POLICY AND PROCEDURE TEMPLATES

Security Management Process Policy	Reference Number: a
Department:	Effective Date:
Page:	Replaces Policy Dated:
Approved By: Compliance Officer and *Information Security Officer*	

PURPOSE:

This policy reflects the Company's commitment to ensure the confidentiality,[1] integrity,[2] and availability[3] of its Information Systems containing Sensitive Information,[4] including electronic protected health information by implementing policies and procedures to prevent, detect, mitigate, and correct security violations.

POLICY:

The Company must ensure the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits.

The Company must protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

The Company must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.

The Company must develop and maintain a security management program to protect ePHI and prevent, detect, contain, and correct security violations.

The Company must conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI which the Company may create, receive, maintain, or transmit on behalf of its clients.

The Company must develop and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to protect the confidentiality, integrity, and

[1] HIPAA defines "confidentiality" as "the property that data or information is not made available or disclosed to unauthorized persons or processes."
[2] HIPAA defines "integrity" as "the property that data or information have not been altered or destroyed in an unauthorized manner."
[3] HIPAA defines "availability" as "the property that data or information is accessible and useable upon demand by an authorized person."
[4] Sensitive information is information which, if lost, misused, or unauthorized access to or modification of could adversely affect the interest or the conduct of the Company, or the privacy of individuals (e.g., personally identifiable information (PII), individually identifiable health information (IIHI) or protected health information (PHI). Sensitive information includes technical and proprietary data, information in routine Company payroll, finance, logistics, and personnel management systems.

availability of ePHI which the Company may create, receive, maintain, or transmit on behalf of its clients.

The Company must develop, implement, maintain, manage, and adhere to its respective policies and procedures for system activity controls.

The Company must develop, implement, and maintain reasonable and appropriate policies and procedures to comply with the HIPAA Security standards, implementation specifications, or other requirements.

The Company must perform periodic technical and nontechnical evaluations in response to regulatory, environmental, or operational changes affecting the security of ePHI, that establish the extent to which their policies and procedures meet the HIPAA Security Rule requirements and any subsequent amendments.

PROCEDURE:

MINIMUM REQUIREMENTS FOR SECURITY MANAGEMENT:

A Security Management process requires the Company to implement and adhere to the policies and procedures to prevent, detect, contain, and correct security violations and ensure the confidentiality, integrity, and availability of all ePHI the Company creates, receives, maintains, or transmits. The Security Management process consists of the following four (4) components:

- Risk analysis
- Risk Management
- Sanctions
- Information System Activity Review

Additionally, the Security Management process requires the Company to develop, implement and maintain policies and procedures to protect ePHI. This process requires the Company to perform periodic technical and nontechnical evaluations in response to environmental or operational changes affecting the security of ePHI. Lastly, the Security Management process requires the Company to conduct periodic evaluations upon their policies, procedures, and controls to determine their effectiveness in securing ePHI.

1. Conduct a Risk Assessment

The Company will conduct an accurate and thorough assessment of the potential risks[5] and vulnerabilities[6] to the confidentiality, integrity, and availability of its ePHI. Risk assessments will identify: (i) threats[7] to the Company (i.e., operations, assets, or individuals); (ii) internal and external

[5] Risk is a "measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." NIST SP 800-30, rev. 1 - Guide for Conducting Risk Assessments (Sept. 2012)

[6] Vulnerability is "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." NIST SP 800-30, rev. 1 - Guide for Conducting Risk Assessments (Sept. 2012)

[7] Threat is "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." NIST SP 800-30, rev. 1 - Guide for Conducting Risk Assessments (Sept. 2012)

vulnerabilities to the Company; (iii) the harm (i.e., consequences/impact) that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur.

The Company will generally follow the risk assessment framework found in the following documents:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 rev. 1 – Guide for Conducting Risk Assessments (Sept. 2012);
- NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View Risk Management Guide for Information Systems (March 2011);
- NIST 800-53, rev. 4 (initial public draft)- Security and Privacy Controls for Federal Information Systems and Organizations (Feb 2012);
- NIST SP 800-53A, rev 1 - Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans (June 2010);
- NIST SP 800-66 rev. 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Oct 2008);
- NIST HIPAA Security Rule Toolkit; and
- HHS Guidance on Risk Analysis Requirements under the HIPAA Security Rule.

