*The following security policies and procedures have been developed by AIG Business Solution (P) Ltd. for its internal use only in its role as a hybrid entity under HIPAA. These policies and procedures were developed to bring company into compliance with the Health Insurance Portability and Accountability Act of 1996 Security Rule.*

# HIPAA Security Policies and Procedures Table of Contents

Contents

[1. Executive Summary 3](#_Toc471233665)

[1.1 Introduction 3](#_Toc471233666)

[1.2 Scope 4](#_Toc471233667)

[2. Administrative Safeguards 8](#_Toc471233668)

[2.1 Security Management Process (164.308(a)(1)) 8](#_Toc471233669)

[2.2 Assigned Security Responsibility (164.308(a)(2)) 10](#_Toc471233670)

[2.3 Workforce Security (164.308(a)(3)) 11](#_Toc471233671)

[2.4 Information access Management (164.308(a)(4) 12](#_Toc471233672)

[2.5 Security Awareness and Training (164.308(a)(5)) 13](#_Toc471233673)

[2.6 Security Incident Procedures (164.308(a)(6)) 15](#_Toc471233674)

[2.7 Contingency Plan (164.308(a)(7)) 17](#_Toc471233675)

[2.8 Evaluation (164.308(a)(8)) 19](#_Toc471233676)

[2.9 Business Associate Contracts and Other Arrangements (164.308(b)(1)) 21](#_Toc471233677)

[3. Physical Safeguards 23](#_Toc471233678)

[3.1 Facility Access Controls (164.310(a)(1)) 23](#_Toc471233679)

[3.2 Workstation Use (164.310(b)) 25](#_Toc471233680)

[3.3 Workstation Security (164.310(c)) 26](#_Toc471233681)

[3.4 Device and Media Controls (164.310(d)(1)) 27](#_Toc471233682)

[4. Technical Safeguards 28](#_Toc471233683)

[4.1 Access Control (164.312(a)(1)) 28](#_Toc471233684)

[4.2 Audit Control (164.312(b)) 30](#_Toc471233685)

[4.3 Integrity (164.312(c)(1)) 32](#_Toc471233686)

[4.4 Person or Entity Authentication (164.312(d)) 34](#_Toc471233687)

[4.5 Transmission Security (164.312(e)(1) 35](#_Toc471233688)

[SECTION I 48](#_Toc471233689)

[AIG Business Solution (P) Ltd. Server IT Security Procedures 48](#_Toc471233690)

[SECTION II 49](#_Toc471233691)

[AIG Business Solution (P) Ltd. Data Classification 49](#_Toc471233692)

[PUBLIC 49](#_Toc471233693)

[PRIVATE 49](#_Toc471233694)

[CONFIDENTIAL 50](#_Toc471233695)

[AIG Business Solution (P) Ltd. Network IT Security Procedures 51](#_Toc471233696)

[Acceptable Use Policy 51](#_Toc471233697)

[Enforcement through Access Control Lists 55](#_Toc471233698)

[Physical Security 55](#_Toc471233699)

[Entity Authentication procedures 58](#_Toc471233700)

[Password Policy 58](#_Toc471233701)

[Policies and procedures to address security incidents 61](#_Toc471233702)

[Data Security 61](#_Toc471233703)

[AntiVirus Policy 61](#_Toc471233704)

[Firewall Policy 63](#_Toc471233705)

[Clear Desk and Screen Policy 64](#_Toc471233706)

[Activating and modifying accounts to laptops / workstations and EHR systems 65](#_Toc471233707)

[New User Registration/ Deregistration/ Access Control Policy 65](#_Toc471233708)

[Policy and procedures that specify audit and accountability 67](#_Toc471233709)

[HIPAA Compliance Team 67](#_Toc471233710)

[Human Resources 67](#_Toc471233711)

[HIPAA Training 68](#_Toc471233712)

[Legal and Regulatory Compliance Policy 68](#_Toc471233713)

[IT Security Standards for Servers and Desktops 70](#_Toc471233714)

[Policy and procedures that specify physical and environmental safeguards used 72](#_Toc471233715)

[Physical Access Policy Standard 72](#_Toc471233716)

[Email Policy (HIPAA) 75](#_Toc471233717)

[Internet Policy 77](#_Toc471233718)

[Document Control 79](#_Toc471233719)

[Glossary 82](#_Toc471233720)

[Abbreviation 86](#_Toc471233721)

## 1. Executive Summary

This document summarizes the HIPAA security standards and explains some of the structure and organization of the

Security Rule. The document was created to help educate readers about security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security safeguards set out in the Rule. This document is intended as an aid/resource to understanding security concepts discussed in the HIPAA Security Rule and does not supplement, replace, or supersede the HIPAA Security Rule itself.

The HIPAA Security Rule focuses on the safeguarding of electronic protected health information (EPHI). All covered entities under HIPAA must comply with the HIPAA Security Rule, which establishes a set of security standards for protecting certain health care information.

The standards and guidelines listed in this document can be used to support the requirements of HIPAA. These standards are based on the objectives of providing appropriate levels of information security according to a range of risk levels. The guidelines recommend the types of information and information systems to be included in each category. In addition, this document will also recommend minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each category.

Emphasis will be placed on:

* Ensuring an information security program in place and trained personnel assigned to manage and support the program
* Integration of security in the business processes
* Implementation and management of a security plan to manage the security requirements set forth by the HIPAA Security Rule

### 1.1 Introduction

Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to simplify and standardize health care administrative processes, thereby reducing costs and other burdens on the health care AIG Business Solution (P) Ltd. try. The HIPAA statute comprises five titles:

Title I HIPAA Health Insurance Reform

Title II HIPAA Administrative Simplification

Title III HIPAA Tax Related Health Provisions

Title IV Application and Enforcement of Group Health Plan Requirements

Title V Revenue Offsets

Title II, includes the HIPAA administrative simplification requirements that address how electronic health care transactions are transmitted and stored. Pursuant to these provisions of HIPAA, the Secretary of Health and Human Services (HHS) adopted several sets of rules (in addition to the Security Rule) implementing the HIPAA administrative simplification requirements.

HHS has published, proposed or final rules related to the following five components of health care AIG Business Solution (P) Ltd. try practices:

* Code sets used to identify health care services
* Identifiers used for unique designations for employers and health care providers
* Electronic data interchange transactions
* Security
* Privacy

This document addresses only the security component of the HIPAA statute.

### 1.2 Scope

This document is designed to help educate AIG Business Solution (P) Ltd. personnel about IT security concepts included in the HIPAA Security Rule. It is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, and does not supplement, replace, or supersede the Security Rule itself. Anyone seeking clarifications of the HIPAA Security Rule should send e-mail to askhipaa@cms.hhs.gov, or contact the CMA HIPAA hotline at 1866-282-0659. This hotline was established for the specific purpose of providing assistance with questions related to HIPAA and its requirements.

#### 1.2.1 HIPAA Security Rule

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). All covered entities under HIPAA must comply with the HIPAA Security Rule, which establishes a set of security standards for securing certain health information. As per general HIPAA standards, covered entities are the ones that meet the following descriptions:

* Health Care Providers - Any provider of medical or other health services, or supplies, that transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.
* Health Plans - Any individual or group plan that provides or pays the cost of health care.
* Health Care Clearinghouses - Any public or private entity that processes health care transactions from a standard format to a nonstandard format, or vice-versa.

This section summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule.

#### 1.2.2 HIPAA Goals and Objectives

The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of electronic protected health information (EPHI).

* **Confidentiality** is the “property that data or information is not made available or disclosed to unauthorized persons or processes.”
* **Integrity** is the “property that data or information has not been altered or destroyed in an unauthorized manner.”
* **Availability** is “the property that data or information is accessible and usable upon demand by an authorized person.”

#### 1.2.3 Security Rule Organization

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security measures. Each security measure of the HIPAA Security Rule can be categorized as being an Administrative, Physical or Technical safeguard.

* Administrative safeguards are defined as the “administrative actions, policies, and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”
* Physical safeguards are defined as the “security measures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.”
* Technical safeguards are defined as the “technology and the policy and procedures for is use that protect electronic protected health information and control access to it.”

Each security safeguard can also be categorized as being either a standard or an implementation specification. An “implementation specification” is a more detailed description of the method or approach that covered entities can use to meet a particular standard. Each set of safeguards comprises a number of specific implementation specifications that are either required or addressable. If an implementation specification is described as required, the specification must be implanted. If it is addressable, then the covered entity must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment. If the covered entity chooses not to implement a specification, the entity must either document the reason or implement an alternative measure.

These categories of safeguards encompass the continuum of security for electronic health care information for covered entities under HIPAA. The security process begins with the policies and the procedures that establish personnel behavior and provide a framework for acceptable access to and uses of protected health information. These administrative controls are the foundation for the HIPAA Security Rule. The physical safeguards support limitations to restricted spaces and equipment, including materials that contain electronic protected health information. Technical safeguards apply specifically to information systems and are measures of protection associated with the actual hardware, software, and networks for these systems.

