critical business functions. Activities include:

- □ Validation of restored systems' functionality and data integrity
- □ Evaluation of data recovery point and determining any data loss
- □ Controlled restart of business function operations

Remain at the Recovery Site(s) Phase

In the event that a multiple-day stay at the recovery site(s) is required, there are actions that must be taken due to this extended stay. This phase begins at the beginning of the second day of operations at the recovery site(s). It ends as soon as the ERT declares that the primary site is ready to be reoccupied and the decision to return to the primary site has been made.

Return to Primary Site Phase

This phase begins when the ERT makes the decision to return to the primary site. It ends as soon as full operations have been re-established at the primary site.

Testing

SoftServe BCP testing and validation is performed for each IE BCP independently. Each IE BCP should be tested/revised on annual basis.

BCP testing is performed using following methodologies:

- □ **Table-top** (structured walk-through) test for Emergency Response Team, validating organizational readiness and identifying potential gaps or show-stoppers;
- □ **Technical test** (only for Data Center IE BCP), performed by IT to validate critical system recovery procedures;

- □ **Evacuation drill** (orientation test) for building loss related IEs to verify personnel awareness.

BCP testing is scheduled year ahead in the way to create minimal disruption for company business operations.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

a. A covered entity or business associate must, in accordance with § 164.306:

  1.

    i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

    ii. *Implementation specifications*:

      A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

      B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

      C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

      D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

  2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

  3.

    i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

    ii. *Implementation specifications*:

      A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

      B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

      C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4.

i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. *Implementation specifications*:

A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

ii. *Implementation specifications*. Implement:

A. *Security reminders* (Addressable). Periodic security updates.

B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

i. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. *Implementation specifications*:

A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

   B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
   C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
   D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of **contingency plans.**
   E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other **contingency plan** components.

8. *Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Contingency Plan (§ 164.308(a)(7)

We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

Contingency Plan (§ 164.308(a)(7)

Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption. The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Policy Number: 11.2
Effective Date: 3/26/2013
Last Revised: 7/292014

Emergency Mode Operations Policy

Assumptions

- □ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.

- □ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).
- □ Individually identifiable health information must be protected during emergencies, even as it is protected during normal operations. This Emergency Mode Operations Policy is designed to ensure the protection and availability of individually identifiable health information and Protected Health Information during emergencies requiring **SoftServe Inc.** to operate in "emergency mode".
- □ Our Emergency Mode Operations Plan must be implemented and executed in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary.

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to establish this Emergency Mode Operations Policy to implement procedures to enable continuation of critical business processes for the protection of individually identifiable health information while operating in emergency mode.
- □ It is the Policy of **SoftServe Inc.** to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.
- □ Our Emergency Mode Operations Plan shall be executed whenever **SoftServe Inc.** must operate in "emergency mode".
- □ "Emergency Mode" shall be in effect and activated whenever one or more of the following conditions applies:
    - Electrical power is unavailable for more than eight (or specify other number) hours.
    - Fire, flood, storm or other natural disaster renders our normal business facility unavailable or unusable for more than eight (or specify other number) hours.
    - Any other condition renders our normal business facility unavailable or unusable for more than eight (or specify other number) hours.

Procedures

1. Introduction

1.1. Purpose

The purpose of this plan is to set out the steps the **SoftServe** will take to survive a **disaster,** whether minor, moderate or major incidents (i.e. the loss of a significant part of the business operation for more than a few hours). Theft, fire, flood, bomb, vehicle collision, chemical spillage are typical causes. Loss of a single file server is not a disaster; a burn out of a computer room certainly would be. The Emergency Response Team will follow this plan, and the management team are committed to it.

1.2. Life cycle

Following a disaster, the typical response **life-cycle** would be:

1. Emergency response to assess level of damage, decide whether to invoke the plan and at what level, to notify Management and affected employees;

2. Provision of an emergency level of service;
3. Restoration of key services;
4. Recovery to business as normal.

1.3. Target times

Target times have been established for the above stages:

1. To be completed within two business hours of the disaster;
2. Within six business hours of the disaster;
3. Within two days of the disaster;
4. Within five days of the disaster.

1.4. Key resources

The **key resources** of the organization are:

- □ ***SoftServe*** *Employees* - provision of services is dependent on the knowledge and skills of existing employees.
- □ *Premises (Sites):*
  - Ukraine:
    - Lviv (Lviv1, Lviv2, Lviv3, Lviv4),
    - Dnipropetrovs'k (Dnipropetrovsk, Dnipropetrovsk2),
    - Sevastopol (Sevastopol, Sevastopol2),
    - Rivne (Rivne),
    - Ivano-Frankivsk (I.Frankivsk),
    - Chernivtsi (Chernivtsi)
  - USA: Fort Myers, FL
- □ *Telephony* - the telephone lines
- □ *Network* - Extranet, LAN, Internet, Intranet, Wi-Fi
- □ *Hardware* - the data, software, hardware - file servers, PCs, printers etc., structured cabling for data and telephony, LAN equipment, WAN equipment.
- □ *Software* - Project Infrastructure, Automated Project Environment, Financial application, HR Applications
- □ *Paper records* and filing systems.
- □ *Essential Services* - Electricity, heating, lighting, water, air-conditioning, telephony service, Internet service.

1.5. Strategic issues

The strategic issues affecting the development of this plan are:

[Set out here the key issues that affect the structure of your business continuity plan – what alternative sites and facilities are available, which services you need to have working within how long, what the key dependencies on your organization are, etc. – the business continuity risk assessment (ISMS DOC 17.2 Business Continuity Risk Assessment Standard) is a key input here].

1.5.1 Alternative sites; business continuity sites; use of a disaster recovery service.

1.5.2 The key need immediately following disaster is what, and how will it be handled? I.e. what services have to be restored first, and how quickly does it have to happen?

1.5.3 What additional risk issues might there be around telecommunications and data links?

1.5.4 How long can be allowed to restore operations completely, what limiting factors are there, and what other issues have to be taken into account?

1.5.5 How will [employees/staff] continue working, what will they do, what records will they maintain? Use of wireless laptops, PDAs, cellphones could be paramount here – with security implications.

1.5.6 Storage of records and backup procedures (fireproof safes, offsite storage, how to access?)

1.5.7 What are the repercussions of a disaster – press, customers, suppliers, others?

1.6. Document maintenance

This plan will be maintained in accordance ISMS DOC 17.4 Business Continuity Testing Standard.

1.7. Version control and distribution

Latest Version of Business Continuity Plan is printed and copies stored in each of premises storage spaces and available to employees, to management and to members of the Emergency Response Team in the event of an emergency.

2. Business Processes

2.1. Outward facing services

For external Office Support essential services of the organization (electricity, water, heating etc.) responsible Y. Stohniy (OS Department), other 3rd party services (including but not limited to Internet, telephony etc.) are under responsibility of V. Bychynskiy (ITAM Department).

Services provided by IT department can be found by next link https://confluence.softserveinc.com/display/ITBP/IT+Services+Portfolio

Alternates are identified in Section 4.3 Alternates of this document.

2.2. Inward facing services.

The internal services of the **SoftServe** (the ones that supply services to other parts of the organization): Finance, Marketing, IT, HR Department each department manager responsible for services within own department. The information assets that are involved in them are listed in dedicated document available by following link.

2.3. Priorities

Following a disaster, the immediate business service priorities are (in descending order):

- □ 3rd Party Services
    - Electricity
    - Telephony
    - Internet
    - Water
    - Air-conditioning
- □ Internal Services
    - Financial
    - InO
    - Security
    - ITSD
    - HR
    - ITAM
    - OS

2.4. Range of risks

2.4.1 A severe staff shortage could require partial invocation of the Business Continuity Plan. Managers/Executives (generic/line) must inform the Emergency Response Team of a critical staff shortage as soon as, in their opinion, they have insufficient employees available to offer an effective service. This sort of problem could be caused by industrial action on public transport, severe weather, etc.

2.4.2 Failure of electricity, Denial of Service attack, server room disaster that might affect key services or systems and which would take the business 'off line' for 6 hours should invoke appropriate BCP.

Continuity plans for each of these eventualities have been developed and are (as required by ISMS DOC 17.1 Business Continuity Planning Standard) appended to this plan.

3. Emergency Response

3.1. Alert, escalation and plan invocation

3.1.1 There are a number of different possible disasters, each of which may require partial or complete invocation of the BCP, or of one of the special appended plans. Each of the sites of the **SoftServe** has a standard, rehearsed alert, escalation and BCP invocation procedure which is set out in this section.

3.1.2 Where the premises need to be evacuated, the BCP invocation plan identifies two evacuation assembly points:

- ❑ Lviv1 - Recreation Park across the V.Velykogo Street and parking space near Barvinok Market; Lviv2, Lviv3, Lviv4 - parking space across of Palace of "Zaliznychnykiv";
- ❑ The second assembly point for all Development Centers in Lviv is Stadium "Dynamo", str. Volodymyra Yaneva 10.

Employees have practiced evacuation and visitors wear badges with evacuation instructions; in evacuation, customer-handling staff remove the visitor's book.

3.1.3 The responsible officer identified in Section 2.1 of the BCP, must inform the Emergency Response Team that a critical business system is unavailable if either an identified problem has not been fixed/alternative arrangements made within two hours of notification of the problem or if the problem is unlikely to be corrected within two hours of its failure. The Emergency Response Team will then decide the extent to which the BCP or one of the min-BCPs must be invoked.

3.2. Emergency Response Team (ERT)

The team comprises those employees listed on the Emergency Team Contact Card. Contact details are available by following link

All staff are issued with a card containing Emergency Response Team contact details, to be used in the event of a disaster.

The responsibilities of the Emergency Response Team are to:

- ❑ Respond immediately to a potential disaster and call emergency services,
- ❑ Assess the extent of the disaster and its impact on the business,
- ❑ Decide which elements of the Business Continuity Plan should be invoked,
- ❑ Establish and manage a Service Continuity Team to maintain vital services,
- ❑ Establish and manage a Disaster Recovery Team to return to normal operation,
- ❑ Ensure employees are notified and allocate responsibilities and activities as required.

3.3. Emergency Response Team Assembly Location

In the event of a disaster, the members of the Emergency Response Team will attempt to contact each other and agree an assembly location for the Emergency Response Team.

In the absence of any other communication, members of the Emergency Response Team will make their way to the standard assembly location listed in section 3.2

Information about this location should be shared with Telephone handling team, administrative team, procurement, depending on prioritization of what has to be restored by when and what's involved in doing that.

3.4. Emergency Response Team Action

The members of the Emergency Response Team will take on roles and delegate activities to other employees according to the situation. The Emergency Response Team will set clear objectives, defining responsibilities and priorities, and provide decisive leadership in dealing with business continuity issues.

The exact action to be taken will depend upon the circumstances; an *ERT Action Checklist* is listed at the end of section 3.

3.5. Disaster Recovery Team

The composition of the team will be decided by the Emergency Response Team.

The responsibilities of the team are to:

- ❑ Establish facilities for an emergency level of service within 6 business hours,
- ❑ Restore key services within two days of the disaster,
- ❑ Recover to business as usual within five days of the disaster,
- ❑ Coordinate activities with the service continuity team,
- ❑ Report to the emergency response team.

3.6. Service Continuity Team

The composition of the team will be decided by the Emergency Response Team.

The responsibilities of the team are to:

- ❑ Ensure that key services continue with a minimum of disruption,
- ❑ Agree the resource requirements with the disaster recovery team,
- ❑ Coordinate activities with the service managers,
- ❑ Report to the Emergency Response Team.

Continuity plans have been prepared by the Managers/Executives (generic/line) in respect of their services, and are available by following link (not developed yet).

Emergency alert, escalation and BCP invocation procedure applies at all the SoftServe's sites available by following listed in section 5.3.

ERT DISASTER ACTION CHECKLIST:

Note: This action checklist is designed for emergency situations; there are a number of circumstances in which appropriate action does not require the full response.

- ✓ Evacuation and calling of emergency services;
- ✓ Calling Tree;

- ✓ Emergency Response Team Office;
- ✓ Call Logging;
- ✓ Events;
- ✓ Employees;
- ✓ Facilities **-** buildings, furniture, equipment - assessing damage; determining immediate and longer term needs; obtaining supplies; dealing with insurers and loss adjusters;
- ✓ IT, Telephony, Data, Records
- ✓ Service Continuity
- ✓ R&D;
- ✓ Production;
- ✓ Manufacturing;
- ✓ Logistics/Transport;
- ✓ Media;
- ✓ Finance;
- ✓ Salvage **-** obtaining help with recovery.

4. Personnel

4.1. General responsibilities of employees

It is intended that all employees/staff will receive training in disaster reaction and in their general and specific disaster responsibilities. The *Disaster Checklist for Staff* (Appendix 1 to this section) which is issued to all [employees/staff] together with a credit card sized disaster card containing contact information.

4.2. Specific Responsibilities

Specific responsibilities related to the disaster will be allocated by the emergency response team as required; it is likely to include the following:

- □ Premises
- □ Finance
- □ IT
- □ Media
- □ Staff
- □ Etc.

4.3. Alternates

List of key employees that should have an alternate nominated who has the knowledge and ability to be able to deputize available by following link (not developed yet) List all the roles identified in 2.1 and 2.2 above.

4.4. Staff Communications

Personnel records are stored from corporate back-up repository. A list of all employees (including: home telephone number, address, and next of kin) stored at password protected and encrypted HR system with limited access. Access to this information authorized by HR Director directly.

When talking to an employee in the immediate aftermath of a disaster, follow the *Staff Call Checklist*. Immediate communications to site-located employees should be routed through the Emergency Evacuation Delegated personnel.

4.5. Health and Safety

The Health and Safety Procedures (Accident Procedure and Fire Evacuation Procedures) can be found by following link. These procedure should be followed in the event of a disaster, and are available on the circulated ERT Disks.

Trained first aiders list available by following link.