The Company will utilize the following framework when conducting a risk assessment:

a. Frame the Risk by developing a set of assumptions, constraints, risk tolerances, and priorities/trade-offs that align with the Company's approach for managing risk. This process will include the following activities:

   i. Identify assumptions that affect how the Company assesses, responds to, and monitors its risk; and

   ii. Identify, characterize, and provide representative examples of threat sources, vulnerabilities, consequences/impacts, and likelihood determinations.

b. Select appropriate risk assessment methodologies that reflect the Company's governance, culture, and divergent missions/business functions;

c. Identify the constraints on conducting risk assessment, risk response, and risk monitoring activities within the Company (e.g., financial limitations; legacy information systems dependency; legal, regulatory, and/or contractual);

d. Identify the level of risk tolerance for the Company; and

e. Identify priorities and trade-offs that the Company considers in managing risk.

The Company will conduct a risk assessment on a periodic basis (e.g., annually), upon the occurrence of significant operational/environmental changes, and changes in the legal environment, utilizing the steps outlined in its Risk Assessment policy.

2. Maintain Risk Management Strategy

The Company must develop and maintain a risk management strategy in order to ensure the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits. The risk management framework consists of the following six components:

- Categorize Information System
- Select Security Controls
- Implement Security Controls
- Assess Security Controls
- Authorize Information System
- Monitor Security Controls

a. Categorize Information System

The Information Security Officer and designated IT Department Workforce Members, including contractors, will categorize the Company's information systems in a manner that will include the following activities:

i. Categorize the Company's information system and document results in the security plan;

ii. Describe the Company's information system (including system boundary) and document in the security plan; and

iii. Register the Company's information system with appropriate organizational program/management offices.

b. Select Security Controls

The Information Security Officer and designated IT Department Workforce Members, including contractors, will select security controls for the Company's information systems by minimally conducting the following activities:

i. Identify the Company's security controls as common controls (security controls inherited by one or more of the Company's information systems) for its information systems and document the controls in a security plan (or equivalent document).

ii. Select the security controls for the information system and document the controls in the security plan, which consists of the following:

1. Choosing a set of baseline security controls;

2. Tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance;

3. Supplementing the tailored baseline security controls, with additional controls and/or control enhancements, if necessary, to address unique organizational needs; and

4. Specifying minimum assurance requirements.

iii. Develop continuous monitoring strategy for security control effectiveness. This strategy should include:

1. Configuration management and control processes;

2. Security impact analyses on proposed or actual changes to the Company's information system and its environment of operation;

3. An assessment of selected security controls; and

4. Security status reporting to appropriate Company personnel.

iv. Obtain an independent review and approval of the security plan to ensure completeness, consistency, and satisfaction of stated security information system requirements.

c. Implement Security Controls

To address this component, the Information Security Officer and designated IT Department Workforce Members, including contractors, will implement the selected security controls by minimally conducting the following activities:

i. Implement the security controls specified in the security plan; and

ii. Document the security control implementation and provide a functional description of the control implementation.

d. Assess Security Controls

The Company must assess its security controls through the following processes:

i. Develop, review, and approve a plan to assess the security controls to establish appropriate expectations for the security control assessment; and bind the level of effort for the security control assessment;

ii. Assess security controls in accordance with the security assessment plan's procedures;

iii. Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment; and

iv. Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

e. Authorize Information System

The Company must authorize its information system by performing the following processes:

i. Prepare an action plan and milestones based on the security assessment report findings and recommendations, excluding any remediation actions taken;

ii. Assemble the security authorization package (security plan, the security assessment report, and action plan and milestones[8]) and submit the package to appropriate personnel for adjudication;

iii. Determine the Company's operational, assets, and individuals' risks (including mission, functions, image, or reputation); and

iv. Evaluate the acceptability of the Company's operations, assets, and individuals' risk.

f. Monitor Security Controls

The Company must monitor its security controls, utilizing activities that include the following:

i. Determine the security impact of proposed or actual changes to the information system and its operational environment;

ii. Assess selected technical, management, and operational information system security controls in accordance with the Company's defined monitoring strategy, which will include the following:

1. Test all changes in the staging environment before rolling out to production in order assess the security impact of any changes to the system and environment of operations;