1.2.4 HIPAA Security Standards and Implementation Specifications

Table 1. HIPAA Security Standards and Implementation Specifications[[1]](#footnote-1)

|  |  |  |  |
| --- | --- | --- | --- |
| **Standards** | **Sections** | **Implementation Specifications** | |
| **Required** | **Addressable** |
| **Administrative Safeguards** | | | |
| Security Management Process | 164.308(a)(1) | * Risk Analysis * Risk Management * Sanction Policy * Information System Activity * Review |  |
| Assigned Security Responsibility | 164.308(a)(2) | * None |  |
| Information Access Management | 164.308(a)(4) | * Isolating Health Care Clearinghouse * Function | * Access Authorization * Access Establishment and Modification |
| Security Awareness Training | 164.308(a)(5) | * None | * Security Reminders * Protection from Malicious Software * Log-in Monitoring * Password Management |
| Security Incident Protection | 164.308(a)(6) | Response and Reporting |  |
| Contingency Plan | 164.308(a)(7) | * Data Backup Plan * Disaster Recovery Plan * Emergency Mode Operation Plan | * Testing and Revision Procedure * Applications and Data Criticality Analysis |
| Evaluation | 164.308(b)(1) | None |  |
| Business Associate Contracts and Other Arrangements | 164.308(b)(1) | Written Contract or Other Arrangement |  |
| **Physical Safeguards** | | | |
| Facility Access Controls | 164.310(a)(1) | * None |  |
| Implementation Specifications | 164.310(a)(2) | * None | * Contingency Operations * Facility Security Plan * Access Control and Validation Procedures * Maintenance Records |
| Workstation Use | 164.310(b) | * None |  |
| Workstation Security | 164.310(c) | * None |  |
| Device and Media Controls | 164.310(d)(1) | * Disposal * Media Re-use | * Accountability * Data Backup and Storage |
| **Technical Safeguards** | | | |
| Implementation Specifications | 164.312(d)(2) | * None |  |
| Access Control | 164.312(a)(1) | * Unique User Identification * Emergency Access Procedure | * Automatic Logoff * Encryption and Decryption |
| Audit Control | 164.312(b) | * None |  |
| Integrity | 164.312(c)(1) | * None | * Mechanism to Authenticate Electronic * Protected Health Information |
| Person or Entity | 164.312(d) | None |  |
| Transmission Security | 164.312(e)(1) | None | Integrity Controls  Encryption |

This section associates AIG Business Solution’s Policy and Procedure for Computer, Network Usage, Acceptable Use of Electronic Communications Devices, and Computer and Electronic Communications

Facilities, with the respective Security Rule topic standards to facilitate their use in applying the HIPAA Security Rule. Each HIPAA Security Rule standard is outlined in a tabular module format. The modules are composed of the following components:

The **Key Activities** column lists for each HIPAA Security Rule standard some suggested key activities that are usually associated with a particular security function. The activities are not all-inclusive, and there may be many additional activities an entity will need to consider, specific to its own operations. Note that the HIPAA Security Rule associates several “implementation specification: for each standard, as listed in Table 1. Not all modules address all the standard’s associated implementation specifications, as they are meant to serve as a general introduction to the security topics raised by the standards of the HIPAA Security Rule.

The **Descriptive** column includes an expanded explanation about the key activities. The descriptions include types of activities an organization may pursue in addressing a specific security function. These abbreviated explanations are designed to help get an entity started in addressing the HIPAA Security Rule.

The **Questions** will help to determine whether or not the elements described have actually been considered or completed. They serve as a starting point for the entity to examine its security practices as they relate to the HIPAA Security Rule. Affirmative answers to the questions do not imply that the entity is meeting all of the requirements of the HPAA security requirement. However, if an entity has already incorporated considerations raised by these questions into its information security program, those efforts may signal that the entity is taking appropriate steps. It is expected that many entities with existing information security infrastructures already in place will have considered the HIPAA Security Rule and have taken steps to incorporate policies and procedures tailored to fit the requirements of the HIPAA Security Rule.

## 2. Administrative Safeguards

### 2.1 Security Management Process (164.308(a)(1))

HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Activities** | | **Description** | **Questions** |
| 1. Identify Relevant Information Systems | | * Identify all information systems that house individually identifiable health information. * Include all hardware and software that are used to collect, store, process, or transmit protected health information. * Analyze business functions and verify ownership and control of information system elements as necessary. | * Has all the hardware and software for which the organization is responsible been identified and inventoried? * Is the current information system configuration documented, including connections to other system? Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated? |
| 2. Conduct Risk Assessment | | **Risk assessment typically includes the following steps:**   * Determine system characterization: * Hardware * Software * System interfaces * Data and information * People System mission. * Identify any vulnerability or weakness in security procedures or safeguards. * Identify events that negatively impact security. * Identify the potential impact that a security breach could have on an entity’s operations or assets, including loss of integrity, availability, or confidentiality. * Recommend security controls for the information and the system, including all the technical and nontechnical protections in place to address security concerns. * Determine residual risk. * Document all outputs and outcomes from the risk assessment activities. | * Are there any prior risk assessments, audit comments, security requirements, and/or security test results? * Are there resources available? (I.e., ITS, AIG Business Solution (P) Ltd., Listservs, mass media, virus alerts, vendors, etc.) * What are the current and planned controls? * Is the facility located in a region prone to any natural disasters such as earthquakes, floods, or fires? Has responsibility been assigned to check all hardware and software to determine whether selected settings are enabled? And, unnecessary settings disabled? * Is there an analysis of current safeguards on effectiveness relative to the identified risks? |
| 3. | Acquire IT Systems and Services | * Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Consideration for their selection should include the following: * Applicability of the IT solution to the intended environment. The sensitivity of the data. * The organization’s security policies, procedures and standards. Other requirements such as resources available for operation, maintenance, and training. | * How will new security controls work with the existing IT structure? Have the security requirements of the organization been compared with the security features of existing or proposed hardware and software? Has a cost-benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified? * Has a training strategy been developed? |
| 4. | Create and Deploy Policies and  Procedures | * Document the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. * Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices. Create procedures to be followed to accomplish particular security related tasks. | * Are policies and procedures in place for security? (Refer to current * AIG Business Solution (P) Ltd./AIG Business Solution (P) Ltd. security policies and procedures in place.) * Are there user manuals available and are they up-to-date? (Refer to current HR manuals and employee/ staff manuals available.) * Is there a formal documented system/department security plan? Is there a process for communicating policies and procedures reviewed and updated as needed? * (e.g., is this addressed during regularly scheduled staff meetings?) |

### 2.2 Assigned Security Responsibility (164.308(a)(2))

HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Select a Security Official to be Assigned Responsibility for HIPAA Security | * Identify the individual[[2]](#footnote-2) who will ultimately be responsible for security * Select an individual who is able to assess the effective security and to serve as a point of contact for security policy, implementation and monitoring.2 | * Who in the organization: * Oversees the development and communication of security policies and procedures? * Is responsible for conducting the risk assessment? * Handles the results of periodic security evaluations? * Directs IT security purchasing and investment? * Ensures that security concerns have been addressed in system implementation? |
| 2. | Assign and Document the Individual’s Responsibility | * Document the individual’s responsibilities in a job description. * Communicate this assigned role to the entire organization. | * Is there a complete job description that accurately reflects the assigned security duties and responsibilities? Have the staff members in the organization been notified as to whom to call in the event of a security problem? |

### 2.3 Workforce Security (164.308(a)(3))

HIPAA Standard: Implement policies and procedures to ensure that all members of the workforce have appropriate access to electron protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraphs (a)(4) of this section from obtaining access to electronic protected health information.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Establish Clear Job Descriptions and Responsibilities | * Define roles and responsibilities for all job functions. * Assign appropriate levels of security oversight, training, and access. Identify, in writing, who has the business need - and who has been granted permission - to view, alter, retrieve, and store electronic health information, and at what times, under what circumstances, and for what purposes. | * Are there written job descriptions that are correlated with appropriate levels of access? * Is there an implementation strategy that supports the designated access authorities? |
| 2. | Establish Criteria and Procedures for Hiring and Assigning Tasks | * Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill specific roles, * e.g., positions involving access and use of sensitive information. Ensure that these requirements are included as part of the personnel hiring process. | * Are applicant’s employment and education references checked? Have appropriate background checks been completed * Have confidentiality agreements stressing privacy and security been signed by the staff member? |
| 3. | Establish Termination Procedures | * Develop a standard set of procedures that should be followed to recover access control devices (Identification [ID] badges, keys, access cards, etc.) when employment ends. * Deactivate computer access accounts (e.g., disable user IDs and passwords). See the Access Controls Standards. | * Are there separate procedures for voluntary termination (retirements, promotion, change of employment) vs. involuntary terminations? * (termination for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions)? Is there a standard checklist for all action items that should be completed when an employee leaves * (return of all access devices, deactivation of log-on accounts, delivery of any needed data solely under the employee’s control)? |

### 2.4 Information access Management (164.308(a)(4)

HIPAA Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements for subpart E of this part.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Determine Criteria for Establishing  Access | * Decide how the person with the assigned security responsibility will consistently grant access to others within the organization. * Document which process will be used to select the basis for restricting access. * Choose between identity-based access (by name) or role-based access (by job or other appropriate means). | * Does the organization’s IT operating system have the capacity to set access controls? * Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties? Will access be identity-based on their job requirements? |
| 2. | Determine Who Should be Authorized to Access Information Systems | * Establish standards for granting access. * Provide formal authorization from the appropriate authority before granting access to sensitive information. | * Are duties separated such that only the minimum necessary electronic health information is made available to each staff member based on their job requirements? |
| 3. | Evaluate Existing Security Measures Related to Access Controls | * Evaluate access controls already in place or implement new access controls as appropriate. * Coordinate with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification, and authentication of users, and physical access controls. | * Are access policies reviewed and updated routinely? * Do all employees receive appropriate security training? * Are authentication mechanisms used to verify the identity of those accessing systems? * Does management regularly review the list access authorizations and update as necessary? * What policies and procedures are already in place for access control safeguards? |

### 2.5 Security Awareness and Training (164.308(a)(5))

HIPAA Standard: Implement security awareness and training program for all members of its workforce (including management).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Conduct a Training Needs Assessment | * Determine the training needs of the organization. * Interview and involve key personnel in assessing security training needs. | * What awareness, training, and education programs are needed (e.g., what is required)? * What is the current status regarding how these needs are being addressed (e.g., how well are current efforts working)? * Where are the gaps between the needs and what is being done (e.g., what more needs to be done)? * What are the training priorities? |
| 2. | Develop and Approve a Training  Strategy and a Plan | * Address the specific HIPAA policies that require awareness and training in the written training strategy. * Outline the written training plan, the scope of the awareness and training program; the goals; the target audiences; the learning objectives; the deployment methods, evaluation, and measurement techniques; and the frequency of training. | * Is there a procedure in place to ensure that everyone in the organization receives security awareness training? * What type of security training is needed to address specific technical topics based on job responsibility? When should training be scheduled to ensure that compliance deadlines are met? * Is security awareness discussed with all new hires (e.g., employee orientation)? * Are security topics reinforced during routine staff meetings? |
| 3. | Develop Appropriate Awareness and Training Content; Create Training Materials; and Determine Best  Delivery Methods | * Select the topics that may need to be included in the training materials such as the following: * Security reminders. * Incident reporting. * How to protect and guard the system from malicious software. Procedures for monitoring login attempts and reporting discrepancies. * Password management and use. Use new and “hot” information from e-mail advisories, online IT security daily news web sites, and periodicals. | * Have employees received a copy of or do they have easy access to the security procedures and policies? Do employees know whom to contact and how to handle a security incident? * Do employees understand the consequences of noncompliance with the stated security policy? * Are employees who travel aware of both physical laptop security issues and how to handle them? * Do employees know the importance of timely application of system patches? |
| 4. | Develop Appropriate Awareness and Training Content; Create Training Materials; and Determine Best  Delivery Methods (Cont’d) | * Deliver training information to staff in the easiest and most cost-efficient manner. * Consider using a variety of media and avenues according to what is appropriate for the organization based on workforce size, location, level of education, etc. | * Is there in-house training staff? What is the security training budget? |
| 5. | Implementing the Training | * Schedule and conduct the training outlined in the strategy and plan. Implement any reasonable technique to disseminate the security message in an organization, including newsletters, screensavers, videotapes, e-mail messages, teleconferencing sessions, staff meetings, and computer-based training. | * Have all employees received adequate training to fulfill their security responsibilities? * What methods are available or already in use to make employees aware of security (e.g., posters or booklets, Web tutorials, Web sites)? |
| 6. | Monitor and Evaluate Training Plan | * Keep the security awareness and training program fresh and current. Conduct training whenever changes occur in the technology and practices as appropriate. * Monitor the training program implementation to be sure all employees participate. * Implement corrective actions when problems arise. | * Are employee training and professional development programs documented and monitored (e.g., responsibility review)? * Is there annual security refresher training? * How are new employees trained on security? |