4.6. Calling Tree

A calling tree mechanism has been devised to share the work of ensuring that all staff are notified of the disaster, rippling down from the Emergency Response Team to the senior managers and then to the rest of the employees. The person discovering the disaster calls a member of the Emergency Response Team, trying in the order listed on their disaster card; if no Emergency Response Team member is available then alternates are tried.

The calling tree and contact numbers for key employees/staff are shown at Appendix 5 of this section.

The calling tree activity is independent of and in parallel to informing site-based employees/staff through the nominated Emergency Evacuation marshals.

DISASTER CHECKLIST FOR STAFF

Inform the responsible manager as identified in Section 2.1 of the BCP, if a key customer service appears to be unavailable.

Maintain your own safety - observe the emergency procedures and follow the instructions of the emergency services.

Help others - but do not take any personal risk.

Use your disaster card - keep it with you at all times, use it to telephone and notify the Emergency Response Team of your whereabouts and to keep in touch.

Maintain Confidentiality - be careful who you talk to, and ensure that what you say does not damage the interests of the organization; do not talk to the media, but refer callers to the media team [ensure their details are on the card].

Be prepared - keep a list of key clients, partners, suppliers, people you work with on a daily basis and other contacts, their telephone numbers and forthcoming commitments. Managers/Executives (generic/line) should also have the home telephone numbers of their direct reports. All customer facing staff should carry contact details for any clients they are meeting within the subsequent 2 days.

Keep services running - be ready to use your initiative.

Maintain security and quality - they are still important.

Be flexible - take on new responsibilities and tasks as the need arises.

Provide support - to other members of staff.

Keep records - so that systems can be updated later.

STAFF CALL CHECKLIST

- □ **Obtain Information:**
  - Caller's name.
  - Their whereabouts and a contact number.
  - Their state of health.
  - What they observed at the site of the disaster.
  - Who else was known to be at the site - other employees/staff or visitors.
  - Knowledge of other employees/staff, who is safe, who is injured.
  - Who they have spoken to, e.g. police or press, and what they have said.
  - Any practical difficulties, e.g. lack of cash, lost home keys, etc.
- □ **Assessment:**
  - Determine how useful the person is likely to be in the immediate future, what roles they could take on, and whether there are likely to be other needs such as trauma counselling.
- □ **Instructions to employee:**
  - The location to which they should report, or to go home.
  - Their responsibilities during disaster recovery e.g.
    - ○ To attempt to continue their normal activities,
    - ○ To take on a specific responsibility, or
    - ○ To do nothing until otherwise advised.
  - When to call again.

CALLING TREE

Calling trees and or order of calling for each department defined by department manager and can be found by following link.

IN CONFIDENCE - EMERGENCY USE ONLY

Staff Home and Mobile contact numbers for each site available.

5. Premises and Facilities

5.1. Overall Approach

[Describe your overall approach to business continuity, first in terms of premises, setting out the key trigger issues that lead to invocation of whatever your alternative premises plans are. If your plan involves an alternative remote site, you should explain why you chose it, set out what services it can provide, describe how those mirror your main site, describe how the security measures at the remote site mirror those at the main site, and set out the procedure for how you access it, including keys, bringing into service, additional equipment required, etc.]

Emergency contacts for use in the event of damage or disruption to office facilities or fabric at existing sites are also listed in this section. All suppliers to the organization are asked to undertake to continue to supply at contracted prices and response times during a disaster.

5.2. Emergency Premises

Contact details for emergency premises:

- ❑ Fire Service- Remote fire monitoring 235-25-86
- ❑ Fire Service- 101
- ❑ Ambulance- 103
- ❑ Police- 102
- ❑ Police- Пульт ВДСО 297-15-43, 297-18-21
- ❑ Police- Remote alarm call ВЕНБЕСТ-295-39-71

5.3. Site Contacts

[Refer back to the contact details in Appendix 4 to Section 4.]

- Ukraine:
  - Lviv (Lviv1, Lviv2, Lviv3, Lviv4) - 032 2409999
  - Dnipropetrovs’k (Dnipropetrovsk, Dnipropetrovsk2) - 056 790 2272
  - Sevastopol (Sevastopol, Sevastopol2) - 0692 466-713
  - Rivne (Rivne) - 0362 634 663
  - Ivano-Frankivsk (I.Frankivsk) - 0342 713 646
  - Chernivtsi (Chernivtsi) - 0372 586 130
- USA: Fort Myers, FL - 239.690.3111

5.4. Board

The **SoftServe's** Board of Directors should be informed as early as practicable. Contact details are available **SoftServe** Explorer (SSE)

5.5. Partners

5.6. Other organization's [that may provide alternative facilities]

5.7. Other Property Contacts

5.8. Landlords

Landlords should be contacted as soon as possible to arrange for their insurers to visit the disaster site; to help with remedial action; and to authorize longer term repairs. Contacts are available by following link.

5.9. Building Work

Contact details of all relevant trades are available below:

- ❑ Yaroslav Stavkovyy (chief Energy) 1222; 0676707931
- ❑ Borys Zarytskyy 067-904-85-34(Energy)
- ❑ Oleksandr Khomiak (Deputy Energy) 1271; 0963546248

5.10. Burglar alarms

Technical details of each installation and emergency contact details for all alarm companies at each site available in ISMS DOC 11.2 Fire and Burglar Alarm Monitoring Standard

5.11. Air conditioning suppliers

- ❑ Volodymyr Kravchuk 0503172515, 0322971496, 0322970049

5.12. Internet service providers

- ❑ Dybtan Aleksandra 044 538-00-08, 044 585-21-13
- ❑ Petro Pelekh 032 2768401, 0676734723, 0676704230

5.13. Key holders

Names and contact details for all key holders at all sites is available below:

- ❑ Marian Petrivskyi 245-73-44,0974776688.
- ❑ Ihor Rudyk 0677309471.
- ❑ Ruslan Honcharskyy 0973319826 \2419680.
- ❑ Ivan Nahrebinchyk 221-07-75, 0975166055.
- ❑ Yuriy Stohniy 0679190527.
- ❑ Roman Onyshko 0977375036
- ❑ Bohdan Badlo 067-7898948/ 636451
- ❑ Volodymyr Matviishyn 063-248-98-48

5.14. Utilities

List of the daytime and out of office hours contact details for all the utilities (Electricity Water Gas Heating) for all your sites available below:

- ❑ Gas service -104, 233-11-63, Ihor Rudyk 0677309471.
- ❑ Vodokanal Manager, 276-20-50
- ❑ Lvivenergo 068, 272-92-92
- ❑ Lviv Teploenergo emergency 260-33-16

5.15. Emergency Services list

Emergency Services list and contacts information can be found below:

- ❑ Yaroslav Stavkovyy (chief Energy) 1222; 0676707931   (Required)
- ❑ Oleksandr Khomiak (Deputy Energy) 1271; 0963546248
- ❑ Roman Zayats 1090; 0675094825. (Required)
- ❑ Denys Shymoniak 3288;   0964142563 (Required)
- ❑ Borys Zarytskyy 067-904-85-34
- ❑ Lvivenergo 068, 272-92-92, 238-99-05

6. Information Systems and Communications

6.1. Paper Records

Some important information exists solely in paper form; this includes:

- ❑ Personnel records
- ❑ Some financial records
- ❑ Signed partner and supplier contracts
- ❑ Some client information.

Key personnel, financial and legal documents are kept in a fire-proof cabinet [which is precisely where?] and certain key documents may be kept offsite [what and where?].

6.2. Computer system

6.2.1 Backup arrangements.

6.2.2 Describe what your emergency computer arrangements are, both for how you restore service and for how you recover from disaster. If this involves buying computing or related equipment, you need to set out here where it comes from, what type of equipment needs to be purchased, what software, etc.]

6.2.3 The relative priorities for restoration of the computer applications will be determined by the [Emergency Response Team] but is likely to be:

[Set out, in terms of your service restoration priorities, what the order of computer system restoration should be].

6.2.4 The planned approach is:

[Set out, step by step, what you will do in order to achieve that restoration requirement]

There are full instructions for the restore operation in the IT Department Working Instructions [which are available where and how?].

6.2.5 The timescale [describe the expected timescale for each of the stages, so that you can easily identify where things are going off track].

6.2.6 The use of existing home based/mobile computer equipment during restoration may be of some limited help in maintaining services. [Managers/Executives (generic/line)] have [PDAs] which contain details of key contacts and meetings.

6.3. Software

An analysis of the relative importance and difficulty of re-installing the key software products in use at the organization, together with contact details is contained in the following table. [This table should link back to your software asset log (REC 7.1B) and you should ensure you have identified how you will restore each type of software if you have to rebuild.]

6.4. Other key services

Also Corporate Websites, Corporation's Social Network Information shall be back up within Backup Procedure.

6.5. Wide Area Network/WLAN/LANs

6.5.1 Set out relative priorities for restoration, options in the short term, and the necessary technical specifications (a detailed network map, with hardware specifications, can be helpful here) and contact details to enable you to restore this service.

6.5.2 The network comprises the following elements:

6.5.3 Contact details are:

6.6. Telephony

6.6.1 [Repeat the exercise with telephony, looking at fixed links as well as at cellphones.]

6.6.2 [Determine what will happen when someone phones a site that is out of action – i.e. what automatic diverting routines do you have?]

6.6.3 For problems affecting the switchboards of handsets, contact

[Provide details for telephone switches, handsets, etc.].

6.6.4 IN THE EVENT OF AN ELECTRICAL POWER FAILURE:

[Set out, for each of the sites, what will happen if there is an electrical power failure, at the site or at the premises of a service (e.g. telecoms) supplier, and how you will deal with this. You should include analogue phone services, diversion services and so on in your plans. This will need to include all the contact details necessary to deal with this issue.]

IT, TELEPHONY, POST contact list available.

7. Media

7.1 Marketing Director will take responsibility for managing the media, working according to guidelines that will be issued by the Emergency Response Team immediately following the disaster.

7.2 Marketing Director should consider two aspects:

- □ Avoiding adverse publicity
- □ Taking the opportunity for useful publicity.

7.3 At the time of disaster media team of Sales and Business Development Director, Marketing Director and pointed personnel from their departments, also as anyone else explicitly authorized by the Emergency Response Team.

7.4 All employees have been told that only the media team is permitted to talk to the media; anyone else contacted should refer callers to the media team.

7.5 Immediately following a disaster, the media team should contact the Local PR agencies to prepare a press bulletin. Contact list of PR agencies available.

7.6 List all the media contacts (names, papers and contact details that might be important) available.

8. Insurance Cover

8.1 In the event of an incident that may lead to a claim, contact details for the organization's insurance brokers available by following link.

8.2 The main policy is with [who]; a second policy is with [who?]. Cover is on [set out full details of the insurance policies, including levels of category in all the categories, policy numbers, renewal dates, excesses, etc.]

8.3 The life assurance policy details in respect of the Chief Executive Officer CEO can be found in Legal Department.

8.4 Insurance assessors may require access to the site to examine damage.

9. Financial and Legal

9.1 An assessment by the emergency response team of the impact on the financial affairs which include: loss of financial documents, loss of revenue, theft of check books etc., loss of cash is available by following link.(doesn't work)

9.2 The immediate financial needs of: cash flow position, temporary borrowing facility, forthcoming payments for taxes, payroll taxes, etc. The contacts for each of listed areas available in Finance Department.

9.3 Bank account details and contact details available in Finance Department and stored in USA and Ukrainian Headquarter.

9.4 The Emergency Response Team will decide whether there may be legal actions resulting from the disaster; in particular, the possibility of claims by or against the organization. Provide details of commercial lawyers who would handle claims on behalf of the **SoftServe**

9.5 If legal actions are possible, then the Board of Directors should be advised.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

b. A covered entity or business associate must, in accordance with § 164.306:

  1.

    i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

    ii. *Implementation specifications*:

      A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

      B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

      C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

      D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
3.
    - i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
    - ii. *Implementation specifications*:
        - A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
        - B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
        - C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
4.
    - i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
    - ii. *Implementation specifications*:
        - A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
        - B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
        - C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
5.
    - i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
    - ii. *Implementation specifications*. Implement:
        - A. *Security reminders* (Addressable). Periodic security updates.
        - B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

i. ***Standard: Contingency plan.*** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. *Implementation specifications*:

A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Contingency Plan (§ 164.308(a)(7)

Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption. The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Effective Date: 3/26/2013
Last Revised: 7/29/2014

Emergency Access Policy

Assumptions

- □ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- □ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency access procedures, in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).
- □ The establishment of emergency access procedures further strengthens the protections we offer to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
- □ These emergency access procedures apply to access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- □ Responsibility for the development and implementation of our emergency access procedures shall reside with Name of Responsible Party or Person, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- □ Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies.
- □ These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
- □ It is the Policy of **SoftServe Inc.** to fully document our emergency access procedures development and implementation, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

1. Introduction

1.1. Purpose

The purpose of this plan is to set out the steps the **SoftServe** will take to survive a **disaster,** whether minor, moderate or major incidents (i.e. the loss of a significant part of the business operation for more than a few hours). Theft, fire, flood, bomb, vehicle collision, chemical spillage are typical causes. Loss of a single file server is not a disaster; a burn out of a computer room certainly would be. The Emergency Response Team will follow this plan, and the management team are committed to it.

1.2. Life cycle

Following a disaster, the typical response **life-cycle** would be:

1. Emergency response to assess level of damage, decide whether to invoke the plan and at what level, to notify Management and affected employees;
2. Provision of an emergency level of service;
3. Restoration of key services;
4. Recovery to business as normal.

1.3. Target times

Target times have been established for the above stages:

1. to be completed within two business hours of the disaster;
2. within six business hours of the disaster;
3. within two days of the disaster;
4. Within five days of the disaster.