2. Regularly conduct ongoing external vulnerability scanning and internal security testing by the Company's IT staff using the Nessus tool; and

iii. Distribute a report to the Company's management on a weekly basis regarding the status of hosted applications with metrics related to availability, SLA performance, security exceptions and other incidents. Conduct remediation

[8] Action plans and milestones should include (i) reports on progress made on current outstanding items listed in the plan; (ii) address vulnerabilities discovered during the security impact analysis or security control monitoring; and (iii) describe the method for addressing those vulnerabilities.

actions based on ongoing monitoring activity results, risk assessments, and outstanding action plan and milestone items;

iv. Use continuous monitoring process results to update the Company's security plan, security assessment report, and action plan and milestones;

v. Report information system security status to appropriate personnel on an ongoing basis in accordance with the monitoring strategy;

vi. Review the reported information system security status on an ongoing basis in accordance with the monitoring strategy to determine the acceptability of risk to the Company's operations and assets; and

vii. Implement an information system decommissioning strategy.

3. Review Records of Information System Activity

The Company will develop, implement and maintain policies and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to discover system misuse and to identify possible security incidents. This process will require the Company to conduct the following minimal activities:

- Regularly review/analyze audit records for indications of inappropriate or unusual activity;
- Investigate suspicious activity or suspected violations;
- Report findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to the appropriate Company personnel; and
- Take necessary actions in response to the audit record reviews/analyses.

4. Evaluation

The Company will perform periodic technical and nontechnical evaluations in response to environmental or operational changes affecting the security of ePHI, that establish the extent to which their security policies and procedures meet the HIPAA Security Rule requirements and any subsequent amendments. This process will at minimum:

a. Evaluate the appropriateness of the policies, procedures, and controls utilized to protect ePHI;

b. Evaluate changes to the Company's information systems environment and configurations; and

c. Evaluate policies, procedures, and controls at least annually.

5. Documentation

The Compliance Officer and/or Information Security Officer will retain a copy of all documentation related to the Company's security management for six (6) years from the date of its creation, or the date when it last was in effect, whichever is later, and in a manner that is consistent with the Company's Documentation policy.

REFERENCES:

HIPAA Security Rule 45 CFR 164.306(a)(1)(General Requirements) *"Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits."*

HIPAA Security Rule 45 CFR 164.308(a)(1)(i)(Security Management Process) "*Implement policies and procedures to prevent, detect, contain, and correct security violations."*

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(A)(Risk Analysis) "*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."*

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(B) (Risk Management) "*Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."*

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(D)(Information System Activity Review) "*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."*

HIPAA Security Rule 45 CFR 164.316(a)(Policies and Procedures) "*Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of [the Security Rule], taking into account those factors specified in §164.306(b)(2)(i),(ii),(iii), and (iv)."*

Risk Analysis	Reference Number:
Department:	Effective Date:
Page:	Replaces Policy Dated:
Approved By: Compliance Officer and *Information Security Officer*	

PURPOSE:

This standard reflects the Company's commitment to regularly conduct accurate and thorough analysis of the potential risks to the confidentiality, integrity, and availability of its Information Systems containing Sensitive Information.

POLICY:

The Company must 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 Company.

The Company's risk assessment policy must address the purpose, scope, roles, responsibilities, management commitment, coordination among the Company's departments, and its Compliance Officer and Information Security Officer;

The Company must develop, disseminate, and review/update its risk assessment on annual basis.

The Company must implement and maintain formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

The Company must implement adequate security measures to reduce risks and vulnerabilities to a reasonable and appropriate level, based on the findings of the risk assessment.

The Company must conduct a risk assessment on any hardware or software application or process within the Company.

PROCEDURE:

The Company will generally follow the risk assessment framework found in the following documents:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 rev 1 – Guide for Conducting Risk Assessments (Sept. 2012),
- NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View Risk Management Guide for Information Systems (March 2011);
- NIST SP 800-40 vol. 2 - Creating a Patch and Vulnerability Management Program (November 2005);
- NIST 800-53, rev. 4 (initial public draft) - Security and Privacy Controls for Federal Information Systems and Organizations (Feb. 2012);

- NIST SP 800-53A, rev 1 - Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans (June 2010); and

- NIST SP 800-66 rev. 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Oct. 2008).