### 2.6 Security Incident Procedures (164.308(a)(6))

HIPAA Standard: Implement policies and procedures to address security incidents.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Determine Goals of Incident Response | * Gain an understanding as to what constitutes a true security incident - something identified as a security breach or an attempted “hack” - in the organization’s environment. Determine how the organization will respond to a security breach. Establish a reporting mechanism and a process to coordinate responses to the security incident. Provide direct technical assistance, advise vendors to address productrelated problems and provide liaisons to legal and criminal investigative groups as needed. | * Has the HIPAA-required security risk assessment resulted in a list of potential physical or technological events that could result in a breach of security? * Is there a procedure in place for reporting and handling incidents? Has an analysis been conducted that related each potential security incident to possible results? * Have the key functions of the organization been prioritized to determine what would need to be restored first in the event of a disruption? |
| 2. | Develop and Deploy an Incident  Response Team | * Identify appropriate individuals to be part of a formal incident response team, when required. | * Do members of the team have adequate knowledge of the organization’s hardware and software? Do members of the team have the authority to speak for the organization to the media, law enforcement, and clients or business partners? Has the incident response team received appropriate training in incident response activities? |
| 3. | Develop Incident Response Procedures | * Document incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team. * Review incident procedures. Update the procedures as required, based on changing organizational needs. | * Does the organization’s size and mission suggest that a staffed security incident hotline be maintained? Does the organization need standard incident report templates to ensure that all necessary information related to the incident is documented and investigated? * Has the organization determined under what conditions information related to a security breach will be disclosed to the media? * Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared? * Has a written incident response plan been developed and provided to the team? |
| 4. | Incorporate Post-Incident Analysis into Updates and Revisions | * Measure effectiveness and update security incident response procedures to reflect lessons learned, and make recommendations for improvements to security controls after a security incident. | * Does the incident response team keep adequate documentation of security incidents that list what weaknesses were exploited and how access to information was gained? Do records reflect new contacts and resources identified for responding to an incident? * Does the organization consider whether current procedures were adequate for responding to a particular security incident? |

### 2.7 Contingency Plan (164.308(a)(7))

HIPAA Standard: 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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Develop Contingency Planning Policy | * Define the organization’s overall contingency objectives. * Establish the organizational framework, roles, and responsibilities for this area. * Address scope, resource requirements, training, testing plan maintenance, and backup requirements. | * What are the primary missions of the entity? * What services must be provided within specified critical timeframes? (Patient treatment, for example, may need to be performed without disruption. By contrast, claims processing may be delayed during an emergency with no long-term damage to the organization.) * Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one? |
| 2. | Conduct an Impact Analysis  (Applications and Data Criticality  Analysis) | * Identify the activities and material that are critical to business operations. * Identify the critical services or operations and the manual and automated processes that support them. Determine the amount of time the organization can tolerate power outages, disruption of services, and/ or loss of capability. * Establish cost-effective strategies for recovering these critical services or processes. | * What hardware, software, and personnel are critical to daily operations? * What is the impact on desired service levels if these critical assets are not available? * What, if any, support is provided by external providers (Internet service providers [ISPs], utilities, or contractors)? * What is the nature and degree of impact on the operation, if any, if the critical resources are not available? |
| 3. | Identify Preventive Measures | * Identify preventive measures for each defined scenario that could result in loss of critical service operation. * Ensure identified preventative measures are practical and feasible in terms of their applicability ina given environment. | * What alternatives for continuing operations of the organization are available in case of loss of any critical function/resource? * What is the cost associated with the preventive measures that may be considered? * Are the preventive measures feasible (affordable and practical for the environment)? * What plans, procedures, or agreements need to be initiated to enable implementation of the preventive measures? |

|  |  |  |  |
| --- | --- | --- | --- |
| 4. | Develop Recovery Strategy | * Finalize the set of contingency procedures that should be invoked for all identified impacts including emergency mode operation. The strategy must be adaptable to the existing operating environment and address allowable outage times and associated priorities identified in Step 2. * Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated. | * Have agreed-upon procedures for each possible type of impact identified been documented? * Has a coordinator who manages, maintains, and updates the plan been designated? * Has an emergency call list been distributed to all employees? Have recovery procedures been documented? * Has a determination been made regarding when the plan needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivers, etc.)? |
| 5. | Develop the Contingency Plan | * Document all decisions made in the previous steps. | * Is there a written plan? * Does it address both disaster recovery and data backup? |
| 6. | Plan Testing, Training, and Execution | * Test the contingency plan on a predefined cycle (stated in policy development under Step 1). * Train those with defined plan responsibilities in their roles. * If possible, involve external entities (vendors, alternative site/service providers) in testing exercises. Make key decisions regarding how the testing is to occur (“tabletop” exercise versus staging a real operational scenario including actual loss of capability). * Decide how to segment the type of testing based on the assessment of business impact and acceptability of sustained loss of service. Consider cost. | * How is the plan to be tested? Does testing lend itself to a phased approach? * Is it feasible to actually take down functions/services for the purpose of testing? * Can testing be done during normal business hours, or must it take place during off-hours? * If full testing is infeasible, has a “tabletop” scenario (classroom-like exercise) been considered? How frequently is the plan to be tested (annually)? * When should the plan be revised? |

### 2.8 Evaluation (164.308(a)(8))

HIPAA Standard: Perform a periodic technical and non-technical evaluation based on 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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Determine Whether Internal or External Evaluation is Most Appropriate | * Decide whether the evaluation will be conducted with internal staff resources or external consultants. Engage external expertise to assist the internal evaluation team where additional skills and expertise is required. * Use internal resources to supplement an external source of help, because these internal resources can provide the best institutional knowledge and history of internal policies and practices. | * Which staff has the technical expertise and experience to evaluate the system? * How much training will staff need on security-related technical and non-technical issues? * What are the credentials required for an outside vendor? * What is the budget for internal resources to assist with an evaluation? Can other external organizations provide assistance if needed? |
| 2. | Develop Standards and Measurements for All Areas and Topics of Security | * Use an evaluation strategy and tool that has substance and can be tracked, such as a questionnaire or checklist, because documentation is key to demonstrating compliance. Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard. * If available, engage corporate, legal, or regulatory compliance staff when conducting the analysis. * Leverage any existing reports or documentation that may already be prepared by the organization addressing compliance, integration, or maturity of a particular security safeguard. | * Have management, operational, and technical issues been considered? Do the elements of the evaluation procedure (questions, statements, and other components) address individual, measurable security safeguards? * Has the procedure been developed and tested in a few areas or systems? * Is the procedure supportive of objectives contained in HIPAA? Does the evaluation tool consider all standards and implementation specifications of the HIPAA Security Rule? |
| 3. | Conduct Evaluation | * Determine in advance what departments and/or staff will participate in the evaluation. * Secure management support for the evaluation process to ensure participation. * Collect and document all needed information. | * Have staff members with knowledge of IT security been consulted in the evaluation team? * Has specifically worded, written approval from senior management been received for any penetration testing? |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | * Collection methods may include the following: * Interviews * Surveys * Outputs of automated tool, such as access control auditing tools, system logs, and results of penetration testing. * Penetration testing is a security testing method where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls. | * Has the process been formally communicated to those who have been assigned roles and responsibilities in the evaluation process? Is an automated tool available to support the evaluation process? |
| 4. | Document Results | * Analyze the evaluation results. * Identify security weaknesses. Document, in writing, every finding and decision. * Develop security program priorities and establish targets for continuous improvement. | * Does the process support development of security recommendations? Has a report been written that highlights key findings and recommendations? * Have steps been taken to ensure that the final report is made available only to those persons designated to receive it? |
| 5. | Repeat Evaluation Periodically | * Establish the frequency of evaluations, taking into account the sensitivity the EPHI controlled by the organization, its size and complexity, and other relevant laws or accreditation requirements. * Repeat evaluations when significant changes to the security environment are made; e.g., if new technology is adopted or there are newly recognized risks to the security of the information. | * Do security policies specify that evaluations will be repeated when changes are made to security practices or the IT system? * Do policies on frequency of security evaluations reflect any and all relevant federal or state laws? |

### 2.9 Business Associate Contracts and Other Arrangements (164.308(b)(1))

HIPAA Standard: A covered entity, in accordance with § 164.306, 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(s) that the business associate appropriately safeguards the information.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Identify Entities that are Business  Associates and Under the HIPAA  Security Rule | * Identify the individual or department who will be responsible for coordinating the execution of business associate agreements. * Reevaluate the list of business associates to determine who has access whether the list is complete and current. * Identify systems covered by the contract/agreement. | * Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected? * Are there any new organizations or vendors that now provide a service or function on behalf of the organization? Such services may include the following: * Claims processing or billing * Data Analysis * Utilization Review * Quality Assurance * Benefit Management * Practice Management * Re-pricing * All other HIPAA-regulated functions. * Hardware Maintenance Have outsourced functions involving the use of protected information been considered such as the following: * Actuarial Services * Data Aggregation * Administrative Services * Accreditation * Financial Services? |
| 2. | Execute New Agreements or Update Existing Agreements as Appropriate | * Identify roles and responsibilities. Include security requirements in business associate contracts/ agreements to address confidentiality, integrity, and availability of sensitive information. * Specify any training requirements associated with the contract/ agreement. | * Who is responsible for coordinating and preparing the final agreement? Does the agreement specify how information is to be transmitted to and from the business associate? Does the agreement stipulate who is to have access to protected information and for what purpose? |
| 3. | Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements are Not Being Met | * Maintain clear lines of communication. * Conduct security reviews. * Establish criteria for measuring contract performance (metrics). | * What is the service being performed? * What is the outcome expected? Is there a process for reporting security incidents related to the agreement? * Is there a need to retain audit logs to support security reviews of the contract? * Is there a process in place for terminating the contract if requirements are not being met and has the business associate been advised of what conditions would warrant termination? |