1.4. Key resources

The **key resources** of the organization are:

- □ ***SoftServe*** *Employees* - provision of services is dependent on the knowledge and skills of existing employees.
- □ *Premises (Sites):*
    - Ukraine:
        - Lviv (Lviv1, Lviv2, Lviv3, Lviv4),
        - Dnipropetrovs'k (Dnipropetrovsk, Dnipropetrovsk2),
        - Sevastopol (Sevastopol, Sevastopol2),
        - Rivne (Rivne),
        - Ivano-Frankivsk (I.Frankivsk),
        - Chernivtsi (Chernivtsi)
    - USA: Fort Myers, FL
- □ *Telephony* - the telephone lines
- □ *Network* - Extranet, LAN, Internet, Intranet, Wi-Fi
- □ *Hardware* - the data, software, hardware - file servers, PCs, printers etc., structured cabling for data and telephony, LAN equipment, WAN equipment.
- □ *Software* - Project Infrastructure, Automated Project Environment, Financial application, HR Applications
- □ *Paper records* and filing systems.
- □ *Essential Services -* Electricity, heating, lighting, water, air-conditioning, telephony service, Internet service.

1.5. Strategic issues

The strategic issues affecting the development of this plan are:

[Set out here the key issues that affect the structure of your business continuity plan – what alternative sites and facilities are available, which services you need to have working within how long, what the key dependencies on your organization are, etc. – the business continuity risk assessment (ISMS DOC 17.2 Business Continuity Risk Assessment Standard) is a key input here].

1.5.1 Alternative sites; business continuity sites; use of a disaster recovery service.

1.5.2 The key need immediately following disaster is what, and how will it be handled? I.e. what services have to be restored first, and how quickly does it have to happen?

1.5.3 What additional risk issues might there be around telecommunications and data links?

1.5.4 How long can be allowed to restore operations completely, what limiting factors are there, and what other issues have to be taken into account?

1.5.5 How will [employees/staff] continue working, what will they do, what records will they maintain? Use of wireless laptops, PDAs, cellphones could be paramount here – with security implications.

1.5.6 Storage of records and backup procedures (fireproof safes, offsite storage, how to access?)

1.5.7 What are the repercussions of a disaster – press, customers, suppliers, others?

1.6. Document maintenance

This plan will be maintained in accordance ISMS DOC 17.4 Business Continuity Testing Standard.

1.7. Version control and distribution

Latest Version of Business Continuity Plan is printed and copies stored in each of premises storage spaces and available to employees, to management and to members of the Emergency Response Team in the event of an emergency.

2. Business Processes

2.1. Outward facing services

For external Office Support essential services of the organization (electricity, water, heating etc.) responsible Y. Stohniy (OS Department), other 3rd party services (including but not limited to Internet, telephony etc.) are under responsibility of V. Bychynskiy (ITAM Department).

Services provided by IT department can be found by next
link https://confluence.softserveinc.com/display/ITBP/IT+Services+Portfolio

Alternates are identified in Section 4.3 Alternates of this document.

2.2. Inward facing services.

The internal services of the **SoftServe** (the ones that supply services to other parts of the organization): Finance, Marketing, IT, HR Department each department manager responsible for services within own department. The information assets that are involved in them are listed in dedicated document available by following link.

2.3. Priorities

Following a disaster, the immediate business service priorities are (in descending order):

- □ 3rd Party Services
  - Electricity
  - Telephony
  - Internet
  - Water
  - Air-conditioning
- □ Internal Services
  - Financial
  - InO
  - Security
  - ITSD
  - HR
  - ITAM
  - OS

2.4. Range of risks

2.4.1 A severe staff shortage could require partial invocation of the Business Continuity Plan. Managers/Executives (generic/line) must inform the Emergency Response Team of a critical staff shortage as soon as, in their opinion, they have insufficient employees available to offer an effective service. This sort of problem could be caused by industrial action on public transport, severe weather, etc.

2.4.2 Failure of electricity, Denial of Service attack, server room disaster that might affect key services or systems and which would take the business 'off line' for 6 hours should invoke appropriate BCP.

Continuity plans for each of these eventualities have been developed and are (as required by ISMS DOC 17.1 Business Continuity Planning Standard) appended to this plan.

3. Emergency Response

3.1. Alert, escalation and plan invocation

3.1.1 There are a number of different possible disasters, each of which may require partial or complete invocation of the BCP, or of one of the special appended plans. Each of the sites of the **SoftServe** has a standard, rehearsed alert, escalation and BCP invocation procedure which is set out in this section.

3.1.2 Where the premises need to be evacuated, the BCP invocation plan identifies two evacuation assembly points:

- ❑ Lviv1 - Recreation Park across the V.Velykogo Street and parking space near Barvinok Market; Lviv2, Lviv3, Lviv4 - parking space across of Palace of "Zaliznychnykiv";
- ❑ The second assembly point for all Development Centers in Lviv is Stadium "Dynamo”, str. Volodymyra Yaneva 10.

Employees have practiced evacuation and visitors wear badges with evacuation instructions; in evacuation, customer-handling staff remove the visitor's book.

3.1.3 The responsible officer identified in Section 2.1 of the BCP, must inform the Emergency Response Team that a critical business system is unavailable if either an identified problem has not been fixed/alternative arrangements made within two hours of notification of the problem or if the problem is unlikely to be corrected within two hours of its failure. The Emergency Response Team will then decide the extent to which the BCP or one of the min-BCPs must be invoked.

3.2. Emergency Response Team (ERT)

The team comprises those employees listed on the Emergency Team Contact Card. Contact details are available by following link

All staff are issued with a card containing Emergency Response Team contact details, to be used in the event of a disaster.

The responsibilities of the Emergency Response Team are to:

- ❑ Respond immediately to a potential disaster and call emergency services,
- ❑ Assess the extent of the disaster and its impact on the business,
- ❑ Decide which elements of the Business Continuity Plan should be invoked,
- ❑ Establish and manage a Service Continuity Team to maintain vital services,
- ❑ Establish and manage a Disaster Recovery Team to return to normal operation,
- ❑ Ensure employees are notified and allocate responsibilities and activities as required.

3.3. Emergency Response Team Assembly Location

In the event of a disaster, the members of the Emergency Response Team will attempt to contact each other and agree an assembly location for the Emergency Response Team.

In the absence of any other communication, members of the Emergency Response Team will make their way to the standard assembly location listed in section 3.2

Information about this location should be shared with Telephone handling team, administrative team, procurement, depending on prioritization of what has to be restored by when and what's involved in doing that.

3.4. Emergency Response Team Action

The members of the Emergency Response Team will take on roles and delegate activities to other employees according to the situation. The Emergency Response Team will set clear objectives, defining responsibilities and priorities, and provide decisive leadership in dealing with business continuity issues.

The exact action to be taken will depend upon the circumstances; an *ERT Action Checklist* is listed at the end of section 3.

3.5. Disaster Recovery Team

The composition of the team will be decided by the Emergency Response Team.

The responsibilities of the team are to:

- ❑ Establish facilities for an emergency level of service within 6 business hours,
- ❑ Restore key services within two days of the disaster,
- ❑ Recover to business as usual within five days of the disaster,
- ❑ Coordinate activities with the service continuity team,
- ❑ Report to the emergency response team.

3.6. Service Continuity Team

The composition of the team will be decided by the Emergency Response Team.

The responsibilities of the team are to:

- ❑ Ensure that key services continue with a minimum of disruption,
- ❑ Agree the resource requirements with the disaster recovery team,
- ❑ Coordinate activities with the service managers,
- ❑ Report to the Emergency Response Team.

Continuity plans have been prepared by the Managers/Executives (generic/line) in respect of their services, and are available by following link (not developed yet).

Emergency alert, escalation and BCP invocation procedure applies at all the SoftServe's sites available by following listed in section 5.3.

ERT DISASTER ACTION CHECKLIST:

Note: This action checklist is designed for emergency situations; there are a number of circumstances in which appropriate action does not require the full response.

- □ Evacuation and calling of emergency services;
- □ Calling Tree;
- □ Emergency Response Team Office;
- □ Call Logging;
- □ Events;
- □ Employees;
- □ Facilities - buildings, furniture, equipment - assessing damage; determining immediate and longer term needs; obtaining supplies; dealing with insurers and loss adjusters;
- □ IT, Telephony, Data, Records
- □ Service Continuity
- □ R&D;
- □ Production;
- □ Manufacturing;
- □ Logistics/Transport;
- □ Media;
- □ Finance;
- □ Salvage **-** obtaining help with recovery**.**

4. Personnel

4.1. General responsibilities of employees

It is intended that all employees/staff will receive training in disaster reaction and in their general and specific disaster responsibilities. The *Disaster Checklist for Staff* (Appendix 1 to this section) which is issued to all [employees/staff] together with a credit card sized disaster card containing contact information.

4.2. Specific Responsibilities

Specific responsibilities related to the disaster will be allocated by the emergency response team as required; it is likely to include the following:

- □ Premises
- □ Finance
- □ IT
- □ Media
- □ Staff
- □ Etc.

4.3. Alternates

List of key employees that should have an alternate nominated who has the knowledge and ability to be able to deputize (not developed yet) List all the roles identified in 2.1 and 2.2 above.

4.4. Staff Communications

Personnel records are stored from corporate back-up repository. A list of all employees (including: home telephone number, address, and next of kin) stored at password protected and encrypted HR system with limited access. Access to this information authorized by HR Director directly.

When talking to an employee in the immediate aftermath of a disaster, follow the *Staff Call Checklist*. Immediate communications to site-located employees should be routed through the Emergency Evacuation Delegated personnel.

4.5. Health and Safety

The Health and Safety Procedures (Accident Procedure and Fire Evacuation Procedures) can be found by following link. These procedure should be followed in the event of a disaster, and are available on the circulated ERT Disks.

Trained first aiders list available by following link.

4.6. Calling Tree

A calling tree mechanism has been devised to share the work of ensuring that all staff are notified of the disaster, rippling down from the Emergency Response Team to the senior managers and then to the rest of the employees. The person discovering the disaster calls a member of the Emergency Response Team, trying in the order listed on their disaster card; if no Emergency Response Team member is available then alternates are tried.

The calling tree and contact numbers for key employees/staff are shown at Appendix 5 of this section.

The calling tree activity is independent of and in parallel to informing site-based employees/staff through the nominated Emergency Evacuation marshals.

DISASTER CHECKLIST FOR STAFF

Inform the responsible manager as identified in Section 2.1 of the BCP, if a key customer service appears to be unavailable.

Maintain your own safety - observe the emergency procedures and follow the instructions of the emergency services.

Help others - but do not take any personal risk.

Use your disaster card - keep it with you at all times, use it to telephone and notify the Emergency Response Team of your whereabouts and to keep in touch.

Maintain Confidentiality - be careful who you talk to, and ensure that what you say does not damage the interests of the organization; do not talk to the media, but refer callers to the media team [ensure their details are on the card].

Be prepared - keep a list of key clients, partners, suppliers, people you work with on a daily basis and other contacts, their telephone numbers and forthcoming commitments. Managers/Executives (generic/line) should also have the home telephone numbers of their direct reports. All customer facing staff should carry contact details for any clients they are meeting within the subsequent 2 days.

Keep services running - be ready to use your initiative.

Maintain security and quality - they are still important.

Be flexible - take on new responsibilities and tasks as the need arises.

Provide support - to other members of staff.

Keep records - so that systems can be updated later.

STAFF CALL CHECKLIST

- □ **Obtain Information:**
  - Caller's name.
  - Their whereabouts and a contact number.
  - Their state of health.
  - What they observed at the site of the disaster.
  - Who else was known to be at the site - other employees/staff or visitors.
  - Knowledge of other employees/staff, who is safe, who is injured.
  - Who they have spoken to, e.g. police or press, and what they have said.
  - Any practical difficulties, e.g. lack of cash, lost home keys, etc.
- □ **Assessment:**
  - Determine how useful the person is likely to be in the immediate future, what roles they could take on, and whether there are likely to be other needs such as trauma counselling.
- □ **Instructions to employee:**
  - The location to which they should report, or to go home.
  - Their responsibilities during disaster recovery e.g.
    - To attempt to continue their normal activities,
    - To take on a specific responsibility, or
    - To do nothing until otherwise advised.
  - When to call again.

CALLING TREE

Calling trees and or order of calling for each department defined by department manager.

IN CONFIDENCE - EMERGENCY USE ONLY

Staff Home and Mobile contact numbers for each site available.

5. Premises and Facilities

5.1. Overall Approach

[Describe your overall approach to business continuity, first in terms of premises, setting out the key trigger issues that lead to invocation of whatever your alternative premises plans are. If your plan involves an alternative remote site, you should explain why you chose it, set out what services it can provide, describe how those mirror your main site, describe how the security measures at the remote site mirror those at the main site, and set out the procedure for how you access it, including keys, bringing into service, additional equipment required, etc.]

Emergency contacts for use in the event of damage or disruption to office facilities or fabric at existing sites are also listed in this section. All suppliers to the organization are asked to undertake to continue to supply at contracted prices and response times during a disaster.

5.2. Emergency Premises

Contact details for emergency premises:

- □ Fire Service- Remote fire monitoring 235-25-86
- □ Fire Service- 101
- □ Ambulance- 103
- □ Police- 102
- □ Police- Пульт ВДСО 297-15-43, 297-18-21
- □ Police- Remote alarm call ВЕНБЕСТ-295-39-71

5.3. Site Contacts

[Refer back to the contact details in Appendix 4 to Section 4.]

- Ukraine:
    - Lviv (Lviv1, Lviv2, Lviv3, Lviv4) - 032 2409999
    - Dnipropetrovs’k (Dnipropetrovsk, Dnipropetrovsk2) - 056 790 2272
    - Sevastopol (Sevastopol, Sevastopol2) - 0692 466-713
    - Rivne (Rivne) - 0362 634 663
    - Ivano-Frankivsk (I.Frankivsk) - 0342 713 646

  - Chernivtsi (Chernivtsi) - 0372 586 130
- USA: Fort Myers, FL - 239.690.3111

5.4. Board

The **SoftServe's** Board of Directors should be informed as early as practicable. Contact details are available **SoftServe** Explorer (SSE)

5.5. Partners

5.6. Other organization's [that may provide alternative facilities]

5.7. Other Property Contacts

5.8. Landlords

Landlords should be contacted as soon as possible to arrange for their insurers to visit the disaster site; to help with remedial action; and to authorize longer term repairs. Contacts are available by following link.