Using the NIST framework, the Company will evaluate the following areas during the course of its risk assessment:

a. File servers and their processes and procedures through which these systems are administered and/or maintained;

b. Database servers and their processes and procedures through which these systems are administered and/or maintained;

c. Application servers and their processes and procedures through which these systems are administered and/or maintained;

d. Networks and their processes and procedures through which these systems are administered and/or maintained;

e. Portable computing devices, such as laptops, thumb-drives, smart phones, personal digital assistants, CDs, and other portable media, and the associated use, transport, transmission and receipt of, and the disclosure to and from these devices, encryption, media destruction and other protections for the electronic protected health information contained on these devices; and

f. Company policies and procedures relating to ancillary business processes other than IT compliance with State and Federal law, rules and regulations as they may apply to the HIPAA Security and Privacy Rules.

1. Determination of Risk Assessment/Risk Assessment Type

Whenever there is a change in the operational environment, or other triggering event, the Company must conduct a risk assessment. The following triggering events will require the Company to conduct a risk assessment:

a. Time.

The Company must conduct a risk assessment at least every two years to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Company's electronic protected health information.

b. Significant Operational/Environmental Changes.

The Company must conduct a risk assessment upon the determination that the Company has experienced a "significant" operational/environmental change. Additionally, this change would

require a corresponding administrative policy and procedure change that accurately reflects that activity.

c. Changes in the Legal Environment.

The Company must conduct a risk assessment upon the occurrence of material changes in the HIPAA Security and Privacy Rules, federal, state and/or local laws, rules and regulations. A material change is one that causes an effect on the requirements regarding the confidentiality, integrity, and availability of ePHI and requires the Company to make an adjustment in the operationalization of its compliance efforts.

2. Conducting a Risk Assessment

The Compliance Officer and/or Information Security Officer must conduct minimally the following basic steps as part of the risk assessment process:

a. Identify the scope of the risk assessment and determine what department(s) or business area(s) will be the subject of the risk assessment;

b. Identify risk assessment team members;

c. Meet with team members and develop a schedule for the start and end dates of the risk assessment;

d. Present risk assessment project plan to the Company's audit committee and/or leadership council to discuss the dissemination of the tool and other considerations;

e. Once the project has received approval to proceed, provide formal notification to Workforce Members through email and minimally provide the following information:

i. Risk Assessment commencement date;

ii. Department(s) and/or Area(s) to be assessed; and

iii. Projected Risk Assessment end date.

f. Conduct the risk assessment;

g. Incorporate periodic vulnerability scanning activities on the Company's information system and hosted applications to identify and report/remediate new vulnerabilities potentially affecting the system/applications, utilizing the following steps:

i. Employ vulnerability scanning tools (such as web-based application scanners, static analysis tools, binary analyzers) to scan:

1. Patch levels,

2. Functions,

3. Ports,

4. Protocols, and

5. Services that should not be accessible to users or devices, and improperly configured or incorrectly operating information flow control mechanisms.

ii. Employ vulnerability scanning techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting and making transparent, checklists and test procedures; and

3. Measuring vulnerability impact;

iii. Analyze vulnerability scan reports and results from security control assessments;

iv. Remediate legitimate vulnerabilities within 30 days or earlier in accordance with the Company's assessment of risk; and

v. Share the information obtained from the vulnerability scanning process and security control assessments with IT Governance Committee to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

h. Draft the risk assessment report which documents findings and recommendations;

i. Present the report to the Company's compliance board and senior management;

j. Incorporate input from senior management and develop a Company remediation plan; and

k. Evaluate the Company's risk management plan for possible amendments.

3. Documentation

The Compliance Officer and/or Information Security Officer will retain a copy of all risk assessments and related documentation, including any amendments to the risk assessment, and the Company remediation plan for six (6) years as required by and in a manner that is consistent with the Company's Documentation policy.

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(A)(Risk Analysis) "*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.*"

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(B)(Risk Management) "*Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.*"

Data Backup Plan Standard	Reference Number:
Department:	Effective Date:
Page:	Replaces Policy Dated:
Approved By: Compliance Officer and *Information Security Officer*	

PURPOSE:

This standard reflects the Company's commitment to backup and securely store all *Sensitive Information, including ePHI*, on its *Information Systems.*

POLICY:

The Company must utilize procedures for creating a retrievable, exact copy of ePHI, when needed, before the Company moves the equipment.