## 3. Physical Safeguards

### 3.1 Facility Access Controls (164.310(a)(1))

HIPAA Standard: 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. (Note: Supports the Information Access Management Administrative Standard and Access Control Standard.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Conduct an Analysis of Existing  Physical Security Vulnerabilities | * Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. * Assign degrees of significance to each vulnerability identified. * Highest priority should be on the following primary types of facilities: * Data centers. * Peripheral equipment locations. * IT staff offices. * Workstation locations. | * Do non-public areas have locks and cameras? * Are workstations protected from public access or viewing? Are entrances and exits secured? Do policies and procedures already exist regarding access to and use of facilities and equipment? What is the threat environment? Are there possible natural or manmade disasters that could happen in our environment? * Do normal physical protections exist (locks on doors, windows, wet., and other means of preventing unauthorized access)? |
| 2. | Identify Corrective Measures | * Identify and assign responsibility for the measures and activities necessary to correct deficiencies. Develop and deploy policies and procedures to ensure that repairs, upgrade, and/or modifications are made to the appropriate physical areas of the facility. | * Who is responsible for security? * \Who is responsible for facility/ physical security? * Are policies and procedures already in place? Do they need to be revised? * What training will be needed for emp0loyees to understand the policies and procedures? * How will we document the decisions and actions? * Are we dependent on a landlord or particular group of department to make physical changes to meet the requirements? |

|  |  |  |  |
| --- | --- | --- | --- |
| 3. | Develop a Facility Security Plan | * Document appropriate measures to provide physical security protection for EPHI in a covered entity’s possession. * Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. | * Is there an inventory of facilities and existing security practices? What are the current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.)? * Who is responsible for the facility plan? * Is there a contingency plan already in place, under revision, or under development? |
| 4. | Develop Access Control Procedures | * Develop policies and procedures to provide facility access to authorized personnel and visitors. | * What policies and procedures are in place for controlling access by staff, contractors, visitors, and probationary employees? * How many access points exist in each facility? Is there an inventory? * Is monitoring equipment necessary? |
| 5. | Establish Contingency Operations  Procedures | * Develop policies and procedures to provide appropriate facility access to emergency response personnel. | * Who need access to the facility in the event of disaster? * What is the backup plan for facility access? * Who is responsible for implementing the contingency plan in each department, unit, etc.? * What is the backup plan for emergency access to EPHI? * Have all types of potential disasters been considered (fire, flood, earthquake, etc.)? * Have clear lines of authority been established for crisis management type decisions? |

### 3.2 Workstation Use (164.310(b))

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Identify Workstation Types and  Functions or Uses | * Inventory work[[3]](#footnote-3)stations and devices. Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues. * Classify workstations based on the capabilities, connections, and allowable activities for each workstation used. | * Do we have an inventory of workstation types and locations in the department or organization? Who is responsible for this inventory and its maintenance? What tasks are commonly performed on a given workstation or type of workstation? * Are there wireless tools in use as “workstations?” If so, what types and for what purpose? (Examples include Personal Digital Assistance (PDAs), laptops with wireless Internet connections, etc.) |
| 2. | Identify Expected Performance of  Each Type of Workstation | * Develop and document policies and procedures related to the proper use and performance of workstations. | * How are workstations used in dayto-day operations? * What are key operational risks that could result in a breach of security? |

### 3.3 Workstation Security (164.310(c))

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Identify All Methods of Physical  Access to Workstations | * Document the different ways workstations are accessed by employees and non-employees. | * Is there an inventory of all current workstations? * Are any workstations located in public areas? * Are laptops used as workstations? Are Personal Digital Assistants (PDAs) used as workstations? |
| 2. | Analyze the Risk Associated with  Each Type of Access | * Determine which type of access holds the greatest threat to security. | * Are any workstations in areas that are more vulnerable to unauthorized viewing of the data they contain? What are the options for making modifications to the current access configuration? |
| 3. | Identify Physical Safeguards | * Document the options for deploying physical safeguards that will minimize the risk of security of electronic health information. | * What safeguards are in place (i.e., locked doors, screen barriers, cameras, guards)? * Do any workstations need to be relocated to enhance physical security? * Have employees been trained on security? * Do mobile workstations have the ability to encrypt data storage and transmission? |

### 3.4 Device and Media Controls (164.310(d)(1))

HIPAA Standard: 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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Evaluate Methods of Final Disposal of Electronic Health Information  (EPHI) | * Determine and document the appropriate methods to dispose of hardware, software, and the data itself. Assure that EPHI is properly destroyed and cannot be recreated. | * What data is maintained by the organization, and where? * Is data on removable, reusable media such as tapes and CDs? Is there a process for destroying data on hard drives and file servers? What are the options for disposing of data on hardware? What are the costs? |
| 2. | Develop and Implement Procedures for Reuse of Electronic Media | * Ensure that health information previously stored on electronic media cannot be accessed and reused. Identify removable devices and their use. * Ensure that EPHI is removed from reusable media before it is used to record new information. | * Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? Is one individual and/or department responsible for coordinating the disposal of data, and the reuse of the hardware and software? * Are employees appropriately trained on security and risks to EPHI when reusing software and hardware? |
| 3. | Maintain Records of Hardware,  Media, and Personnel | * Ensure that EPHI is not inadvertently released or shared with any unauthorized party. * Ensure that an individual is responsible for, and record the receipt and removal of hardware and software with EPHI. | * Where is the data stored (what type of media)? * What procedures already exist regarding tracking of hardware and software within the organization? What procedures exist to track hardware and software internally? Who is responsible for maintaining records of hardware and software? |
| 4. | Develop Backup Procedures to Ensure That the Integrity of Electronic Health Information Will Not Be Jeopardized During Equipment Relocation | * Ensure that an exact, retrievable copy of the data is retained and protected. | * Are backup files maintained offsite? Do backup procedures exist? Who has this responsibility? * Are backup procedures documented and available to other staff? * If data were to be unavailable for a period of time, what would the business impact be? * Is there a contingency plan in place? |

## 4. Technical Safeguards

### 4.1 Access Control (164.312(a)(1))

HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). (Note: Supports the Information Access Management Administrative Standard and Facility Access Controls Physical Standard.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Analyze Workloads and Operations to Identify the Access Needs of All Users | * Identify an approach for access control. * Consider all applications and systems containing electronic health information that should only be available to approved users. | * What are the applications/systems that require access controls? What user roles are defined for those applications/systems? Where is the health information supporting those applications/ systems currently housed (i.e., stand -alone PC, network)? * Are data and/or systems being accessed remotely? |
| 2. | Identify All Data and Systems Where Access Control is a Requirement. | * Determine the scope and degree of access control needed. | * How are systems accessed (viewing data, modifying data, creating data)? * Are passwords being used? * If so, are they unique by individual? |
| 3. | Ensure That All System Users Have Been Assigned a Unique Identifier. | * Ensure that system activity can be traced to a specific user. * Ensure that the necessary data is available in the system logs to support audit and other related business functions. | * How should the identifier be established (length and content)? Should the identifier be selfselected or randomly generated? How often should the identifier be changed? |
| 4. | Develop Access Control Policy. | * Establish a formal policy for access control that will guide the development of procedures. | * Have rules of behavior been established and communicated by system users? * How will rules of behavior be enforced? * Has a determination been made on use of encryption? |
| 5. | Implement Access Control Procedures Using Selected Hardware and Software. | * Implement the policy and procedures using a cost-effective hardware/software solution. | * Who will manage the access controls procedures? * Are current users trained in access control management? * Will user training be needed to implement access control procedures? |
|  | 6. Review and Update User Access. | * Enforce policy and procedures as a matter of ongoing operations. Determine if any changes are needed for access control mechanisms. * Establish procedures for updating access when users require the following: * Initial access. * Increased access. * Access to different systems or applications than those they currently have. | * Have new employees/users been given proper instructions for protecting data and systems? * What are the procedures for new employee/user access to data and systems? * Are there procedures for reviewing and, if appropriate, modifying access authorization for existing users? |
|  | 7. Establish an Emergency Access Procedure. | * Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems. | * When should the emergency access procedure be activated? * Who is authorized to make the decision? * Who has assigned roles in the process? * Is the emergency access procedure to be a default emergency procedure, which has been established and communicated to all users, or is it a process restricted to, and conducted by a few authorized individuals? * Can it be activated on a user-byuser basis? |
|  | 8. Terminate Access if it is No Longer Required. | * Ensure only those with a need to know have access to protect data and systems. | * Are rules being enforced to remove access by staff members who no longer have a need to know because they have changed assignments or have stopped working for the organization? |
|  | 9. NOTE: | * The descriptions and questions/tasks that appear in this standard assume that the appropriate policies have been written and that the Security * Official, the Security Management * Plan and infrastructure are in place. |  |

### 4.2 Audit Control (164.312(b))

HIPAA Standard: Implement hardware, software, and/or procedure mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Determine the Systems or Activities that Will be Tracked or Audited. | * Determine the appropriate scope of any system audits that will be necessary based on the size and needs of the covered entity. * Use results or risk assessment to determine which systems and activities should be tracked and audited. Determine what data needs to be captured. | * Where is EPHI at risk in the organization? * What systems, applications, or processes make data vulnerable to unauthorized or inappropriate tampering, users, or disclosures? * What activities will be monitored * (Create, Read, Update, Delete = * CRUD)? * What should the audit record include (i.e., user ID, event type/date/ time)? |
| 2. | Select the Tools that Will be Deployed for Auditing and System Activity Reviews. | * Evaluate existing system capabilities and determine if any changes or upgrades are necessary. | * What tools are in place? What are the most appropriate monitoring tools for the organization (third party, freeware, or operating system provided)? * Are changes/upgrades cost effective? |
| 3. | Develop and Deploy the Information System Activity Reviews. | * Document and communicate to the workforce the facts about the organization’s decisions on audits and reviews. | * Who is responsible for the overall audit process and results? * How often will audits take place? How often will audit results be analyzed? * What is the organization’s sanction policy for employee violations? Where will audit information reside (i.e., separate server)? |
| 4. | Develop Appropriate Standard Operating Procedures. | * Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports. | * How will exception reports or logs be reviewed? * Where will monitoring reports be filed and maintained? * Is there a formal process in place to address system misuse, abuse, and fraudulent activity? * How will managers and employees be notified, when appropriate, regarding suspect activity? |
| 5. | Implement the Audit/System Activity Review Process. | * Activate the necessary audit system. Begin logging and auditing procedures. | * What mechanisms will be implemented to assess the effectiveness of the audit process (metrics)? What is the plan to revise the audit process when needed? |
| 6. | NOTE: | * The descriptions and questions/tasks that appear in this module assume that the appropriate policies have been written and that the Security * Official, the Security Management Plan and infrastructure are in place. |  |