5.9. Building Work

Contact details of all relevant trades are available below:

- □ Yaroslav Stavkovyy (chief Energy) 1222; 0676707931
- □ Borys Zarytskyy 067-904-85-34(Energy)
- □ Oleksandr Khomiak (Deputy Energy) 1271; 0963546248

5.10. Burglar alarms

Technical details of each installation and emergency contact details for all alarm companies at each site available in ISMS DOC 11.2 Fire and Burglar Alarm Monitoring Standard

5.11. Air conditioning suppliers

- □ Volodymyr Kravchuk 0503172515, 0322971496, 0322970049

5.12. Internet service providers

- □ Dybtan Aleksandra 044 538-00-08, 044 585-21-13
- □ Petro Pelekh 032 2768401, 0676734723, 0676704230

5.13. Key holders

Names and contact details for all key holders at all sites is available below:

- □ Marian Petrivskyi 245-73-44,0974776688.
- □ Ihor Rudyk 0677309471.
- □ Ruslan Honcharskyy 0973319826 \2419680.
- □ Ivan Nahrebinchyk 221-07-75, 0975166055.

- □ Yuriy Stohniy 0679190527.
- □ Roman Onyshko 0977375036
- □ Bohdan Badlo 067-7898948/ 636451
- □ Volodymyr Matviishyn 063-248-98-48

5.14. Utilities

List of the daytime and out of office hours contact details for all the utilities (Electricity Water Gas Heating) for all your sites available below:

- □ Gas service -104, 233-11-63, Ihor Rudyk 0677309471.
- □ Vodokanal Manager, 276-20-50
- □ Lvivenergo 068, 272-92-92
- □ Lviv Teploenergo emergency 260-33-16

5.15. Emergency Services list

Emergency Services list and contacts information can be found below:

- □ Yaroslav Stavkovyy (chief Energy) 1222; 0676707931 (Required)
- □ Oleksandr Khomiak (Deputy Energy) 1271; 0963546248
- □ Roman Zayats 1090; 0675094825. (Required)
- □ Denys Shymoniak 3288; 0964142563 (Required)
- □ Borys Zarytskyy 067-904-85-34
- □ Lvivenergo 068, 272-92-92, 238-99-05

6. Information Systems and Communications

6.1. Paper Records

Some important information exists solely in paper form; this includes:

- □ Personnel records
- □ Some financial records
- □ Signed partner and supplier contracts
- □ Some client information.

Key personnel, financial and legal documents are kept in a fire-proof cabinet [which is precisely where?] and certain key documents may be kept offsite [what and where?].

6.2. Computer system

6.2.1 Backup arrangements.

6.2.2 Describe what your emergency computer arrangements are, both for how you restore service and for how you recover from disaster. If this involves buying computing or related equipment, you need to set out here where it comes from, what type of equipment needs to be purchased, what software, etc.]

6.2.3 The relative priorities for restoration of the computer applications will be determined by the [Emergency Response Team] but is likely to be:

[Set out, in terms of your service restoration priorities, what the order of computer system restoration should be].

6.2.4 The planned approach is:

[Set out, step by step, what you will do in order to achieve that restoration requirement]

There are full instructions for the restore operation in the IT Department Working Instructions [which are available where and how?].

6.2.5 The timescale [describe the expected timescale for each of the stages, so that you can easily identify where things are going off track].

6.2.6 The use of existing home based/mobile computer equipment during restoration may be of some limited help in maintaining services. [Managers/Executives (generic/line)] have [PDAs] which contain details of key contacts and meetings.

6.3. Software

An analysis of the relative importance and difficulty of re-installing the key software products in use at the organization, together with contact details is contained in the following table. [This table should link back to your software asset log (REC 7.1B) and you should ensure you have identified how you will restore each type of software if you have to rebuild.]

6.4. Other key services

Also Corporate Websites, Corporation's Social Network Information shall be back up within Backup Procedure.

6.5. Wide Area Network/WLAN/LANs

6.5.1 Set out relative priorities for restoration, options in the short term, and the necessary technical specifications (a detailed network map, with hardware specifications, can be helpful here) and contact details to enable you to restore this service.

6.5.2 The network comprises the following elements:

6.5.3 Contact details are:

6.6. Telephony

6.6.1 Repeat the exercise with telephony, looking at fixed links as well as at cellphones.

6.6.2 [Determine what will happen when someone phones a site that is out of action – i.e. what automatic diverting routines do you have?]

6.6.3 For problems affecting the switchboards of handsets, contact

[Provide details for telephone switches, handsets, etc.].

6.6.4 IN THE EVENT OF AN ELECTRICAL POWER FAILURE:

[Set out, for each of the sites, what will happen if there is an electrical power failure, at the site or at the premises of a service (e.g. telecoms) supplier, and how you will deal with this. You should include analogue phone services, diversion services and so on in your plans. This will need to include all the contact details necessary to deal with this issue.]

IT, TELEPHONY, POST contact list available.

7. Media

7.1 Marketing Director will take responsibility for managing the media, working according to guidelines that will be issued by the Emergency Response Team immediately following the disaster.

7.2 Marketing Director should consider two aspects:

- ❑ Avoiding adverse publicity
- ❑ Taking the opportunity for useful publicity.

7.3 At the time of disaster media team of Sales and Business Development Director, Marketing Director and pointed personnel from their departments, also as anyone else explicitly authorized by the Emergency Response Team.

7.4 All employees have been told that only the media team is permitted to talk to the media; anyone else contacted should refer callers to the media team.

7.5 Immediately there is a disaster, the media team should contact the Local PR agencies to prepare a press bulletin. Contact list of PR agencies available.

7.6 List all the media contacts (names, papers and contact details, that might be important) available.

8. Insurance Cover

8.1 In the event of an incident that may lead to a claim, contact details for the organization's insurance brokers available by following link.

8.2 The main policy is with [who]; a second policy is with [who?]. Cover is on [set out full details of the insurance policies, including levels of category in all the categories, policy numbers, renewal dates, excesses, etc.]

8.3 The life assurance policy details in respect of the Chief Executive Officer CEO can be found in Legal Department.

8.4 Insurance assessors may require access to the site to examine damage.

9. Financial and Legal

9.1 An assessment by the emergency response team of the impact on the financial affairs which include: loss of financial documents, loss of revenue, theft of check books etc., loss of cash is available by following link.(doesn't work)

9.2 The immediate financial needs of: cash flow position, temporary borrowing facility, forthcoming payments for taxes, payroll taxes, etc. The contacts for each of listed areas available in Finance Department.

9.3 Bank account details and contact details available in Finance Department and stored in USA and Ukrainian Headquarter.

9.4 The Emergency Response Team will decide whether there may be legal actions resulting from the disaster; in particular, the possibility of claims by or against the organization. Provide details of commercial lawyers who would handle claims on behalf of the **SoftServe**

9.5 If legal actions are possible, then the Board of Directors should be advised.

HHS Security Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312

A covered entity or business associate must, in accordance with § 164.306:

a.
   1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
   2. *Implementation specifications*:
      - i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
      - ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
      - iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
      - iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control.

In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Comment: We received one comment stating that the proposed implementation feature "Procedure for emergency access," is not access control and recommending that emergency access be made a separate requirement.

Response: We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the "Access controls" standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

Policy Number: 11.4
Effective Date: 3/26/2013
Last Revised: 7/29/2014

Policy on Testing and Revision of Contingency and Emergency Plans and Procedures

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).

- □ Emergency and contingency plans, and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of **SoftServe Inc.**
- □ Individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to periodically test, and revise as necessary, all emergency preparedness plans, including emergency and contingency plans.
- □ It is the Policy of **SoftServe Inc.** that all individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Procedures

- □ Emergency and contingency plans are the responsibility of the designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
- □ Emergency and contingency plans shall be reviewed, and revised if necessary, at least annually (or specify other time period). Copies of all such plans shall remain on file and be available to all personnel.
- □ Emergency and contingency plans shall be rehearsed, with all team members participating in such rehearsals, at least twice annually (or specify other time period).
- □ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall fully document all emergency preparedness plans, including emergency and contingency plans, and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.

Strategy

If the event occurs at **SoftServe** office(s), which may interrupt critical business functions, primarily delivery of services to the **SoftServe** customers, for period longer than 7 days, designated business functions will need to be performed from alternate location(s) or by alternate personnel.

Scope

Business Continuity/Disaster Recovery Plan covers (BCP) restoration of company business operations in following **Interruption Events**:

- □ **Loss of one or several corporate sites**. Such events might occur via severe structural damage of the buildings, where they reside. This covers partial or full destruction of company assets located within these buildings. Alternatively, Development Center might be considered lost by actions preventing company staff from entering the premises, e.g.: hostile takeover of facilities, legal action resulting in office seizure, etc.

- **Unavailability of one or several corporate sites**. This may be caused by extended unavailability of critical utility or communication services, like electrical power, water and plumbing, heating, telecommunications, etc. It is assumed that such event do not damage company assets and they can be used for immediate recovery actions
- **Loss of Data Center**
- **Unavailability of Data Center.**
- **Loss of personnel.** Such event may occur together with loss of site and results in death, injuries or extended sickness of company personnel.

Assumptions

- Business Continuity/Disaster Recovery Plan is prepared to address high impact residual risks. BCP does not describe risk mitigation actions introduced into daily company operations, like backup Internet channels for Development and Data Center, redundant power supply for the buildings, deployed emergency power generators, that is risk controls continuously operated by the company.
- Business Continuity/Disaster Recovery Plan does not address country-level events.
- Corporate representative offices and U.S. headquarters do not constitute critical assets in terms of business continuity. In the event of loss or unavailability of our US offices, phone and email connectivity will be rerouted to European headquarters and handled by Ukraine-based personnel.
- Climate in Ukraine is mostly temperate continental, with low risks of major natural disasters, such as hurricanes, floods or tornadoes that cause serious damages to the facilities. Known climate events in the cities affected power supply lines, which have recovery time within 1-2 days.
- Ukraine is not on a major fault line, and therefore does not experience earthquakes or volcano eruptions.

Organization

BCP Documentation

SoftServe Business Continuity/Disaster Recovery Plan consists of following standalone documents, which are executed if Interruption Event(s) occur:

- **Emergency Response Team Organization**
- **Business Continuity Plan** for each **Interruption Event (IE BCP)**, like loss of Lviv4 or Dnipro2 office or unavailability of Data Center at Lviv1.
- **Building Evacuation Plans (BEPs)** for each of **SoftServe** offices. Evacuation plans include floor plans provided by respective building owner.

BCP Phases

Initial Response Phase

The Initial Response phase begins as soon as an **Initial Response Team (IRT)** member is informed of an interruption event that has occurred, or is about to occur. It ends when the IRT:

- ❑ Determines that the event does not pose a threat to critical functions, or
- ❑ Decides to notify the **Emergency Response Team (ERT)**.

Assessment Phase

The Assessment Phase begins as soon as the ERT is notified of an event. It ends when the predetermined threshold of a disaster situation has been met or the Executive Emergency Management Teams (EEMT) agrees to declare a disaster and begin the **Emergency Declaration Phase**.

Emergency Declaration Phase

The **Emergency Declaration Phase** begins when the ERT determines that the event will impact critical function processing and that it is necessary to activate emergency action plans. When the ERT decides to declare an Emergency, it must also establish the Level of the Emergency. There are three levels:

Level 1: Maintain operations at primary site, alert teams, continue to monitor event impact and prepare for possible relocation.

Level 2: Relocate Level 2 Critical functions to Alternate Site, continue other operations at primary site, continue to monitor event impact and prepare for possible Level 3 declaration.

Level 3: Relocate all Critical functions to Alternate Site.

During the Emergency Declaration Phase all parties involved in the emergency action plans are contacted and mobilized, and begin to activate the emergency procedures in their respective plans. The Emergency Declaration Phase is complete when the interruption event has either been terminated by the ERT or all critical functions have been relocated to their Alternate Site.

Recovery Site Preparation and Systems Restoration Phase

The **Recovery Site Preparation Phase** activities include:

- ❑ All activities required to prepare the Alternate Site(s) for the mission critical functions that are being relocated from their primary site(s).
- ❑ All activities required to restore all designated data processing systems, functions and facilities that are required to support mission critical business functions.

The phase begins when the Recovery Site Support Teams and Data Center Recovery Teams arrive at the recovery site and ends when:

- ❑ All designated recovery site preparations have been completed
- ❑ All designated critical systems have been restored, restarted and turned over to the business functions they support.

Relocation Phase

The **Relocation Phase** begins as soon as all recovery site preparations have been completed. It ends as soon as all mission critical business function teams have been transported and have arrived at the recovery site. Relocation Phase activities Include:

- ❑ Communicating and coordinating transportation arrangements for the critical business functions teams
- ❑ Meeting the teams as they arrive and directing them to the designated recovery work spaces

Business Functions Start-up Phase

The **Business Functions Start-up Phase** begins when critical systems have been recovered and there are enough critical business function team employees at the recovery site(s) to begin the highest priority operations. It ends when the recovery site(s) are adequately staffed to support the all mission critical business functions. Activities include:

- ❑ Validation of restored systems' functionality and data integrity
- ❑ Evaluation of data recovery point and determining any data loss
- ❑ Controlled restart of business function operations

Remain at the Recovery Site(s) Phase

In the event that a multiple-day stay at the recovery site(s) is required, there are actions that must be taken due to this extended stay. This phase begins at the beginning of the second day of operations at the recovery site(s). It ends as soon as the ERT declares that the primary site is ready to be reoccupied and the decision to return to the primary site has been made.

Return to Primary Site Phase

This phase begins when the ERT makes the decision to return to the primary site. It ends as soon as full operations have been re-established at the primary site.