The Company will protect the confidentiality, integrity, and availability of backup information at its storage locations.

PROCEDURES:

The Company will utilize the following procedures as part of its backup process:

1. The Company will identify a secure, environmentally controlled location for offsite backup media storage, considering:

   a. Geographic area

   The Information Security Officer will consider the distance from the Company to the off-site location and the likelihood of the storage site being affected by the same disaster as the Company;

   b. Accessibility

   The Information Security Officer will consider the length of time necessary to retrieve Sensitive Information, including ePHI, from storage and the storage facility's operating hours;

   c. Security

   The Information Security Officer will ensure that the storage facility's security capabilities and the confidentiality requirements it imposes on its Workforce Members meet or exceed the data's sensitivity and security requirements;

   d. Environment

   The Information Security Officer will review the storage facility's structural and environmental conditions (i.e., temperature, humidity, fire prevention, and power management controls) to determine whether they meet or exceed the data's protection requirements; and

   e. Cost

The Information Security Officer will consider the C's cost of shipping, operational fees, and disaster response/recovery services.

f. Additional considerations.

The Information Security Officer will consider the following when considering a facility:

i. hours of the location;

ii. ease of accessibility to backup media;

iii. physical storage limitations; and

iv. The proposed contract terms for utilizing the location.

2. The Company will make backups of user-level and system-level information contained in its information system on a pre-determined basis that is consistent with the Company's recovery time and recovery point objectives.

3. The Company will make backups of its information system documentation including security-related documentation on a pre-determined basis that is consistent with the Company's recovery time and recovery point objectives.

4. As part of its backup process, the Company perform the following tasks:

a. Test its backup information on a weekly basis to verify media reliability and information integrity;

b. Utilize a sample of its backup information in the restoration of selected information system functions as part of the Company's contingency plan testing process;

c. Store backup copies of its critical information system software (e.g., for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems) and other security-related information (e.g., organizational inventories of hardware, software, and firmware components.) in a separate facility or in a fire-rated container that is not collocated with the operational system;

d. Maintain a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations;

e. Utilize and enforce a two-person rule for the deletion or destruction of Sensitive Information, including ePHI, critical information system software, and other security-related information.

5. In addition to backing up data, the Company will also back up system software and drivers, and store software and software licenses in an alternate location.

6. The Company will back-up image loads for client systems (such as desktops and portable systems) and store at an alternate location, along with the following:

   a. Complete documentation of the software included in the image load;

   b. Any configuration information for the type of computer for which the image is intended; and

   c. Installation instructions.

7. As part of its backup process, the Company will perform the following tasks:

   a. Designate file-naming conventions ;

   b. Describe media rotation frequency;

   c. Prescribe a method for transporting data offsite;

   d. Include documentation that data back-ups have been successfully completed by the scheduled date and time; and

   e. Include a documented procedure for retrieving one or more back up files in a non-disaster mode when files need to be restored due to routine use.

8. The Company will utilize automated processes to backup its Sensitive Information, including ePHI.

9. The Company will utilize the results of its business impact analysis to guide its backup processes.

10. The Company will coordinate its backup storage process with its contingency solutions.

REFERENCES:

HIPAA Security Rule 45 CFR 164.308(a)(7) (ii)(A) (Data Backup Plan) *"Establish and implement procedures to create and maintain retrievable exact copies of Sensitive Information."*

Workforce Sanctions Standard	Reference Number:
Department:	Effective Date:
Page:	Replaces Policy Dated:
Approved By: Compliance Officer and *Information Security Officer*	

PURPOSE:

This standard reflects the Company's commitment to apply appropriate sanctions against Workforce Members who fail to comply with its security policies and procedures.

STANDARD:

The Company must have a formal, documented process for applying appropriate sanctions to Workforce Members who do not comply with its HIPAA policies and procedures. Sanctions must be commensurate with the severity of the non-compliance with the Company's security policies and procedures.