### 4.3 Integrity (164.312(c)(1))

HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Identify All Users Who are Authorized to Access Electronic Protected Health Information. | * Identify all approved users with the ability to alter or destroy data. | * How are users authorized to access the information? * Is there a sound basis established as to why they need the access? Have they been trained on how to use the information? * Is there an audit trail established for access to the information? |
| 2. | Indentify Any Possible Unauthorized Sources That May be Able to Intercept the Information and Modify It. | * Identify scenarios that may result in modification to the electronic health information by unauthorized sources (i.e., hackers, disgruntled employees, business competitors). Consider conducting this activity as part of your Risk Analysis. | * What are likely sources that could jeopardize information integrity? What can be done to protect the integrity of the information when it is residing on a system (at rest)? What procedures and policies can be established to decrease or eliminate alteration of the information during transmission (i.e., encryption)? * How feasible and cost-effective to the environment are the options being considered? |
| 3. | Develop the Integrity Policy and Requirements. | * Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps. | * Have the requirements been discussed and agreed to by identified key personnel involved in the processes that are affected? * Have the requirements been documented? * Has a written policy been developed and communicated to system users? |
| 4. | Implement Procedures to Address These Requirements. | * Identify which methods will be used to protect the information from modification. * Identify tools and techniques to be developed or procured that support the assurance of integrity. | * Are current audit, logging, and access control techniques sufficient to address the integrity of the information? * If not, what additional techniques can we apply to check information integrity (i.e., quality control processes, transactions and output reconstruction)? * Can additional training of users decrease instances attributable to human errors? |

|  |  |  |  |
| --- | --- | --- | --- |
| 5. | Establish a Monitoring Process to Access How the Implemented Process is Working. | * Review existing processes to determine if objectives are being addressed. * Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised. | * Are there reported instances of information integrity problems and have they decreased since integrity procedures have been implemented? Does the process, as implemented, provide a higher level of assurance that information integrity is effective? |

### 4.4 Person or Entity Authentication (164.312(d))

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **Description** | **Questions** |
| 1. | Determine Authentication Applicability to Current Systems/ Applications. | * Identify methods available for authentication. Authentication is the process of establishing the validity of a transmission’s source or verifying an individual’s authorization claim for specific access privileges to information and information systems. | * What authentication methods are available? * What are the advantages and disadvantages of each method? * What will it cost to implement the available methods in our environment? * Do we have trained staff who can maintain the system or do we need to consider outsourcing some of the support? |
| 2. | Evaluate Authentication Options Available. | * Weigh the relative advantages and disadvantages commonly used in authentication approaches. There are four commonly used approaches available:  1. Something a person knows, such as a password. 2. Something a person has or is in possession of, such as a token (smart card, ATM card, etc.). 3. Some type of biometric identification a person provides, such as a fingerprint. 4. A combination of two or more of the above approaches. | * What are the strengths and weaknesses of each available option? Which can be best supported with assigned resources (budget/ staffing)? * What level of authentication is appropriate based on our assessment of risk to the information/systems? Do we need to acquire outside vendor support to implement the process? |
| 3. | Select and Implement Authentication Option. | * Consider the results of the analysis conducted under Step 2 above, and select appropriate authentication methods. * Implement the methods selected into your operations and activities. | * Has necessary user and support staff training been completed? * Have formal authentication policy and procedures been established and communication? * Has necessary testing been completed to ensure that the authentication system is working as prescribed? * Do the procedures include ongoing maintenance and updates? * Is the process implemented in such a way that it does not compromise the authentication information * (password file encryption, etc.)? |

### 4.5 Transmission Security (164.312(e)(1)

HIPAA Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Key Activities** | **1Description** | **2Questions** |
| 1. | Identify Any Possible Unauthorized Sources that May be Able to Intercept and/or Modify the Information. | * Identify scenarios that may result in modification to the electronic protected health information (EPHI) by unauthorized sources during transmission (i.e., hackers, disgruntled employees, business competitors). | * What measures exist to protect EPHI? * What measures are planned to protect EPHI> * Is there an auditing process in place? * Is there assurance that information is not altered during transmission? Are there trained staff members to monitor transmissions? |
| 2. | Develop a Transmission Security Policy. | * Establish a formal (written) set of requirements for transmitting electronic protected health information. | * Have the requirements been discussed and agreed to by identified key personnel involved in transmitting electronic health information? * Has a written policy been developed and communicated to system users? |
| 3. | Implement Procedures for Transmitting Electronic Health Information Using Hardware/Software if Needed. | * Identify methods of transmission that will be used to protect electronic health information. * Identify tools and techniques that will be used to support the transmission security policy. | * Is encryption needed to effectively protect the information? * Is encryption feasible and cost effective in this environment? * Are staff members skilled in the use of encryption? |

#### 1. DEFINITIONS

**Authorized use:**

Use of computing and networking resources shall be limited to those resources and purposes for which access is granted. Use for political purposes is prohibited (see Section 39-01-04 of the ND Century Code). Use for private gain or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under governing institution or system procedures, or, when not expressly authorized, such use is incidental to job duties or limited in time and scope, and such use does not: (1) interfere with AIG Business Solution (P) Ltd. operation of information technologies or electronic mail services; (2) burden the AIG Business Solution (P) Ltd. with incremental costs; or (3) interfere with the user's obligations to the institution or AIG Business Solution (P) Ltd.

**Authorized user(s):**

Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the AIG Business Solution (P) Ltd. These resources are extended to accomplish tasks related to the individual's status with AIG Business Solution (P) Ltd. or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the AIG Business Solution (P) Ltd. For the purposes of this policy, no attempt is made to differentiate among users by the user's group. These policies treat all users similarly, whether student, faculty, staff or other authorized user, in terms of expectations of the user's conduct.

**Campus IT Department:**

Official central information technology department as designated by the institution's president or chief executive officer.

**Campus Information Technology Security Officer:**

Individual, designated by the Institution, responsible for IT security policy education and enforcement, and coordination of incident investigation and reporting.

**Campus Judicial Officers:**

The designated Campus Judicial Officers for students, or appropriate supervising authority for faculty and staff, as defined by the Institution.

**AIG Business Solution (P) Ltd. Chief Information Officer Council representative (CIO):** The senior staff member responsible for information technology.

**Computing and networking resources:**

Computing resources and network systems including, but not limited to, computer time, data processing, and storage functions; computers, computer systems, servers, networks, and their input/output and connecting devices; and any related programs, software and documentation. Further, it is understood that any device that connects to a campus network, whether wired or wireless, is expected to comply with all AIG Business Solution (P) Ltd. and institutional policies and procedures.

**Electronic information:**

Any electronic text, graphic, audio, video, digital record, digital signature or message stored on or transported via electronic media. This includes electronic mail messages and web pages.

**HECN:**

The North Dakota Higher Education Computer Network, which has been given the responsibility of maintaining the computer and network systems for the North Dakota University System.

**Institution:**

One of the eleven colleges or universities within the North Dakota University System.

**Open record:**

Electronic information used in support of college, university or AIG Business Solution (P) Ltd. business, regardless of where the electronic information originated or resides may be subject to open records laws of North Dakota (see Section 44-04-18 of the ND Century Code).

**Scrubbed:**

The act of ensuring that no data is retrievable from a storage device according to current "best practice."

**Sensitive data:**

Any data, the unauthorized disclosure of which may place the Institution or AIG Business Solution (P) Ltd. at risk.

**Server:**

Any device that provides computing service to multiple computers or individuals.

**Student record:**

As defined by the Family Educational Rights and Privacy Act of 1974 (FERPA), a student educational record includes records containing information directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

**Unit:**

Department, office or other entity within an institution.

**Update:**

A new release (or version) or a piece of software that is generally understood to be an error correction release and does not contain new functionality.

**Upgrade:**

A new release (or version) of a piece of software that contains new functionality.

**User:**

See Authorized User(s)

#### 2. INDIVIDUAL PRIVILEGES

The following individual privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.

##### 2.1 Privacy

In general, all electronic information shall be free from access by any but the authorized users of that information. Exceptions to this basic principle shall be kept to a minimum and made only when essential to:

1. meet the requirements of the state open records law and other statutory or regulatory requirements;
2. protect the integrity of the College or University and the rights and property of the State;

1.

1. allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like (see 4.3, 4.4).

##### 2.2. Encryption and password protection

When using encryption utilities or password protection schemes on institutional information or computing equipment, a unit-level recovery process must be used. No data protection schemes may be used to deprive a unit or institution from access to data or computing equipment to which they are entitled.

##### 2.3. Freedom from harassment and undesired information

All members of the campus community have the right not to be harassed by computer or network usage of others (see 3.1.3.).

**2.4. Appeals of sanctions**

Individuals may appeal any sanctions according to the process defined for their Institution.

#### 3. INDIVIDUAL RESPONSIBILITIES

Each member of the campus community enjoys certain privileges and is responsible for the member's actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community.

##### 3.1. Respect for rights of others and legal and policy restrictions

Users are responsible to all other members of the campus community in many ways. These include the responsibility to:

* respect and value the right of privacy;
* recognize and respect the diversity of the population and opinion in the community, and;
* comply with AIG Business Solution (P) Ltd. and Institution policy and all laws and contracts regarding the use of information that is the property of others.

###### 3.1.1 Privacy of information

All electronic information which resides on AIG Business Solution (P) Ltd. and institution computers, and any data on any device that connects, wired or wireless, to the campus network may be determined to be subject to the open records laws of North Dakota.

Individuals are prohibited from looking at, copying, altering, or destroying another individual's electronic information without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so unless the information has been placed in a public area such as a web site.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. The [AIG Business Solution (P) Ltd. Data Classification and Information Technology Security Standard](http://www.ndus.nodak.edu/uploads/document-library/1620/P-1901.2-DATA.STD.12-14-2007.PDF) further defines and explains AIG Business Solution (P) Ltd. and institution data classifications, standards, and security responsibilities.