Testing

SoftServe BCP testing and validation is performed for each IE BCP independently. Each IE BCP should be tested/revised on annual basis.

BCP testing is performed using following methodologies:

- ❑ **Table-top** (structured walk-through) test for Emergency Response Team, validating organizational readiness and identifying potential gaps or show-stoppers;
- ❑ **Technical test** (only for Data Center IE BCP), performed by IT to validate critical system recovery procedures;
- ❑ **Evacuation drill** (orientation test) for building loss related IEs to verify personnel awareness.

BCP testing is scheduled year ahead in the way to create minimal disruption for company business operations.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308

c. A covered entity or business associate must, in accordance with § 164.306:

1\.

i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

ii. *Implementation specifications*:

A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

3\.

i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. *Implementation specifications*:

A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4\.

i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. *Implementation specifications*:

   A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

   B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

   C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

ii. *Implementation specifications*. Implement:

   A. *Security reminders* (Addressable). Periodic security updates.

   B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

   C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

   D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

i. ***Standard: Contingency plan.*** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. *Implementation specifications*:

   A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

   B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Contingency Plan (§ 164.308(a)(7)

Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption. The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Policy Number: 11.5
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Risk Management Process Policy

Assumptions

- ❑ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.
- ❑ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

Policy Statement

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this policy.

- ❑ It is the Policy of **SoftServe Inc.** to establish, implement, and maintain an appropriate risk management process.
- ❑ Such a risk management process shall be under the direct control and supervision of the designated Privacy Official, or other responsible party (if no Privacy Official has been

designated), and shall involve legal counsel, information technology, records management, senior management, and any other parties or persons deemed to be appropriate to the process.

- □ Business and information-technology "best practices", along with the research and recommendations of the National Institute for Standards and Technology ("NIST"), shall be included in the development and execution of the risk management process.
- □ **SoftServe Inc.'s** risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- □ The results of the risk management process shall be input into management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

Procedures

Responsibilities

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

- □ **The Chief Information Security Officer**. CISO is responsible for ensuring that the **SoftServe**'s risk management framework meets the requirements of the Board of Directors and of identified legislative or regulatory requirements in terms of risk management.
- □ **Senior Management.** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates risks requires the support and involvement of senior management. Also, Senior Management stands as **Information Owners (or Primary Asset Owners)** are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.
- □ **The VP IT.** The VP IT is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
- □ **Secondary Asset Owners (further SA owners).** SA owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of information within secondary assets they own. Typically the SA owners are responsible for changes to their assets. Thus, they usually have to approve and sign off on changes to their assets (e.g., system enhancement, major changes to the

software and hardware). SA owners must therefore understand their role in the risk management process and fully be involved this process:
identify threats, vulnerabilities, suggest controls and implement them.

- □ **Business and Functional Managers.** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper information security.

Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated within the organization. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4.

Risk is a function of the **likelihood** of a given **threat** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to information must be analyzed in conjunction with the potential vulnerabilities and the controls in place. Impact refers to the magnitude of harm that could be caused by a threat’s exercise of vulnerability. The level of impact is governed by the potential relative value for the information asset and resources affected. The risk assessment methodology encompasses nine primary steps, which are described in Sections 3.1 through 3.9

- □ Step 1 Asset Identification (Section 3.1)
- □ Step 2 Threat Identification (Section 3.2)
- □ Step 3 Vulnerability Identification (Section 3.3)
- □ Step 4 Control Analysis (Section 3.4)
- □ Step 5 Likelihood Determination (Section 3.5)
- □ Step 6 Impact Analysis (Section 3.6)
- □ Step 7 Risk Determination (Section 3.7)
- □ Step 8 Control Recommendations (Section 3.8)
- □ Step 9 Results Documentation (Section 3.9)

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

Asset Identification

In assessing risks for information, the first step is to define the scope of the effort. In this step, the boundaries of the organization are identified, along with the resources and the information that constitute the system.

Section 3.1.1 describes the system-related information used to characterize an asset. Section 3.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the information-processing environment.

System-Related Information

Identifying risk for information requires a keen understanding of the information-processing environment. The person or persons who conduct the risk assessment must therefore first collect all possible relative information, which is usually includes:

- Hardware
- Software
- Site
- Data and information
- Personnel
- Network
- Third Party Services

Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering relative information.

- **Questionnaire.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting assets. The questionnaire could also be used during on-site visits and interviews.
- **On-site Interviews.** Interviews with support, operations and management personnel can enable risk assessment personnel to collect useful information (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security.
- **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information

about the security controls used by and planned. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

- ❑ **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently (for example, a network mapping tool).

Output from Step 1 - all relative assets are identified, a good picture of the organizational, environment, and delineation boundaries is established.

Threat Identification

A threat is the potential for a particular threat-origin to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat does not present a risk when there is no vulnerability that can be exercised.

- ❑ **Threat:** The potential for a threat- source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat Identification

The goal of this step is to identify the potential threats and compile a threat statement listing potential threats that are applicable to the secondary assets being evaluated. A threat is defined as any circumstance or event with the potential to cause harm to an IT system. The common threats can be natural, human, or environmental.

Common Threats

- ❑ Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- ❑ Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- ❑ Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.

A threat is defined as any circumstance or event with the potential to cause harm to information. The common threats-sources can be natural, human, or environmental.

In assessing threats, it is important to consider all potential threats that could cause harm to information and its processing environment. For example, although the threat statement for an information located in a desert may not include "natural flood" because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threats through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threats. Table 3.2.2.1 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threats that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

Table 3.2.2.1: Human Threats.

Threat-Origin	**Motivation**	**Threat Actions**
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing

		• System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Vulnerability Identification

The analysis of the threat to information must include an analysis of the vulnerabilities associated with the organization environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

- **Vulnerability:** A flaw or weakness in organization's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

Vulnerability sources

Vulnerabilities associated within organization can be identified via the information-gathering techniques described in Section 3.1.2.

A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the IT system assessed
- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses

Control Analysis

The goal of this step is to analyze the controls that have been implemented by the organization to minimize or eliminate the likelihood of the risk. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current controls must be considered.

Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

❑ Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

❑ Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

Control Analysis Technique

As discussed in Section 3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization’s control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist’s validity.

Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- ❑ Threat-source motivation and capability
- ❑ Nature of the vulnerability
- ❑ Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat with certain frequency can be described as very high, high, medium, low or very low.

Asset owner using the Frequency Table below assesses the frequency of threat occurring.

Table 3.5.1: Frequency of threat occurring

Frequency of threat occurring (Level)	**Frequency of threat occurring (Description Statements)**
Very High	Has happened more than once per year at the Location
High	Has happened of the Location or more than once per year in Organization
Medium	Has happened in our Organization or more than once per year in the Industry
Low	Heard of in the Industry
Very Low	Never heard of in the Industry

The probability of _vulnerability being breached by a threat is assessed by security analyst and/or asset owner   using the Probability Table below.

Table 3.5.2: Probability of vulnerability being breached

Probability of vulnerability being breached (Level)	**Probability of vulnerability being breached (Description Statements)**
Very High	The vulnerability is EXPECTED to be exploited or triggered in most circumstances
High	The vulnerability will PROBABLY be exploited or triggered in most circumstances

Medium	The vulnerability MIGHT be exploited or triggered at some time but is not expected
Low	The vulnerability COULD be exploited or triggered at some time
Very Low	The vulnerability MAY be exploited or triggered in exceptional circumstances

The likelihood level is to be estimated by considering the frequency at which the threat is likely to occur in the future and the probability of the threat exploiting and/or breaching the vulnerability when it does occur: (Likelihood = Frequency of threat occurring x Probability of vulnerability being breached) by asset owner using the Risk Likelihood Matrix below.

Table 3.5.3: Likelihood matrix

		Probability of vulnerability being breached				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Frequency of threat occurring	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- ❑ Information mission
- ❑ Information criticality
- ❑ Information sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's information assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive data is, the SA owners and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

- ❑ **Loss of Integrity.** System and data integrity refers to the requirement that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the information by either intentional or accidental acts. If the loss information integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality.
- ❑ **Loss of Availability.** If a mission-critical information is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions and customer satisfaction.
- ❑ **Loss of Confidentiality.** Information confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of

confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Table 3.6.1: Risk Impact Level

Impact Level	Impact Level	Financial	Safety	Operational	Reputation	Legal Regulatory
Very High	5	Possible loss >$5M	Permanent injuries / deaths	Catastrophic impact on operations	Extended media coverage; major company embarrassment	Loss of operating license or directors/senior management charged and convicted
High	4	Possible loss $500k - $5M	Permanent injury / stress	Failure of one or more key organizational objectives leading to major disruption	Heavy media coverage	Inquest in to business resulting in an enforcement order fine and court conviction
Medium	3	Possible loss $50k - $500k	Injury requiring medical treatment / long term incapacity	No threat to achievement of objectives but could result in some moderate disruption	Customer comments escalated to management; minor media coverage	Likely fine or prosecution. Administrative undertaking
Low	2	Possible loss $5k - $50k	Injury requiring first aid treatment / temporary loss of time	Minor reduction in effectiveness and efficiency for a short period	Adverse customer comments	Warning issued by regulator
Very Low	1	Possible loss <$5k	Injury resulting in no loss of time	Negligible impact to effectiveness and efficiency	Manageable adverse customer comments	No legal or regulatory consequence

Risk Determination

The purpose of this step is to assess the level of risk to information. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- ❑ The likelihood of a given threat attempting to exercise a given vulnerability
- ❑ The magnitude of the impact should a threat successfully exercise the vulnerability

To measure risk, a risk scale and a risk level matrix must be developed. Table 3.7.1 presents a standard risk level matrix.

Table 3.7.1: Risk Level Matrix

		Impact Level				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Likelihood	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the information to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- ❑ Effectiveness of recommended options

- ❑ Legislation and regulation
- ❑ Organizational policy
- ❑ Operational impact
- ❑ Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact and feasibility of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Results Documentation

Once the risk assessment has been completed the results should be documented in an official reports – Risk Assessment Report (RAR), Risk Treatment Plan (RTP), Risk Treatment Action Plan (RTAP).

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. A risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

A risk treatment plan is a plan of measure what should be taken in regard to identified risks based on risk assessment report. After RTP is approved, RTAP should be prepared where detailed information for controls implementation should be stated: approved budged, schedule, responsible persons, effectiveness measurement methods and its frequency.

Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the **least-cost approach** and implement the **most appropriate controls** to decrease mission risk to an acceptable level, with **minimal adverse impact** on the organization's resources and mission.

This section describes risk mitigation options (Section 4.1), the risk mitigation strategy (Section 4.2), an approach for control implementation (Section 4.3), control categories (Section 4.4), the cost-benefit analysis used to justify the implementation of the recommended controls (Section 4.5), and residual risk (Section 4.6).

Risk Mitigation Options

Risk mitigation is a systematic methodology used by SA owner to reduce risks. Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Tolerance (Acceptance).** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Termination (Avoidance).** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Treatment (Limitation).** To treat the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability, threat frequency or vulnerability probability level of bean breached (e.g., use of supporting, preventive, detective controls)
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and information, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

Risk Mitigation Strategy

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

- ❑ **When vulnerability (or flaw, weakness) exists →** implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.

- □ **When a vulnerability can be exercised →** apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
- □ **When the attacker's cost is less than the potential gain →** apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- □ **When loss is too great →** apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

The strategy outlined above, with the exception of the third list item ("When the attacker's cost is less than the potential gain"), also applies to the mitigation of risks arising from environmental or unintentional human threats (e.g., system or user errors). (Because there is no "attacker," no motivation or gain is involved).

Approach for control implementation

When control actions must be taken, the following rule applies:

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk mitigation methodology describes the approach to control implementation:

- Step 1- Prioritize Actions

Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization's interest and mission.

Output from Step 1 - **Actions ranking from Very High to Very Low**

- Step 2- Evaluate Recommended Control Options

The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization. During this step, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

Output from Step 2 - **List of feasible controls**

- Step 3 - Conduct Cost-Benefit Analysis

To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted. Section 4.5 details the objectives and method of conducting the cost-benefit analysis.

Output from Step 3 - **Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls**

- Step 4 - Select Control

On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization's mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the information and the organization. During this step, a Develop a Risk Treatment Plan

Output from Step 4 - **Selected control(s)**

- Step 5 - Assign Responsibility

Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

Output from Step 5 - **List of responsible persons, budget and schedule**

- Step 6 - Develop a Risk Treatment Action Plan

During this step, a Risk Treatment Action Plan (or controls implementation plan) is developed. The plan should, at a minimum, contain the following information:

- ❑ Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- ❑ Recommended controls (output from risk assessment report)
- ❑ Prioritized actions (with priority given to items with Very High and High risk levels)
- ❑ Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- ❑ Required resources for implementing the selected planned controls
- ❑ Lists of responsible teams and staff
- ❑ Start date for implementation
- ❑ Target completion date for implementation
- ❑ Maintenance requirements
- ❑ Budget

The controls implementation plan prioritizes the implementation actions and projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. Appendix C provides a sample summary table for the controls implementation plan.

Output from Step 6 - **Risk Treatment Action Plan**

- Step 7- Implement Selected Control(s)

Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk. Residual risk is discussed in Section 4.6.

Output from Step 7 - **Residual risk**

Control Categories

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat damage to an organization's mission.

The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

Cost-Benefit Analysis

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

- ❑ Determining the impact of implementing the new or enhanced controls
- ❑ Determining the impact of not implementing the new or enhanced controls
- ❑ Estimating the costs of the implementation. These may include, but are not limited to, the following:

  - Hardware and software purchases
  - Reduced operational effectiveness if system performance or functionality is reduced for increased security
  - Cost of implementing additional policies and procedures
  - Cost of hiring additional personnel to implement proposed policies, procedures, or services
  - Training costs
  - Maintenance costs

- ❑ Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

Risk Acceptance

This risk acceptance approach is applied throughout the organization in respect of information risks.