PROCEDURE:

1. Identifying Violations

The Company and appropriate personnel must take the following steps to determine whether a Workforce Member fails to comply with the Company's HIPAA policies and procedures:

a. The Compliance Officer and/or Information Security Officer discover(s) that a Workforce Member may have failed to comply with the Company's HIPAA Privacy and Security policies and procedures;

b. The Compliance Officer and/or Information Security Officer will investigate the incident and determine whether the Workforce Member's activities were non-compliant with the Company's HIPAA policies and procedures. The investigation will include the following components:

i. An evaluation of the facts and circumstances;

ii. An interview with the Workforce Member;

iii. An interview with other Workforce Members and/or contractors who may have knowledge and/or involvement in the particular incident;

iv. A report that documents the findings of the investigation;

v. If the incident involves the unauthorized access, use and/or disclosure of PHI/ePHI, the Compliance Officer and/or Information Security Officer will refer to the Company's *Breach Notification* policy, to evaluate whether the Workforce Member's actions constituted a breach of

PHI/ePHI and comply with the policy's ten (10) step process, including its mitigation, evaluation, notice and logging requirements; and

vi. If the incident requires additional access, use and/or disclosures by law enforcement, health oversight agencies, or judicial and administrative proceedings, the Compliance Officer and/or Information Security Officer will refer to the Company's *Uses and/or Disclosures of Protected Health Information for which an authorization or opportunity to agree or object is not required (No Authorization Required)* policy and procedures.

c. The Compliance Officer and/or Information Security Officer will determine the appropriate sanctions if the findings indicate that the Workforce Member violated the Company's HIPAA policies and procedures, and based on the number and type of past violations, if any;

d. The Company's Human Resources department, after consultation with the Compliance Officer and/or Information Security Officer, will make the recommendation on the sanctions and impose the sanctions on the Workforce Member, documenting the sanctions in a file designated for sanctions and the Workforce Member's personnel file.

e. The Compliance Officer and/or Information Security Officer after review, consultation, and coordination with the Company's Human Resources department, will advise the Workforce Member and his or her department head of the findings and sanctions.`

2. Disciplinary Action Requirements

The Company must take disciplinary action against Workforce Members who fail to comply with the Company's HIPAA policies and procedures in the following manner:

a. Take corrective or disciplinary action against Workforce Members, based on information obtained from evaluating Workforce Member compliance with the Company's HIPAA policies and procedures. This evaluation requires the Company's management and executive team to utilize minimally the following activities to ensure Workforce Member compliance:

i. Monitor workforce member activity and system use;

ii. Audit system logs;

iii. Shadow user sessions;

iv. Review email or other electronic communications; and

v. Investigate reports and claims of Workforce Member HIPAA policy and procedure violations.

b. Vary the type and severity of the sanction based on the type and severity of the violation, whether the violation causes any liability or loss to the Company, the harm to the individuals whose PHI was affected, and/or whether the violation has been repeated.

c. Include termination of Workforce Member employment or use of services, and/or referral for criminal and/or civil prosecution, warnings, or additional security awareness training as potential responses under the sanction process.

d. Apply sanctions equally regardless of job title/position, with no requirements for advance notices, written or verbal warnings, or probationary periods.

3. Disciplinary Action Requirements

The Company will develop, implement, maintain and utilize the following disciplinary actions for Workforce Members who violate or fail to comply with the Company's HIPAA policies and procedures:

a. Dismissal

i. The Company may dismiss any Workforce Member if the Compliance Officer and/or Information Security Officer determines that the Workforce Member engaged in the following activities:

1) Knowingly and maliciously disclosed PHI/ePHI;

2) Attempted to sell or did sell PHI/ePHI, based on a determination of the Compliance Officer and/or Information Security Officer;

3) Accessed PHI/ePHI for personal gain or with malicious harm; or

4) Negligently failed to comply with the Company's HIPAA policy and procedures by disclosing PHI/ePHI, resulting in harm to an individual, Workforce Member or the Company.

ii. In addition to imposing sanctions, including criminal and civil prosecution, the Company should refer to the following policies:

1) The Company's *Uses and/or Disclosures of Protected Health Information for which an authorization or opportunity to agree or object is not required (No Authorization Required)* policy and procedures, if the Compliance Officer and/or Information Security Officer determine(s) that the violation requires

additional disclosures and/or notifications to the following entities:

a. Health oversight agencies;

b. Law enforcement; or

c. Judicial and administrative proceedings; and

2) The Company's *Breach Notification* policy, to evaluate whether the Workforce Member's actions constituted a breach of PHI/ePHI and to comply with the policy's ten (10) steps, including mitigation, evaluation, notice and logging requirements.