Except to the extent that a user lacks control over messages sent to the user, electronic information is deemed to be in the possession of a user when that user has effective control over the location of its storage.

###### 3.1.2 Intellectual property

Users are responsible for recognizing and honoring the intellectual property rights of others. Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted material and computer programs in violation of copyright laws. Software subject to licensing must be properly licensed and all users must strictly adhere to all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.).

When reproducing, or distributing information, users are responsible for the observation of copyright rights and other intellectual property rights of others and all state and federal laws, Institutional and AIG Business Solution (P) Ltd. policies. Generally materials owned by others cannot be used without the owner's permission. Written consent from the copyright owner is normally necessary to reproduce or distribute copyrighted material. There are some exceptions such as fair use in teaching and in research.

Documentation of consent to use copyrighted materials must be kept on record and made available to institution officials upon request. The AIG Business Solution (P) Ltd. assumes no obligation to monitor users for infringing activities, but will, when such activities are called to the appropriate official's attention, investigate to determine if there is likely infringement and make appropriate responses.

Users should also be careful of the unauthorized use of trademarks. Certain uses of such marks online on websites or in domain names can constitute trademark infringement. Unauthorized use of an institution's name in these situations can also constitute trademark infringement.

###### 3.1.3 Harassment

Users may not use AIG Business Solution (P) Ltd. or AIG Business Solution (P) Ltd. Insti ntution computers or networks to harass any other person.

Prohibited activities include, but are not limited to: (1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right or institutional sanction to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

##### 3.2. Responsible use of resources

Users are responsible for knowing to which resources they have been granted access, and refraining from all acts that waste or prevent others from using these resources, or from using them in ways proscribed by the AIG Business Solution (P) Ltd. or AIG Business Solution (P) Ltd. institutions or state or federal laws.

##### 3.3. Information integrity

Electronic information is easily manipulated. It is the user's responsibility to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct if the information or communication is contrary to expectations. It is important to verify that information with the source.

##### 3.4. Use of personally managed systems

Any device connecting directly to a AIG Business Solution (P) Ltd. or institution network, whether via wire or wireless or modem device must be administered and maintained in a manner consistent with the policies of the AIG Business Solution (P) Ltd. and institution and all applicable laws, including access and security issues. Anti-virus software should be installed and any software installed (especially operating system and anti-virus software) should be kept up-to-date with regard to security patches.

Personal firewalls should be deployed when their installation will not interfere with the function of the device or the administration of the network; and such firewalls should be configured to allow minimal traffic.

At a minimum, password facilities should be utilized to ensure that only authorized individuals can access the system.

Passwords should be a minimum of eight characters and a combination of upper and lower case letters, numbers and special characters, as the system allows. They should not be words found in a dictionary. Nor should they be something that is easily discerned from knowledge of the owner. Passwords should not be written anywhere and not sent via email or shared with others. System administrators will ensure that passwords are not readable in plain text on the systems.

The administrative account/login and password should be changed to values specified by the campus IT department; and any system default "guest" account/login should be assigned a password and disabled.

All unnecessary software and services should be disabled.

Any device configured as a server must be registered with the campus IT department.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. The [AIG Business Solution (P) Ltd. Server Information Technology Security Standard](http://www.ndus.nodak.edu/uploads/document-library/839/1901.2-SERVER.PDF) further defines AIG Business Solution (P) Ltd. and institution server standards and security responsibilities.

It is the responsibility of the owner/administrator of a personally managed system to maintain logs appropriate to the type of server and to make those logs available to AIG Business Solution (P) Ltd. or institution personnel as needed.

The HECN manages the name space and IP subnets for the AIG Business Solution (P) Ltd. Policies pertaining to these services can be found at [http:// www.AIG Business Solution (P) Ltd.nodak.edu/uploads/document-library/835/1901.2-DNS.PDF](http://www.ndus.nodak.edu/uploads/document-library/835/1901.2-DNS.PDF)

###### 3.4.1 Video transmission devices

All audio and/or video transmission devices (web cams, etc.) must be utilized in a manner consistent with these policies and all applicable laws.

##### 3.5. Access to computing and networking resources

The AIG Business Solution (P) Ltd. makes every effort to provide secure, reliable computing and networking resources. However, such measures are not foolproof and the security of a user's electronic information is the responsibility of the user.

Administrative desktop computers should be behind locked doors when the office is unoccupied and access to these devices should be based on minimal need.

Under no circumstances may an external network be interconnected to act as a gateway to the campus network without coordination and explicit approval from the campus IT department.

###### 3.5.1 Sharing of access

Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

Institution Departments or Administrative Offices; or Institution-wide Help Desk or information functions; or officially recognized Faculty, Staff or Student Organizations may be granted permission for multi-user accounts with common authentication, for approved purposes. Requests for these types of accounts must come from the individual assuming responsibility for the activity of the account and be approved by the AIG Business Solution (P) Ltd. Chief Information Officer Council representative. Only the person responsible for the activity of the account is authorized to share access and authentication information and only persons individually entitled to access AIG Business Solution (P) Ltd. systems may be given access to these accounts.

###### 3.5.2 Permitting unauthorized access

Authorized users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users (see section 1).

###### 3.5.3 Use of privileged access

Access to information should be provided within the context of an authorized user's official capacity with the AIG Business Solution (P) Ltd. or AIG Business Solution (P) Ltd. institutions. Authorized users have a responsibility to ensure the appropriate level of protection over that information.

###### 3.5.4 Termination of access

When an authorized user changes status (e.g., terminates employment, graduates, retires, changes positions or responsibilities within the Institution, etc.), the user must coordinate with the unit responsible for initiating that change in status to ensure that access authorization to all institution resources is appropriate. A user may not use computing and networking resources, accounts, access codes, privileges, or information for which the user is not authorized.

###### 3.5.5. Backups

While the AIG Business Solution (P) Ltd. will make every effort to provide reliable computing facilities, ultimately it is the individual user's responsibility to maintain backups of their own critical data. Such backups should be stored in a secure off-site location.

###### 3.5.6 Device registration

Any desktop computer and any network addressable device that connects to a campus network should be approved by and registered with the campus IT department.

##### 3.6. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. Any security incidents should be reported to the system administrators and the Campus IT Security Officer.

###### 3.6.1 Decoding access control information

Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

###### 3.6.2. Denial of service

Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any computer system or network are prohibited.

###### 3.6.3 Harmful activities

Harmful activities are prohibited. Examples include, but are not limited to, IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

**3.6.4. Unauthorized activities** Authorized users may not:

* damage computer systems;
* obtain extra resources not authorized to them;
* deprive another user of authorized resources, or
* gain unauthorized access to systems by using knowledge of:

a special password; loopholes in computer security systems; another user's password, or access abilities used during a previous position.

###### 3.6.5. Unauthorized monitoring

Authorized users may not use computing resources for unauthorized monitoring or scanning of electronic communications without prior approval of the campus CIO or the campus or AIG Business Solution (P) Ltd. IT Security Officer.

##### 3.7. Academic dishonesty

Use of AIG Business Solution (P) Ltd. computing facilities to commit acts of academic dishonesty will be handled through existing campus procedures which address allegations of academic dishonesty.

##### 3.8. Personal business

Computing and networking resources may not be used in connection with compensated outside work or for private business purposes unrelated to the AIG Business Solution (P) Ltd. or institutions, except in accordance with the AIG Business Solution (P) Ltd. Consulting Policy.

#### 4. AIG Business Solution (P) Ltd. AND AIG Business Solution (P) Ltd. INSTITUTION PRIVILEGES

##### 4.1. Control of access to information

AIG Business Solution (P) Ltd. and AIG Business Solution (P) Ltd. institutions may control access to their information and the devices on which it is stored, manipulated, and transmitted, in accordance with the policies of the Institution and AIG Business Solution (P) Ltd. and federal and state laws. Access to information and devices is granted to authorized AIG Business Solution (P) Ltd. personnel as necessary for the performance of their duties and such access should be based on minimal need to perform those duties.

**4.2. Imposition of sanctions**

The Institution may impose sanctions on anyone who violates the Computer and Network Usage Policy.

##### 4.3. System administration access

A system administrator (i.e., the person responsible for the technical operation of a particular machine) may access electronic information as required for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all rights to privacy of information are to be preserved to the greatest extent possible.

##### 4.4. Monitoring of usage, inspection of electronic information

The Electronic Communications Privacy Act allows system administrators or other authorized campus and AIG Business Solution (P) Ltd. employees to access a person's electronic information in the normal course of employment, when necessary, to protect the integrity of computing and networking resources or the rights or property of the Institution or AIG Business Solution (P) Ltd. Additionally, other laws, including the U.S.A. P.A.T.R.I.O.T. ACT of 2001, may expand the rights and responsibilities of campus administrators. Electronic information may be subject to search by law enforcement agencies under court order.

The AIG Business Solution (P) Ltd. and Institution may also specifically monitor the activity, systems and accounts of individual users of the Institutions' computing and networking resources without notice. This includes individual login sessions, electronic information and communications. This monitoring may occur in the following instances:

1. The user has voluntarily made them accessible to the public.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institution or to protect the Institution or AIG Business Solution (P) Ltd. from liability.
3. There is reasonable cause to believe that the user has violated, or is violating, Institution or AIG Business Solution (P) Ltd. policies or any applicable laws.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
5. Upon receipt of a legally served directive of appropriate law enforcement agencies.
6. Upon receipt of a specific complaint of suspected or alleged violation of policy or law regarding a specific system or activity.

Any such monitoring must be accomplished in such manner that all privileges and right to privacy are preserved to the greatest extent possible and with the prior permission of the Campus ITSO or CIO, if reasonable.

For further information, please see 2.1 for information on privacy.

##### 4.5 Suspension of individual privileges

AIG Business Solution (P) Ltd. and Institutions operating computers and networks may suspend computer and network privileges of a user:

* to protect the integrity, security or functionality of the Institution or AIG Business Solution (P) Ltd. and/or their resources or to protect the Institution or

AIG Business Solution (P) Ltd. from liability;

* to protect the safety or well-being of members of the community, or

* upon receipt of a legally served directive of appropriate law enforcement agencies or others.

Access will be promptly restored when the protections are assured, unless access is suspended as a result of formal disciplinary action imposed by Campus Judicial Officers, HECN or other legal officers.

##### 4.6 Retention of access

User accounts are assigned to a specific individual at a specific institution within the AIG Business Solution (P) Ltd. When a specific affiliation is terminated, the AIG Business Solution (P) Ltd. or Institution may elect to terminate the user's account, transfer the account, continue the account for a limited period of time, or, in the case of e-mail, temporarily redirect incoming communications.