- □ Understand the **nature of risk and business affect** in order to determine the acceptable level of risk.
- □ Assess the risk level in terms of business impact and its likelihood using.
- □ Understand what type of control(s) should be applied to mitigate the risk.
- □ Understand the cost to safeguard and mitigate the risk.
- □ Perform cost/benefit analysis.
- □ Decide whether the risk should be accepted.

Risk that could result in non-compliance with regulation or law, or could result in human harm cannot be accepted.

Table: Risk Acceptance (Last modified: 25 July 2014 - 04:14 PM)

Risk Level	**Responsibility for Risk Acceptance**	**Example (see Table: Risk Calculation Matrix)**
Very High	Shall be mitigated	Possible loss >$5M
High	Board of Directors	Possible loss $500k - $5M
Medium	CEO	Possible loss $50k - $500k
Low	Executive & Senior Management (EVP, SVP, VP)	Possible loss $15k - $50k
Very Low	Middle Level Management (SBU Managers, Department Directors)	Possible loss < $15k

Risk Level as '**Low**' and **'Very Low'** considered as acceptable level. Acceptable risk level was defined taking into account BIA and was approved by BoD.

Residual Risk

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.

Implementation of new or enhanced controls can mitigate risk by -

- Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat /vulnerability pairs
- Reducing the threat occurring frequency by adding a targeted control to reduce the capacity and motivation of a threat-source
- Reducing the magnitude of the adverse impact
- Reducing the probability that vulnerability can be breached level.
- In some cases control may affect combination of above parameters. For example, control related to physical security decreases vulnerability probability of physical security vulnerability in related risk(s), at same moment this control reduces the threat frequency of physical eavesdropping threat within the network risks.

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no organization's systems are risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

Evaluation and Assessment

In most organizations, the all its parts continually be expanded and updated, its components changed, replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) This series of guidance's will assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A).

Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements. An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines. Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process.

We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.

Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to *"Implement policies and procedures to prevent, detect, contain, and correct security violations."* (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard.

Section 164.308(a)(1)(ii)(A) states:
RISK ANALYSIS (Required).
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

The following questions adapted from NIST Special Publication (SP) 800-665 are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing the Security Rule:

- □ Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- □ What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- □ What are the human, natural, and environmental threats to information systems that contain e-PHI?

In addition to an express requirement to conduct a risk analysis, the Rule indicates that risk analysis is a necessary tool in reaching substantial compliance with many other standards and implementation specifications.

For example, the Rule contains several implementation specifications that are labeled "addressable" rather than "required." (68 FR 8334, 8336 (Feb. 20, 2003).) An addressable implementation specification is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document

why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so.
(See 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306(d)(3).)

The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Organizations should use the information gleaned from their risk analysis as they, for example:

- □ Design appropriate personnel screening processes. (45 C.F.R. § 164.308(a)(3)(ii)(B).)
- □ Identify what data to backup and how. (45 C.F.R. § 164.308(a)(7)(ii)(A).)
- □ Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a)(2)(iv) and (e)(2)(ii).)
- □ Address what data must be authenticated in particular situations to protect data integrity. (45 C.F.R. § 164.312(c)(2).)
- □ Determine the appropriate manner of protecting health information transmissions. (45 C.F.R. § 164.312(e)(1).)

Important Definitions
Unlike "availability", "confidentiality" and "integrity", the following terms are not expressly defined in the Security Rule. The definitions provided in this guidance, which are consistent with common industry definitions, are provided to put the risk analysis discussion in context. These terms do not modify or update the Security Rule and should not be interpreted inconsistently with the terms used in the Security Rule.

Vulnerability
Vulnerability is defined in NIST Special Publication (SP) 800-30 as *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."* Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of e-PHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical.

- □ <u>Non-technical vulnerabilities may include</u> ineffective or non-existent policies, procedures, standards or guidelines.
- □ <u>Technical vulnerabilities may include</u>: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

Threat
An adapted definition of threat, from NIST SP 800-30, is *"The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- □ <u>Natural threats</u> such as floods, earthquakes, tornadoes, and landslides.
- □ <u>Human threats</u> are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- □ <u>Environmental threats</u> such as power failures, pollution, chemicals, and liquid leakage.

Risk
An adapted definition of risk, from NIST SP 800-30, is: "*The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . Risks arise from legal liability or mission loss due to:*

- □ *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
- □ *Unintentional errors and omissions*
- □ *IT disruptions due to natural or man- made disasters*
- □ *Failure to exercise due care and diligence in the implementation and operation of the IT system."*

Risk can be understood as a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

Elements of a Risk Analysis

There are numerous methods of performing risk analysis and there is no single method or "best practice" that guarantees compliance with the Security Rule. Some examples of steps that might be applied in a risk analysis process are outlined in NIST SP 800-30.6

The remainder of this guidance document explains several elements a risk analysis must incorporate, regardless of the method employed.

Scope of the Analysis

The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)

This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization's risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

Data Collection

An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

Identify and Document Potential Threats and Vulnerabilities

Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Assess Current Security Measures

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

The security measures implemented to reduce risk will vary among organizations. For example, small organizations tend to have more control within their environment. Small organizations tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e- PHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a small organization may differ from those that are appropriate in large organizations.

Determine the Likelihood of Threat Occurrence

The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are "reasonably anticipated."

The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Potential Impact of Threat Occurrence

The Rule also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Level of Risk

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

Finalize Documentation

The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).) The risk analysis documentation is a direct input to the risk management process.

Periodic Review and Updates to the Risk Assessment

The risk analysis process should be ongoing. In order for an entity to update and document its security measures "as needed," which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. For example, if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

In Summary

Risk analysis is the first step in an organization's Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.

Resources

The Security Series papers available on the Office for Civil Rights (OCR) website, http://www.hhs.gov/ocr/hipaa, contain a more detailed discussion of tools and methods available for risk analysis and risk management, as well as other Security Rule compliance requirements.

Visit http://www.hhs.gov/ocr/hipaa for the latest guidance,

FAQs and other information on the Security Rule.

Several other federal and non-federal organizations have developed materials that might be helpful to covered entities seeking to develop and implement risk analysis and risk management strategies. The Department of Health and Human Services does not endorse or recommend any particular risk analysis or risk management model. The documents referenced below do not constitute legally binding guidance for covered entities, nor does adherence to any or all of the standards contained in these materials prove substantial compliance with the risk analysis requirements of the Security Rule. Rather, the materials are presented as examples of frameworks and methodologies that some organizations use to guide their risk analysis efforts.

The National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, is responsible for developing information security standards for federal agencies. NIST has produced a series of Special Publications, available at http://csrc.nist.gov/publications/PubsSPs.html, which provide information that is relevant to information technology security. These papers include:

- ❑ *Guide to Technical Aspects of Performing Information Security Assessments* (SP800-115).
- ❑ *Information Security Handbook: A Guide for Managers* (SP800-100; Chapter 10 provides a Risk Management Framework and details steps in the risk management process).
- ❑ *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (SP800-66; Part 3 links the NIST Risk Management Framework to components of the Security Rule).
- ❑ A draft publication, *Managing Risk from Information Systems* (SP800-39).

The Office of the National Coordinator for Health Information Technology (ONC) has produced a risk assessment guide for small health care practices, called Reassessing Your Security Practices in a Health IT Environment, which is available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848086_0_0_18/SmallPracticeSecurityGuide-1.pdf.

The Healthcare Information and Management Systems Society (HIMSS), a private consortium of health care information technology stakeholders, created an information technology security practices questionnaire, available at:
http://www.himss.org/content/files/ApplicationSecurityv2.3.pdf.
The questionnaire was developed to collect information about the state of IT security in the health care sector, but could also be a helpful self-assessment tool during the risk analysis process.

The Health Information Trust Alliance (HITRUST) worked with industry to create the Common Security Framework (CSF), a proprietary resource available at:
http://hitrustcentral.net/files.
The risk management section of the document, *Control Name: 03.0*, explains the role of risk assessment and management in overall security program development and implementation. The paper describes methods for implementing a risk analysis program, including knowledge and process requirements, and it links various existing frameworks and standards to applicable points in an information security life cycle.

HHS Regulations as Amended January 2013
Security Standards for the Protection of Electronic PHI: General Rules - § 164.306

a. *General requirements*. Covered entities and business associates must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
4. Ensure compliance with this subpart by its workforce.

b. *Flexibility of approach*.

1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

i. The size, complexity, and capabilities of the covered entity or business associate.

ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

iii. The costs of security measures.

iv. The probability and criticality of potential risks to electronic protected health information.

c. *Standards*. A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

d. *Implementation specifications*. In this subpart:

1. Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.
2. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.
3. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must--

i. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

ii. As applicable to the covered entity or business associate--

A. Implement the implementation specification if reasonable and appropriate; or

B. If implementing the implementation specification is not reasonable and appropriate--

1. Document why it would not be reasonable and appropriate to implement the implementation specification; and
2. Implement an equivalent alternative measure if reasonable and appropriate.

e. *Maintenance*. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii)

Policy Number: 11.6
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Risk Management Implementation Policy

Assumptions

□ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.

□ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk management implementation, in accordance with the requirements at § 164.308(a) (1).

□ Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.

□ This Risk Management Implementation Policy shall be considered an integral part of our other Risk Management policies, including, but not limited to, our:
- Risk Management Process Policy, and our
- Risk Analysis Policy

Policy Statement

□ It is the Policy of **SoftServe Inc.** to fully and completely implement our risk management process and all related policies.

□ The implementation of our risk management process, analyses, and improvements shall be under the direct supervision of the designated HIPAA Official or HIPAA Officer.

□ The designated HIPAA Official or HIPAA Officer, or other responsible party (if no Privacy Official has been designated), shall develop and implement a plan, procedures, and a timetable for the implementation of our risk management process in all its aspects. Such actions shall be consistent with our other risk management policies.

Procedures

Responsibilities

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

- **The Chief Information Security Officer**. CISO is responsible for ensuring that the **SoftServe**'s risk management framework meets the requirements of the Board of Directors and of identified legislative or regulatory requirements in terms of risk management.
- **Senior Management.** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates risks requires the support and involvement of senior management. Also, Senior Management stands as **Information Owners (or Primary Asset Owners)** are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.
- **The VP IT.** The VP IT is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
- **Secondary Asset Owners (further SA owners).** SA owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of information within secondary assets they own. Typically the SA owners are responsible for changes to their assets. Thus, they usually have to approve and sign off on changes to their assets (e.g., system enhancement, major changes to the software and hardware). SA owners must therefore understand their role in the risk management process and fully be involved this process:
  identify threats, vulnerabilities, suggest controls and implement them.
- **Business and Functional Managers.** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper information security.

Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated within the organization. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4.

Risk is a function of the **likelihood** of a given **threat** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to information must be analyzed in conjunction with the potential vulnerabilities and the controls in place. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential relative value for the information asset and resources affected. The risk assessment methodology encompasses nine primary steps, which are described in Sections 3.1 through 3.9

- ❑ Step 1 Asset Identification (Section 3.1)
- ❑ Step 2 Threat Identification (Section 3.2)
- ❑ Step 3 Vulnerability Identification (Section 3.3)
- ❑ Step 4 Control Analysis (Section 3.4)
- ❑ Step 5 Likelihood Determination (Section 3.5)
- ❑ Step 6 Impact Analysis (Section 3.6)
- ❑ Step 7 Risk Determination (Section 3.7)
- ❑ Step 8 Control Recommendations (Section 3.8)
- ❑ Step 9 Results Documentation (Section 3.9)

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

Asset Identification

In assessing risks for information, the first step is to define the scope of the effort. In this step, the boundaries of the organization are identified, along with the resources and the information that constitute the system.

Section 3.1.1 describes the system-related information used to characterize an asset. Section 3.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the information processing environment.

System-Related Information

Identifying risk for information requires a keen understanding of the information processing environment. The person or persons who conduct the risk assessment must therefore first collect all possible relative information, which is usually includes:

- ❑ Hardware
- ❑ Software
- ❑ Site
- ❑ Data and information
- ❑ Personnel
- ❑ Network
- ❑ Third Party Services

Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering relative information.

- ❑ **Questionnaire.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting assets. The questionnaire could also be used during on-site visits and interviews.
- ❑ **On-site Interviews.** Interviews with support, operations and management personnel can enable risk assessment personnel to collect useful information (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security.
- ❑ **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned. An organization’s mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.
- ❑ **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently (for example, a network mapping tool).

Output from Step 1 - all relative assets are identified, a good picture of the organizational, environment, and delineation boundaries is established.

Threat Identification

A threat is the potential for a particular threat-origin to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat does not present a risk when there is no vulnerability that can be exercised.

- □ **Threat:** The potential for a threat- source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat Identification

The goal of this step is to identify the potential threats and compile a threat statement listing potential threats that are applicable to the secondary assets being evaluated. A threat is defined as any circumstance or event with the potential to cause harm to an IT system. The common threats can be natural, human, or environmental.

Common Threats

- □ Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- □ Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- □ Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.

A threat is defined as any circumstance or event with the potential to cause harm to information. The common threats-sources can be natural, human, or environmental.

In assessing threats, it is important to consider all potential threats that could cause harm to information and its processing environment. For example, although the threat statement for an information located in a desert may not include "natural flood" because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threats through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threats. Table 3.2.2.1 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threats that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

Table 3.2.2.1: Human Threats.

Threat-Origin	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service)

		• System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Vulnerability Identification

The analysis of the threat to information must include an analysis of the vulnerabilities associated with the organization environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

- ❑ **Vulnerability:** A flaw or weakness in organization’s security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

Vulnerability sources

Vulnerabilities associated within organization can be identified via the information-gathering techniques described in Section 3.1.2.

A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- ❑ Previous risk assessment documentation of the IT system assessed
- ❑ The IT system’s audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- ❑ Vulnerability lists
- ❑ Vendor advisories
- ❑ Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- ❑ Information Assurance Vulnerability Alerts and bulletins for military systems
- ❑ System software security analyses

Control Analysis

The goal of this step is to analyze the controls that have been implemented by the organization to minimize or eliminate the likelihood of the risk. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current controls must be considered.

Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- ❑ Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- ❑ Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

Control Analysis Technique

As discussed in Section 3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization’s control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist’s validity.

Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- ❑ Threat-source motivation and capability
- ❑ Nature of the vulnerability
- ❑ Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat with certain frequency can be described as very high, high, medium, low or very low.

The frequency of threat occurring is assessed by asset owner using the Frequency Table below.

Table 3.5.1: Frequency of threat occurring

Frequency of threat occurring (Level)	Frequency of threat occurring (Description Statements)
Very High	Has happened more than once per year at the Location
High	Has happened of the Location or more than once per year in Organization
Medium	Has happened in our Organization or more than once per year in the Industry
Low	Heard of in the Industry
Very Low	Never heard of in the Industry

The probability of _vulnerability being breached by a threat is assessed by security analyst and/or asset owner using the Probability Table below.

Table 3.5.2: Probability of vulnerability being breached

Probability of vulnerability being breached (Level)	Probability of vulnerability being breached (Description Statements)
Very High	The vulnerability is EXPECTED to be exploited or triggered in most circumstances
High	The vulnerability will PROBABLY be exploited or triggered in most circumstances
Medium	The vulnerability MIGHT be exploited or triggered at some time but is not expected
Low	The vulnerability COULD be exploited or triggered at some time
Very Low	The vulnerability MAY be exploited or triggered in exceptional circumstances

The likelihood level is to be estimated by considering the frequency at which the threat is likely to occur in the future and the probability of the threat exploiting and/or breaching the vulnerability when it does occur: (Likelihood = Frequency of threat occurring x Probability of vulnerability being breached) by asset owner using the Risk Likelihood Matrix below.

Table 3.5.3: Likelihood matrix

		Probability of vulnerability being breached				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Frequency of threat occurring	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- ❑ Information mission
- ❑ Information criticality
- ❑ Information sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

- ❑ If this documentation does not exist or such assessments for the organization's information assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive data is, the SA owners and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).
- ❑ **Loss of Integrity.** System and data integrity refers to the requirement that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the information by either intentional or accidental acts. If the loss information integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality.
- ❑ **Loss of Availability.** If a mission-critical information is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions and customer satisfaction.
- ❑ **Loss of Confidentiality.** Information confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional

disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Table 3.6.1: Risk Impact Level

Impact Level	Impact Level	Financial	Safety	Operational	Reputation	Legal Regulatory
Very High	5	Possible loss>$5M	Permanent injuries / deaths	Catastrophic impact on operations	Extended media coverage; major company embarrassment	Loss of operating license or directors/senior management charged and convicted
High	4	Possible loss $500k - $5M	Permanent injury / stress	Failure of one or more key organizational objectives leading to major disruption	Heavy media coverage	Inquest in to business resulting in an enforcement order fine and court conviction
Medium	3	Possible loss $50k - $500k	Injury requiring medical treatment / long term incapacity	No threat to achievement of objectives but could result in some moderate disruption	Customer comments escalated to management; minor media coverage	Likely fine or prosecution. Administrative undertaking
Low	2	Possible loss $5k - $50k	Injury requiring first aid treatment / temporary loss of time	Minor reduction in effectiveness and efficiency for a short period	Adverse customer comments	Warning issued by regulator
Very Low	1	Possible loss <$5k	Injury resulting in no loss of time	Negligible impact to effectiveness and efficiency	Manageable adverse customer comments	No legal or regulatory consequence

Risk Determination

The purpose of this step is to assess the level of risk to information. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- ❑ The likelihood of a given threat attempting to exercise a given vulnerability
- ❑ The magnitude of the impact should a threat successfully exercise the vulnerability

To measure risk, a risk scale and a risk level matrix must be developed. Table 3.7.1 presents a standard risk level matrix.

Table 3.7.1: Risk Level Matrix

		Impact Level				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Likelihood	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the information to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- ❑ Effectiveness of recommended options

- ❑ Legislation and regulation
- ❑ Organizational policy
- ❑ Operational impact
- ❑ Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact and feasibility of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Results Documentation

Once the risk assessment has been completed the results should be documented in an official reports – Risk Assessment Report (RAR), Risk Treatment Plan (RTP), Risk Treatment Action Plan (RTAP).

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. A risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

A risk treatment plan is a plan of measure what should be taken in regard to identified risks based on risk assessment report. After RTP is approved, RTAP should be prepared where detailed information for controls implementation should be stated: approved budged, schedule, responsible persons, effectiveness measurement methods and its frequency.

Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the **least-cost approach** and implement the **most appropriate controls** to decrease mission risk to an acceptable level, with **minimal adverse impact** on the organization's resources and mission.

This section describes risk mitigation options (Section 4.1), the risk mitigation strategy (Section 4.2), an approach for control implementation (Section 4.3), control categories (Section 4.4), the cost-benefit analysis used to justify the implementation of the recommended controls (Section 4.5), and residual risk (Section 4.6).

Risk Mitigation Options

Risk mitigation is a systematic methodology used by SA owner to reduce risks. Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Tolerance (Acceptance).** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Termination (Avoidance).** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Treatment (Limitation).** To treat the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability, threat frequency or vulnerability probability level of bean breached (e.g., use of supporting, preventive, detective controls)
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and information, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

Risk Mitigation Strategy

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

- □ **When vulnerability (or flaw, weakness) exists →** implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.
- □ **When a vulnerability can be exercised →** apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
- □ **When the attacker's cost is less than the potential gain →** apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- □ **When loss is too great →** apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

The strategy outlined above, with the exception of the third list item ("When the attacker's cost is less than the potential gain"), also applies to the mitigation of risks arising from environmental or unintentional human threats (e.g., system or user errors). (Because there is no "attacker," no motivation or gain is involved).

Approach for control implementation

When control actions must be taken, the following rule applies:

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk mitigation methodology describes the approach to control implementation:

- Step 1- Prioritize Actions

Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization's interest and mission.

Output from Step 1 - **Actions ranking from Very High to Very Low**

- Step 2- Evaluate Recommended Control Options

The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization. During this step, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

Output from Step 2 - **List of feasible controls**

- Step 3 - Conduct Cost-Benefit Analysis

To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted. Section 4.5 details the objectives and method of conducting the cost-benefit analysis.

Output from Step 3 - **Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls**

- Step 4 - Select Control

On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization's mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the information and the organization. During this step, a Develop a Risk Treatment Plan

Output from Step 4 - **Selected control(s)**

- Step 5 - Assign Responsibility

Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

Output from Step 5 - **List of responsible persons, budget and schedule**

- Step 6 - Develop a Risk Treatment Action Plan

During this step, a Risk Treatment Action Plan (or controls implementation plan) is developed. The plan should, at a minimum, contain the following information:

- ❑ Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- ❑ Recommended controls (output from risk assessment report)
- ❑ Prioritized actions (with priority given to items with Very High and High risk levels)
- ❑ Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- ❑ Required resources for implementing the selected planned controls
- ❑ Lists of responsible teams and staff
- ❑ Start date for implementation
- ❑ Target completion date for implementation
- ❑ Maintenance requirements
- ❑ Budget

The controls implementation plan prioritizes the implementation actions and projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. Appendix C provides a sample summary table for the controls implementation plan.

Output from Step 6 - **Risk Treatment Action Plan**

- Step 7- Implement Selected Control(s)

Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk. Residual risk is discussed in Section 4.6.

Output from Step 7 - **Residual risk**

Control Categories

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat damage to an organization's mission.

The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

Cost-Benefit Analysis

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

- □ Determining the impact of implementing the new or enhanced controls
- □ Determining the impact of not implementing the new or enhanced controls
- □ Estimating the costs of the implementation. These may include, but are not limited to, the following:

    - Hardware and software purchases
    - Reduced operational effectiveness if system performance or functionality is reduced for increased security
    - Cost of implementing additional policies and procedures
    - Cost of hiring additional personnel to implement proposed policies, procedures, or services
    - Training costs
    - Maintenance costs

- □ Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

Risk Acceptance

This risk acceptance approach is applied throughout the organization in respect of information risks.

- □ Understand the **nature of risk and business affect** in order to determine the acceptable level of risk.
- □ Assess the risk level in terms of business impact and its likelihood using.
- □ Understand what type of control(s) should be applied to mitigate the risk.
- □ Understand the cost to safeguard and mitigate the risk.
- □ Perform cost/benefit analysis.
- □ Decide whether the risk should be accepted.

Risk that could result in non-compliance with regulation or law, or could result in human harm cannot be accepted.

Table: Risk Acceptance (Last modified: 25 July 2014 - 04:14 PM)

Risk Level	**Responsibility for Risk Acceptance**	**Example (see Table: Risk Calculation Matrix)**
Very High	Shall be mitigated	Possible loss >$5M
High	Board of Directors	Possible loss $500k - $5M
Medium	CEO	Possible loss $50k - $500k
Low	Executive & Senior Management (EVP, SVP, VP)	Possible loss $15k - $50k
Very Low	Middle Level Management (SBU Managers, Department Directors)	Possible loss < $15k

Risk Level as '**Low**' and **'Very Low'** considered as acceptable level. Acceptable risk level was defined taking into account BIA and was approved by BoD.

Residual Risk

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.

Implementation of new or enhanced controls can mitigate risk by -

- □ Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat /vulnerability pairs
- □ Reducing the threat occurring frequency by adding a targeted control to reduce the capacity and motivation of a threat-source
- □ Reducing the magnitude of the adverse impact
- □ Reducing the probability that vulnerability can be breached level.
- □ In some cases control may affect combination of above parameters. For example, control related to physical security decreases vulnerability probability of physical security vulnerability in related risk(s), at same moment this control reduces the threat frequency of physical eavesdropping threat within the network risks.

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no organization's systems are risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

Evaluation and Assessment

In most organizations, the all its parts continually be expanded and updated, its components changed, replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

Security Rule Requirements for Risk Analysis and Risk Management

The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to *"implement policies and procedures to prevent, detect, contain, and correct security violations."*

The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are **Risk Analysis** and **Risk Management**.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to *"implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)]."*

Both risk analysis and risk management are standard information security processes and are critical to a covered entity's Security Rule compliance efforts. As stated in the responses to public comment in the Preamble to the Security Rule, risk analysis and risk management are important

to covered entities since these processes will *"form the foundation upon which an entity's necessary security activities are built." (68 Fed. Reg. 8346.)*
Much of the content included in this paper is adapted from government resources such as the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically *SP 800-30 - Risk Management Guide for Information Technology Systems*. These government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, "*Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.*"

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

Important Definitions to Understand

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including "vulnerability," "threat," and "risk," and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

VULNERABILITY
Vulnerability is defined in NIST SP 800-30 as *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."*

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

THREAT
An adapted definition of threat, from NIST SP 800-30, is "*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- ❑ Natural threats may include floods, earthquakes, tornadoes, and landslides.
- ❑ Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- ❑ Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

RISK
The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

"The net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur.
…Risks arise from legal liability or mission loss due to—

1. *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
2. *Unintentional errors and omissions*
3. *IT disruptions due to natural or man-made disasters*
4. *Failure to exercise due care and diligence in the implementation and operation of the IT system."*

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

Example Risk Analysis and Risk Management Steps

There are numerous methods of performing risk analysis and risk management. There is no single method or "best practice" that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

EXAMPLE RISK ANALYSIS STEPS:

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.

EXAMPLE RISK MANAGEMENT STEPS:

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity "must document" a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

Example Risk Analysis Steps
As previously stated, the Security Rule requires covered entities to conduct an accurate and thorough risk analysis. This section of the paper provides an example approach to risk analysis which may be used by covered entities.

1. Identify the Scope of the Analysis
Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

> *"(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission."*

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity's risk analysis should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

2. Gather Data
Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.
The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity's environment and amount of EPHI held. For example, a small

provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

3. Identify and Document Potential Threats and Vulnerabilities
Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps, but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

IDENTIFY AND DOCUMENT THREATS
Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats.

Covered entities may identify different threats unique to the circumstances of their environment. After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

IDENTIFY AND DOCUMENT VULNERABILITIES
While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both

technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered entities. In contrast, small covered entities will likely rely on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

4. Assess Current Security Measures

The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and nontechnical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EHPI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

5. Determine the Likelihood of Threat Occurrence

Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

“Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used to express the likelihood of occurrence. The ratings used will depend on the covered entity’s approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

- ❑ High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).
- ❑ Medium Likelihood – a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
- ❑ Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

- ❑ Unauthorized access to or disclosure of EPHI.
- ❑ Permanent loss or corruption of EPHI.
- ❑ Temporary loss or unavailability of EPHI.
- ❑ Loss of financial cash flow.
- ❑ Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

QUALITATIVE METHOD

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

QUANTITATIVE METHOD
In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

7. Determine the Level of Risk
Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity’s risk level determination to reasonably anticipated risks to EPHI.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of “high” combined with an impact value of “low” may equal a risk level of “low.” Or a threat likelihood value of “medium” combined with an impact value of “medium” may equal a risk level of “medium.”

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of “high” could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional information to prioritize risk management efforts. One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2),
164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

8. Identify Security Measures and Finalize Documentation

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization's policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation. This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section "Example Risk Management Steps."

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

Example Risk Management Steps

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

1. Develop and Implement a Risk Management Plan

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity's evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity's workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

- ❑ Should certain risks be addressed immediately or in the future?
- ❑ Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- ❑ Risks (threat and vulnerability combinations) being addressed;
- ❑ Security measures selected to reduce the risks;
- ❑ Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity’s actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

2. Implement Security Measures
Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget.

Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

3. Evaluate and Maintain Security Measures
The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

> *"Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 [(the Organizational Requirements)] and this subpart [(the Security Rule)] must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of [EPHI] as described at § 164.316."*

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

> "*Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [EPHI], that establishes the extent to which an entity's security polices and procedures meet the requirements of [the Security Rule]."*

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the EPHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

In Summary
Risk analysis and risk management are the foundation of a covered entity's Security Rule compliance efforts. Risk analysis and risk management are ongoing processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

Policy Number: 11.7
Effective Date: 3/26/2013
Last Revised: 7/28/2014

Risk Analysis Policy

Assumptions

□ **SoftServe Inc.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA regulations.