3) The Company's *Information Access Management* policy if the imposition of sanctions requires modification or termination of the Workforce Member's access rights to PHI/ePHI.

4) The Company's *Access Controls* policy if the imposition of sanctions requires modification or termination of the Workforce Member's physical access rights to the Company and/or PHI/ePHI.

b. Verbal Counseling

The Company requires the Compliance Officer and/or Information Security Officer, or their respective designees to verbally counsel any Workforce Member when that Workforce Member fails to comply or ensure compliance with any Company HIPAA policy for the first occasion of such violation.

i. For these types of violations, the Compliance Officer and/or Information Security Officer, or their respective designees will verbally counsel the workforce member, and

ii. May require the workforce member to review certain portions of the required HIPAA training curriculum as part of the sanctions and re-education/training process.

iii. The Human Resources Department will log any verbal counseling and remedial HIPAA training in a designated sanctions file and the appropriate workforce member file.

c. Written Counseling

The Company requires its Human Resources Department, in consultation and coordination with the Compliance Officer and/or Information Security Officer, or their respective designees to give written counseling to any Workforce Member when that Workforce Member fails to comply or ensure compliance with any Company HIPAA policies and procedures, and has already received one (1) prior verbal counseling.

i. For these types of violations, the Human Resources Department, after consulting with the Compliance Officer and/or Information Security Officer, or the department's designees will provide written counseling to the Workforce Member for the next occasion of noncompliance; and

ii. May require the Workforce Member to participate in additional in-depth HIPAA training as part of the sanctions process.

iii. The Human Resources Department will log any written counseling and remedial HIPAA training in a designated sanctions file and the appropriate Workforce Member personnel file.

d. Repeated Written Counseling

The Company requires the Human Resources Department or its designees, after consulting the Compliance Officer and/or Information Security Officer, and the Company's legal counsel, if necessary, to dismiss any Workforce Member when that Workforce Member fails to comply or ensure compliance with the Company's HIPAA policies and procedures, and who:

i. Has already completed the steps outlined in subsections (b) and (c) of this section, and

ii. Repeated the steps outlined in subsection (c) of this section, and

iii. Accumulated a total of no more than five (5) written counselings over a floating twelve (12) month period beginning with an initial verbal counseling.

4. Documentation

The Compliance Officer and/or Information Security Officer, Human Resources Department, applicable department head and/ the Company's legal counsel will retain all documents related to Workforce Member sanctions, including the sanctions investigation report, documents relating to the breach notification, and uses and disclosures of PHI/ePHI to law enforcement, health oversight agencies, and judicial and administrative proceedings, and access modification/termination for six (6) years as required by and in a manner that is consistent with the Company's Documentation policy.

REFERENCES:

HIPAA Security Rule 45 CFR 164.308(a)(1)(ii)(C)(Sanction Policy) “Apply appropriate sanctions against Workforce Members who fail to comply with the security policies and procedures of the covered entity.”

HIPAA Security Rule 45 CFR 164.316(b)(1)(Documentation) “If an action, activity or assessment is required by [the Security Rule] to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.”

HIPAA Security Rule 45 CFR 164.316(b)(2)(i)(Time Limit) “Retain the documentation required by paragraph (b)(1) of this section for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.”

HIPAA Privacy Rule 45 CFR §164.530(e)(2)(Documentation) “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 [the Privacy Rule].” (This applies when Workforce Member activities involve the unauthorized use, disclosure, alteration, or destruction of PHI)

HIPAA Privacy Rule 45 CFR §164.530(j)(1)(ii)(Documentation) “If a communication is required by [the Privacy Rule] to be in writing, maintain such writing, or an electronic copy, as documentation.”

HIPAA Privacy Rule 45 CFR §164.530(j)(1)(iii)(Documentation) “If an action, activity, or designation is required by [the Privacy Rule] to be documented, maintain a written or electronic record of such action, activity, or designation.”

HIPAA Privacy Rule 45 CFR §164.530(j)(2)(Retention period) “Retain the documentation required by [HIPAA Privacy Rule 45 CFR §164.530(j)(1)] for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.” (This applies when Workforce Member activities involve the unauthorized use, disclosure, alteration, or destruction of PHI)