##### 4.7 Network maintenance

The HECN and the campus networking personnel have the responsibility of maintaining the networks for the benefit of all authorized users. This implies that, in emergency situations, they may, if there is no other way to resolve a problem, request that a device (whether wired or wireless) be disconnected from the network or powered down, or, if necessary, take such action themselves.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. AIG Business Solution (P) Ltd. network standards are further defined in the [AIG Business Solution (P) Ltd. Network Information Technology Security Standard.](http://www.ndus.nodak.edu/uploads/document-library/836/1901.2-NETWORK.PDF)

#### 5. AIG Business Solution (P) Ltd.

The Institution shall ensure that physical or network access to all critical infrastructures shall be monitored; and such access granted and maintained based solely on need.

Individual campuses are expected to develop policies and procedures to address those environments unique to their campus. Such policies or procedures may not be contrary to the express terms or the intent of AIG Business Solution (P) Ltd. policies and procedures.

##### 5.1. Risk management

Periodic risk assessment of information systems infrastructure and data shall be completed by AIG Business Solution (P) Ltd. and Institutions. Any discovered vulnerabilities should be presented to the appropriate campus and AIG Business Solution (P) Ltd. officials.

The networking services and computer operations personnel are responsible for providing adequate disaster recovery plans and procedures for critical systems under their responsibility in the event of a natural or manmade disaster.

###### 5.1.1. Physical concerns

Desktop computers and computer peripherals should be protected from theft and vandalism and any institutionally owned devices should be readily identifiable as institutionally owned. Public access computers should be in a monitored area.

Installations with computer and networking resources will implement reasonable security measures to protect the resources against natural disasters, environmental threats, accidents and deliberate attempts to damage the systems.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. See [AIG Business Solution (P) Ltd. Physical Information Technology Security Standards](http://www.ndus.nodak.edu/uploads/document-library/838/1901.2-PHYSICAL.PDF) for additional information.

###### 5.1.2. Configuration concerns

The Institution's campus IT department shall, for those desktops they manage, change the Administrative login and password, make inaccessible any system defined accounts and turn off any unnecessary software or services. Any access to a server, other than a public server, should be authenticated and logged. Access to all servers should be based on minimal need.

Software with security vulnerabilities will be patched in a timely manner.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. Refer to the AIG Business Solution (P) Ltd. Server Information Technology Security Standard for more information.

##### 5.2. Security procedures

The AIG Business Solution (P) Ltd. and Institutions have the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional computing and networking resources, and to impose appropriate sanctions when security or privacy is abridged.

Each Institution shall designate an Information Technology Security Officer to coordinate the security efforts on their campus. This individual shall be considered an "other school official" determined to have legitimate educational interests for purposes of sharing information under federal law. This person shall coordinate efforts and share information, with other campus officials, as necessary. The Information Technology Security Officer will keep appropriate records of any incidents/investigations on the Officer's campus and, if requested, share those records with the appropriate AIG Business Solution (P) Ltd. personnel.

The AIG Business Solution (P) Ltd. shall designate an Information Technology Security Officer, who will assist the campus Information Technology Security Officers in their duties and who shall be considered an "other school official" determined to have legitimate educational interests for each campus under federal law.

##### 5.3. Public information services

Institutions may configure computing systems to provide information services to the public at large. (Current examples include, but are not limited to "ftp" and "www") However, in so doing, any such systems must comply with all AIG Business Solution (P) Ltd. and institution policies and applicable laws. Particular attention must be paid to the following sections of this policy: 1(Authorized use), 3.1.2 (Intellectual Property) and 3.2 (Responsible use of resources). Use of public services must not cause computer or network loading that impairs other services or impedes access.

##### 5.4 Communications and record keeping

It is the responsibility of each institution that provides computing facilities to: inform users of all applicable AIG Business Solution (P) Ltd. computing policies and procedures; to address, through existing campus judicial procedures any resulting complaints to maintain appropriate records and to inform the AIG Business Solution (P) Ltd. CIO designate of the progress and resolution of any incident responses; and provide an environment consistent with these policies and procedures.

##### 5.5 Backup and retention of data

Normal backup procedures are employed for disaster recovery on AIG Business Solution (P) Ltd. and institution systems. Therefore, if a user removes electronic information, it may still be retrievable by the system administrators. These backups may or may not be retained for an extended period of time. Backed-up electronic information may be available for the investigation of an incident by system administrators or law enforcement personnel. Administrators of the systems may be required to attempt to recover files in legal proceedings.

For data critical to the function of the Institution, a second set of backups should be maintained off-site in a secured protected area.

##### 5.6 Schedule of service

Most scheduled maintenance of AIG Business Solution (P) Ltd. computing and networking resources will be done at pre-announced times. There are times when some computing and networking resources will be unavailable due to unforeseeable circumstances. Problems may arise with electronic information transmission and storage. Such occurrences may cause a disruption to service or loss of data. The AIG Business Solution (P) Ltd. assumes no liability for loss of service or data. However, all efforts must be made to ensure the availability of services at other than scheduled maintenance times.

##### 5.7 Privacy of records

Campus access to student computer records will be governed by existing campus records policies. Generally, student records, including computer records, fall under the Family Educational Rights and Privacy Act of 1974 (FERPA). The computer records of a student are educational records and cannot be released without written consent from the student except as elsewhere defined by institutional policy or state or federal law. The institution's response to subpoenas for student records will be carried out as defined by the institution and state or federal law.

The AIG Business Solution (P) Ltd. CIO is authorized to develop and publish standards for the AIG Business Solution (P) Ltd. institutions. Standards for institutional data and its classifications can be found in the [AIG Business Solution (P) Ltd. Data Classification and Information Technology Security Standard.](http://www.ndus.nodak.edu/uploads/document-library/1620/P-1901.2-DATA.STD.12-14-2007.PDF)

##### 5.8 Domain name services

The HECN administers the nodak.edu domain and IP subnets for AIG Business Solution (P) Ltd. Procedures for adding hosts and related policies can be found in the ["Policy for Name Service and Usage"](http://www.ndus.nodak.edu/uploads/document-library/835/1901.2-DNS.PDF)

**5.9 Virus protection software**

The HECN shall make available virus-protection software for AIG Business Solution (P) Ltd. users and keep available the most current updates.

**5.10 Legal software**

The Institution shall periodically audit institutionally owned devices for proper software licenses.

##### 5.11 Data privacy

Any electronic data asset of the AIG Business Solution (P) Ltd. or the Institution shall be classified as Public, Private or Confidential according to the [AIG Business Solution (P) Ltd. Data Classification and Information Technology Security Standard.](http://www.ndus.nodak.edu/uploads/document-library/1620/P-1901.2-DATA.STD.12-14-2007.PDF)

The owner of data is that person, department or office that is responsible for the integrity of the data. It is the responsibility of the owner of the data to classify the data.

It is the responsibility of anyone using or viewing the data to protect the data at the level determined by the owner of the data or as mandated by law.

Appropriate efforts must be taken to ensure data integrity, confidentiality and availability.

#### 6. PROCEDURES AND SANCTIONS

The AIG Business Solution (P) Ltd. makes every reasonable effort to protect the rights of the individual users of its computing and networking resources while balancing those rights against the needs of the entire user community. The AIG Business Solution (P) Ltd. and Institution will make every effort to resolve any system or network problems in the least intrusive manner possible.

##### 6.1. Investigative contact

If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving AIG Business Solution (P) Ltd. or Institution computing and networking resources, they must inform the Institution's Information Technology Security Officer and the AIG Business Solution (P) Ltd. Information Technology Security Officer.

##### 6.2. Responding to security and abuse incidents

All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. In the AIG Business Solution (P) Ltd., the HECN has been delegated the authority to enforce information security policies and is charged with:

Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.

Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of AIG Business Solution (P) Ltd. or an Institution's resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of AIG Business Solution (P) Ltd. or Institution computing and networking resources. All users and units that have reported to them (other than as in 6.1 above) a security or abuse problem with any AIG Business Solution (P) Ltd. or Institution computing or networking resources, including violations of this policy are to:

Take immediate steps as necessary to ensure the safety and wellbeing of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 4.5, 4.6 and 4.7).

Make appropriate reports on any discovered unauthorized access attempts or other improper usage of institution or AIG Business Solution (P) Ltd. computing and networking resources.

Ensure that the following people are notified: (1) The administrator of the computer, if known. (2) If appropriate, the campus Information Technology Security Officer or the campus IT Department.

##### 6.3. First and minor incident

Minor infractions of these policies are generally resolved informally by the unit administering the accounts or network in conjunction with the Campus Information Technology Security Officer. Minor infractions are those in which the impact on the computer or network resource is minimal and limited to the local network. Resolution of the infraction will include referral to the Code of Student Life, staff or faculty handbooks, or other resources for self-education about appropriate use. In the case of students, a copy of the resolution will be sent to the Campus Judicial Officer.

##### 6.4. Subsequent and/or major violations

Repeated minor infractions or more serious misconduct may result in immediate loss of computer access privileges or the temporary or permanent modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computing facilities, attempts to steal passwords or data, unauthorized use, distribution or copying of licensed software, or other copyrighted materials, use of another's account, harassment or threatening behavior, or crashing the system. Policy violators will be referred by the campus Information Technology Security Officer to the Campus Judicial Officer for further action.

##### 6.5. Range of disciplinary sanctions

Users who violate this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the institution, and legal action. Use that is judged excessive, wasteful, or unauthorized may result in denial of access to computing and networking resources and may subject the user to appropriate disciplinary and/or legal procedures. Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges and will be referred to appropriate college or university offices and/or law enforcement authorities.

##### 6.6. Appeals

Notice of violations and appeals of decisions will follow campus procedures.

**REFERENCE:** SBHE Policy [1901.2](http://www.ndus.edu/policies/sbhe-policies/policy.asp?ref=2429)

**NOTE**: Because of the sensitive nature of Sections I—V of 1901.2, revised version, January 2005, the sections are considered *PRIVATE* and *CONFIDENTIAL*. These sections will not be part of the *PUBLIC* version of 1901.2.

# SECTION I

## AIG Business Solution (P) Ltd. Server IT Security Procedures

For purposes of these procedures, a server is defined as any device that provides computing service to multiple computers or individuals.

Systems administrators should configure their servers based on the assumption that the network they are connected to is insecure. All unused services should be disabled. Any access to a server other than a “public” server (i.e., public web server) should be authenticated and access permission based on minimal need. File access permissions should be set to restrict access to confidential or sensitive data to authorized personnel only.