□ **SoftServe Inc.** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the requirements at § 164.308(a)(1).

□ Risk analysis is an integral part of this organization's overall Risk Management Process Policy and process.

Policy Statement

- □ It is the Policy of **SoftServe Inc.** to conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that we are entrusted with.
- □ Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Official or HIPAA Privacy Officer, or other responsible party (if no Privacy Official has been designated), who shall establish a plan and procedures for the conduct of such analyses.

Procedures

- □ All such risk analyses and assessments shall be conducted periodically, but at least Specify Time Interval (at least annually is suggested).
- □ The risk analysis process shall be modeled upon the risk analysis process recommended by the National Institute for Standards and Technology ("NIST").
- □ The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information
- □ All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy and HIPAA Regulations.

The requirements in respect of a risk assessment tool to deliver an ISO27001-compliant risk assessment as detailed below were drawn from ISO27001:2005 and BS7799-3:2006. The risk assessment tool must address the risk components, relationships between the components, and processes, as described in clauses 5 and 6 of that standard. The additional corporate requirement is that any tool selected must be the least expensive tool available that meets the selection criteria.

The risk assessment tool (Y/N in brackets identifies whether or not BMC RA Module meets the requirement) must enable the Organization to carry out a risk assessment that includes:

- □ Identification of assets [ISO27001 4.2.1 d] ; (Y)
- □ Valuation of the identified assets, taking account of the legal and business requirements and impacts resulting from a loss of confidentiality, integrity and availability [BS7799-3 5.4] (Y);
- □ Identification of significant threats and vulnerabilities for identified assets [ISO27001 4.2.1 e] (Y);
- □ Assessment of the likelihood of the threats and vulnerabilities [ISO27001 4.2.1 e] (Y);
- □ Calculation of risk [ISO27001 4.2.1 e.3] (Y);
- □ Evaluation of risk against a predefined risk scale [BS7799-3 5.8] (Y);
- □ Recording of risk treatment decisions taken, in light of predefined risk acceptance criteria [ISO27001 4.2.1 e.4 and elsewhere] (Y)

- ❑ Risk treatment decisions should include selection of controls from ISO27001 Annex A or from other sources [ISO27001 4.2.1 g] (Y);
- ❑ Storage of initial and subsequent risk assessment results in a database that enables their future review [ISO27001 4.3.1 d through f] (Y).

BMC RA Module

BMC RA Module is a part of BMC Service Desk Tool which allows run Risk Assessment Framework. Its main functions are:

- ❑ Ability to specify level of risk mitigation by each control (countermeasure) - should allow to identify, when applying certain control does not lower risk to acceptable level, mandating secondary control deployment
- ❑ Ability to group assets (or map assets from corporate inventory) into groups with similar threat profile/risk level or scope and applying threats/vulnerabilities/controls on the group level - should decrease time for entering threat/vulnerability combination for each asset
- ❑ Ability to designate:
  - agent - source of the threat
  - threat and frequency of threat occurrence
  - probability of vulnerability breach
- ❑ Support for expanded risk formula: **Risk = Impact x Likelihood = Impact x Frequency of threat occurrence x Probability of vulnerability breach**

Sub-modules

BMC RA Module maintains next sub-modules:

- ❑ **Primary Assets** - information about Primary Asset: Asset Name, Asset Description, Asset Type, In/Out, Owner, impact level for C/I/A also as residual impact level for C/I/A in case control affect primary asset.
- ❑ **Secondary Assets** - information about Secondary Asset: Asset Name, Asset Description, Asset Type, Owner.
- ❑ **Vulnerability** - Information about Vulnerability: Vulnerability Name, Vulnerability Description, Vulnerability Type.
- ❑ **Sec.Asset - Vulnerability** - information related to connection Secondary Asset and Vulnerability: Secondary Asset Name, Vulnerability Name, Actual Vulnerability Probability and Residual Vulnerability Probability in case control affect Vulnerability-Secondary Asset relationship.
- ❑ **Threats** - information about: Threat Name, Threat Description, Threat type, Threat Frequency, Residual Frequency in case we have control affecting the Threat, Affect C/I/A, Origin Accidental/Environmental/Deliberate.

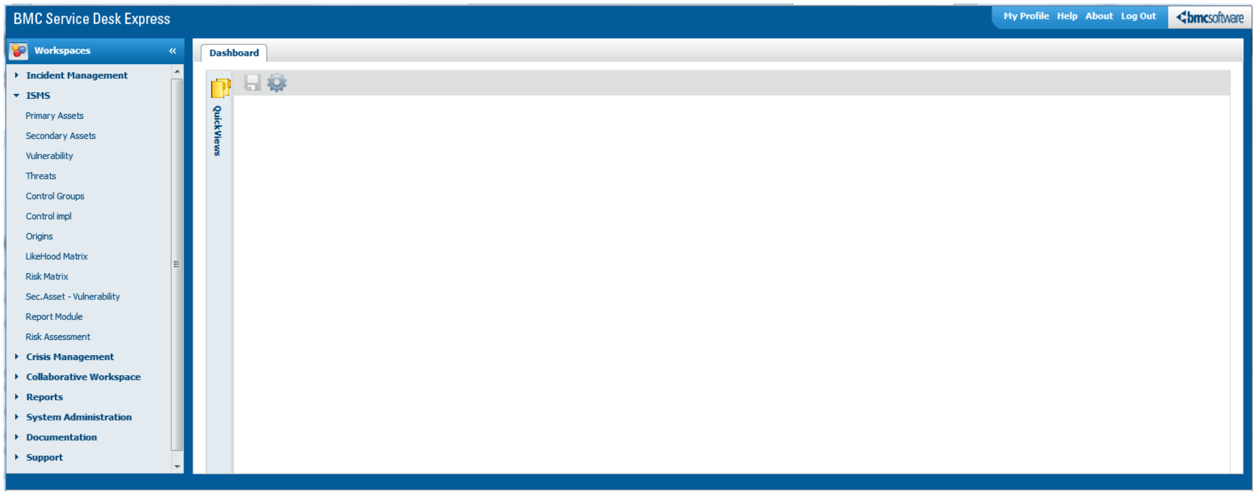
- **Threat origins** - information about Threat origin: Origin Name, Origin Description, Motivation, Possible consequence(s).
- **Control Groups** - information about controls in accordance to ISO/IEC 27001 Annex A Table A.1 – Control objectives and controls: Control Number, Control Name, Control description,
- **Control Impl** - information about specific control (related to existing CI in BMC system): Control Impl Name, Affect P.Asset Impact, Vulnerability Probability, Threat Frequency, Risk handling, Capex budget, Opex budget, Schedule, Scope, Responsible Person: ID, First Name, Last Name, Monitoring Method, Monitoring Frequency, Monitoring responsible person: ID, First Name, Last Name, Is Control Impl effective.
- **LikeliHood Matrix** - supportive sub-module for Likelihood calculation: Threat Frequency, Vulnerability Probability, Likelihood Level.
- **Risk Matrix** - supportive sub-module for Risk calculation: Likelihood, Impact, and Risk.

How module actually works

BMC RA Module is available through internet. All necessary data is collected by using Information-Gathering Techniques described in ISMS DOC 4.1 Risk Management Framework.

3.2.1 Before use, BMC RA Module must be configured appropriately. To start using the module, authorized person should log in at first. If authorization is successful, main window of BMC RA Module appears (pic.3.2.1).

Pic 3.2.1 Main window of BMC RA Module



3.2.2 Process start from setting Primary Assets: Asset Name, Asset Description, Asset Type, In/Out, Owner and impact level for C/I/A;

3.2.3 At next step user fill in all collected information:

- □ Secondary Asset with related Vulnerabilities and current Vulnerability Probability Levels;
- □ Threats which can exploit or trigger Vulnerabilities, Threat Frequency Levels and Threat Origins;
- □ Set connection between appropriate Threats and Vulnerabilities;
- □ Current Control Implementations connected with Threat or Sec.Asset - Vulnerability relationship (depends whether Control affects Threat or Vulnerability);
- □ Each Control Implementation should be provided by appropriate Control Group.

3.2.4 When collected data are set, BMC RA Module will calculate current Risk Levels using LikeliHood Matrix and Risk Matrix;

3.2.5 According to **STEP 8: Control Recommendations** of ISMS DOC 4.1 Risk Management Framework user should set proposed by Asset Owners Controls with residual Vulnerability Probability and Threat Frequency Levels**;**

3.2.6 After all necessary data are set, BMC RA Module will calculate residual Risk Levels.

Report

Risk Assessment Report is a result of providing Risk Assessment in BMC. It is based on reporting system (http://vmsdedbpr/Reports/Pages/Folder.aspx?ViewMode=List).

ISMS Actual RA Report (http://vmsdedbpr/Reports/Pages/Report.aspx?ItemPath=%2fITSM+BMC+Reports%2fISMS%2fISMS+Actual+RA+Report) poses actual risks with currently implemented controls and residual risks with controls what should be in future to reduce a risk.

Document Owner and Approval

The ISMS Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to specified members of staff on the corporate intranet.

This document was approved by the CISO and is issued on a version controlled basis.

References

- ISMS DOC 4.1 Risk Management Framework
- ISO27001 & ISO27002 Training Courses from ITGovernance (UK)

Security Rule Requirements for Risk Analysis and Risk Management

The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to *“implement policies and procedures to prevent, detect, contain, and correct security violations.”*

The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are **Risk Analysis** and **Risk Management**.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”*

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to *“implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)].”*

Both risk analysis and risk management are standard information security processes and are critical to a covered entity’s Security Rule compliance efforts. As stated in the responses to public comment in the Preamble to the Security Rule, risk analysis and risk management are important to covered entities since these processes will *“form the foundation upon which an entity’s necessary security activities are built.” (68 Fed. Reg. 8346.)*
Much of the content included in this paper is adapted from government resources such as the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. These government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, “*Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization’s implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.*"

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

Important Definitions to Understand

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including "vulnerability," "threat," and "risk," and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

VULNERABILITY
Vulnerability is defined in NIST SP 800-30 as *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."*

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

THREAT
An adapted definition of threat, from NIST SP 800-30, is "*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- ❑ Natural threats may include floods, earthquakes, tornadoes, and landslides.
- ❑ Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- ❑ Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

RISK
The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

"The net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur.
…Risks arise from legal liability or mission loss due to—

- *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*

- *Unintentional errors and omissions*
- *IT disruptions due to natural or man-made disasters*
- *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

Example Risk Analysis and Risk Management Steps

There are numerous methods of performing risk analysis and risk management. There is no single method or “best practice” that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

EXAMPLE RISK ANALYSIS STEPS:

- □ Identify the scope of the analysis.
- □ Gather data.
- □ Identify and document potential threats and vulnerabilities.
- □ Assess current security measures.
- □ Determine the likelihood of threat occurrence.
- □ Determine the potential impact of threat occurrence.
- □ Determine the level of risk.
- □ Identify security measures and finalize documentation.

EXAMPLE RISK MANAGEMENT STEPS:

- □ Develop and implement a risk management plan.
- □ Implement security measures.
- □ Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity “must document” a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

Example Risk Analysis Steps

As previously stated, the Security Rule requires covered entities to conduct an accurate and thorough risk analysis. This section of the paper provides an example approach to risk analysis which may be used by covered entities.

1. Identify the Scope of the Analysis

Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

> *"(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission."*

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity's risk analysis should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

2. Gather Data
Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.
The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity's environment and amount of EPHI held. For example, a small provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

3. Identify and Document Potential Threats and Vulnerabilities
Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps, but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

IDENTIFY AND DOCUMENT THREATS
Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats.

Covered entities may identify different threats unique to the circumstances of their environment. After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

IDENTIFY AND DOCUMENT VULNERABILITIES
While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered entities. In contrast, small covered entities will likely rely on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

4. Assess Current Security Measures
The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and nontechnical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EHPI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

5. Determine the Likelihood of Threat Occurrence
Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

“Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used to express the likelihood of occurrence. The ratings used will depend on the covered entity’s approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

❑ High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).

- □ Medium Likelihood – a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
- □ Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

- □ Unauthorized access to or disclosure of EPHI.
- □ Permanent loss or corruption of EPHI.
- □ Temporary loss or unavailability of EPHI.
- □ Loss of financial cash flow.
- □ Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

QUALITATIVE METHOD
The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

QUANTITATIVE METHOD
In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

7. Determine the Level of Risk

Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity's risk level determination to reasonably anticipated risks to EPHI.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of "high" combined with an impact value of "low" may equal a risk level of "low." Or a threat likelihood value of "medium" combined with an impact value of "medium" may equal a risk level of "medium."

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of "high" could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional information to prioritize risk management efforts. One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

8. Identify Security Measures and Finalize Documentation

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization's policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation. This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section "Example Risk Management Steps."

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

Example Risk Management Steps

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

1. Develop and Implement a Risk Management Plan

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity’s evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity’s workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

- ❑ Should certain risks be addressed immediately or in the future?
- ❑ Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- ❑ Risks (threat and vulnerability combinations) being addressed;
- ❑ Security measures selected to reduce the risks;
- ❑ Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity’s actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

2. Implement Security Measures
Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget.

Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

3. Evaluate and Maintain Security Measures
The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

> *"Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 [(the Organizational Requirements)] and this subpart [(the Security Rule)] must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of [EPHI] as described at § 164.316.”*

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

> “*Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [EPHI], that establishes the extent to which an entity’s security polices and procedures meet the requirements of [the Security Rule].”*

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the EPHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

In Summary

Risk analysis and risk management are the foundation of a covered entity's Security Rule compliance efforts. Risk analysis and risk management are ongoing processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.