Server administrators should regularly check for new services installed that allow access from the network.

Software with security vulnerabilities will be patched in a timely manner. In situations where an identified vulnerability cannot be quickly patched, action such as increased monitoring or further restricting access to the affected application will be taken. System administrators will monitor vulnerability notifications relevant to their platform(s) and application(s).

Servers that have been compromised should be disconnected, fixed and documented prior to reconnecting to the network.

Remote access to the server for server administrators should be restricted to only those clients who need it using a software firewall of VPN or similar method. User remote access will be authenticated and may be further restricted based on the function of the server.

If the server only needs access to the internal network, external access should be filtered (i.e., dedicated DHCP server, and internal Web server).

System administrators will respect the resumed confidentiality of all data, looking at it only when given permission or where required to maintain the proper functioning of the server. The use of scanners or monitors is prohibited without the explicit permission from the admin.

Any exchange of authentication information between the client and the server should be done over an encrypted connection. Any connection that has the potential to transmit confidential or sensitive data should be encrypted. Sensitive or confidential data should be encrypted to ensure data confidentiality and integrity when transmitted over a network.

Servers shall be configured to log any activity relevant to the purpose of the server, as well as any security-related events. Such logs shall be retained for a minimum of thirty (30) days. Access log backups will be kept for a minimum of forty-two (42) days. Servers’ clocks shall be synchronized with Universal time servers to ensure the usefulness of timestamps in log files.

Data shall be protected against disaster by making regular backups. A second set of backups for mission-critical data should be maintained off-site in a secured, protected area.

Data should be properly scrubbed from any server hardware (i.e., server tapes, external disk arrays) before the hardware is scrapped to prevent the unintentional release of data.

Security incidents will be reported to the appropriate officials. End-users will be notified in the event that a security incident results in the disclosure, or possible disclosure, or confidential data.

All servers will be “registered” with the IT department.

# SECTION II

## AIG Business Solution (P) Ltd. Data Classification

Any electronic data asset of the AIG Business Solution (P) Ltd. or Institution shall be classified as Public, Private or Confidential, according to the following guidelines.

**Public Data:** Public data is defined as data that any entity, either internal or external to the organization can access.

**Private Data:** Private data includes information that AIG Business Solution (P) Ltd. is under legal or contractual obligation to protect. Private information disclosed to authorized external users must be done so under a non-disclosure agreement.

**Confidential Data:** Confidential data is information that is not be to publicly disclosed. The disclosure, use, or destruction of Confidential Data can have adverse effects on the company, and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Confidential information must not be copies without authorization from the identified owner.

Examples of AIG Business Solution (P) Ltd. Data Classification Schema:

### PUBLIC

**Employee Information:**

|  |  |  |
| --- | --- | --- |
| * Name | * Gender | * Birth date |
| * Job titles | * Job description | * Education and training |
| * Previous work experience | * First and last employment | * Existence and status of complaints |
| * Terms of buy-out agreements | * Final disposition of disciplinary action | * Work location |
| * Work phone number | * Honors and awards received | * Gender |
| * Home address (\*) | * Home telephone number (\*) |  |

(\*) Unless employee has requested non-disclosure (suppress).

The above information is public, unless the employee has requested non-disclosure (suppress).

**Other**:

|  |
| --- |
| * Budgets |
| * Financial data on public sponsored projects |
| * Invoices and purchase orders |

### PRIVATE

**Employee Information:**

|  |  |  |
| --- | --- | --- |
| * Employee ID number | * Expense reimbursements | * Location of assets |
| * Donors | * Payroll time sheets | * Ethnicity |
| * Citizenship | * Citizen visa code | * Veteran and disability status |
| * Salary | * Expense reimbursements | * Terms of buy-out agreements |
| * Payroll time sheets |

### CONFIDENTIAL

|  |  |
| --- | --- |
| * Legal investigations conducted by the company | * Sealed bids |
| * Trade secrets or intellectual property such as research activities | * Social Security Number |
| * Gross pension | * Value and nature of fringe benefits |
| * Health records | * Passwords |
| * Server access details |  |

The owner of a data item is that person, department, or office that is responsible for the integrity of the data. It shall be the responsibility of the owner of the data to classify the data. However, all individuals accessing data are responsible for the protection of the data at the level determined by the owner of the data or as mandated by law. Any data not yet classified by the owner shall be deemed Confidential. Access to data items may be further restricted by law, beyond the classification systems of the organization.

All data access must be authorized under the principle of least privilege and based on minimal need and all access to Confidential data must be authenticated and logged.

When necessary, data transmission and storage should be encrypted. Sensitive data such as student records should be encrypted to ensure data confidentiality and integrity when transmitted over a network.

Data having value beyond the person that created it or data critical to the mission of the AIG Business Solution (P) Ltd. shall be located, or backed up, on centralized servers maintained by the organization.

Appropriate effort shall be taken to protect data integrity, confidentiality and availability wherever it may reside: on a production server, on a disk array, on tape, on CD ROM, etc.

Prior to redistribution of medial, all data must be scrubbed from any media not scheduled for destruction.

**SECTION III**

# AIG Business Solution (P) Ltd. Network IT Security Procedures

## Acceptable Use Policy

**Statement of Policy**

All Staff of the organization must adhere to an acceptable use policy. This policy embodies the principles of appropriate use of organization's resources.

**Target Audience**

The target audience for this document is any person with access to any resources owned or managed by the organization.

**Scope**

The Scope of this policy encompasses the use of following resources controlled by the organization.

1. Computer systems (Desktops and Laptops)
2. Telephone systems (IP, Digital & Analog)
3. Copier machines
4. Printers
5. Fax machines
6. Scanners
7. File downloads, Backups, Maintenance
8. Library Books, Reference material and process manuals.

All persons accessing these resources are governed by this policy.

**Responsibilities**

1. Users of Resources Responsible For:
   1. Conforming to this policy at all times.
   2. Ensuring they understand the importance and detail of this policy.
2. AIG-HIPAA-Team responsible for
   1. Ensuring compliance with this policy
   2. Working with HIPAA Compliance team and other teams as appropriate in order to address breaches to this policy.
3. Admin Team Responsible for:
   1. Ensuring compliance with this policy
   2. Implement policy in areas under its control.
   3. Checking periodically on activities carried out through the contractors to comply with the policy.

**Procedure**

1. Confidentiality of Information
   1. Information placed upon computer systems of the organization is considered the property of the organization. Information must not be used for any purpose other than as a course of the business duties of the user.
   2. Although generally respecting the privacy of its users, organization's HIPAA Compliance team or the AIG-HIPAA-Team staff upon the management request may at any time and for any reason monitor electronic communications and documents conducted via its computer systems and networks.
   3. Users should consider the sensitivity of information before allowing it to leave secured premises by either electronic or physical means.
2. Use of Computer Systems
   1. Users must be considerate with the use of computer systems. Systems are provided for work related activities.
   2. Theft of accounts or identity: Users shall not fraudulently use or attempt to fraudulently use another user's account or identity. Prohibited activities also include stealing another individual's password through "social engineering" (duping someone into revealing a password), capturing passwords through the use of hardware or software, procuring or using tools which are designed to compromise system security, or otherwise gaining unauthorized access to any other user's account. Exception: AIG-HIPAA-Team may use "cracking" tools to locate and close security holes in the computer systems.
   3. User shall not leave their system, which is actively logged into the organization's domain or network unattended or unsecured. They shall log off or lock the system before they leave their desk.
   4. Service denial: A user shall not intentionally exhaust computer system resources (e.g., disk space, bandwidth, paper, CPU time, etc.), particularly when such resource exhaustion blocks authorized access to computer system resources.
   5. Vandalism: Users shall not damage or destroy computer hardware, software, or data unless authorized to do so. In particular, users shall not negligently or intentionally damage or destroy data that belongs to another user unless authorized to do so.
   6. Negligence: Users of the organization's computer systems shall exercise due diligence when working with applications that, used incorrectly, can damage equipment or data, particularly when said applications require special skills or knowledge to use correctly.
   7. Supervisors are responsible for verifying that their subordinates are both sufficiently skilled to perform assigned tasks and sufficiently careful in the performance of those tasks. Failure to exercise due diligence may result in restriction, suspension, or revocation of access authority.
   8. Logging: Organization's computer systems automatically log e-mail   and other traffic. Logged information generally includes user addresses and other header information, logon and logoff times, workstation IDs, etc. This information is required by AIG-HIPAA-Team to verify consistent and proper system operation. E-mail message bodies are not logged normally, but may be monitored.
   9. Business documents: A supervisor of an unavailable organization's employee may request, in writing, with specificity, that a AIG-HIPAA-Team member accesses the unavailable employee's computer files and obtain a copy of the requested document
   10. Former employees: A former employee's computer system files will be transferred to the appropriate supervisor and/or the person who replaces the former employee.
   11. The users shall not be given administrative access to the systems. This would restrict them from installing software, access administrative utilities etc. A user who would specifically need administrative access shall obtain the same till completion of task, through a request to AIG-HIPAA-Team and compulsory approval from the team head and AIG-HIPAA-Team manager.
   12. Environment: Computer usage may result in physical problems including, but not limited to, eye strain, carpal tunnel syndrome, and other repetitive stress injuries. Users are encouraged to inform AIG-HIPAA-Team, supervisors, or the Human Resources office of environmental conditions related to computer usage that may adversely affect them, in an effort to assist organization in providing a safe work environment.
   13. Installation and Use of Software and Hardware
       1. Users must not install software or hardware without the written authorization of senior management. Explicitly forbidden is pirated software, downloaded freeware, copyrighted materials such as MP3 music files and computer security / hacking tools.
       2. Any additional software apart from the ones installed by default shall be installed by the AIG-HIPAA-Team after due approval from the team head and AIG-HIPAA-Team manager.
   14. Control on Desktops  
       All desktops are protected with CD Read/Write Access, Floppy drive access, USB port access and Bias Setting. These controls shall be in place when the desktop assigned to any Users.
   15. Control on Laptops  
       Laptops are provided to Senior Management and Business Development Managers. Access to USB port and CD write access shall be removed to Business Development Managers. Such access shall be given only when the Laptop is carried to abroad for business purpose based on recommendation from Business Development head.
3. Telephone systems
   1. Digital phones or IP phones shall be provided to the processes that require them for business purposes. The phones will be provided after approval from the operations head and AIG-HIPAA-Team head.
   2. All transactions including voice, duration, numbers dialed etc. over the digital phones shall be recorded and monitored by the quality and AIG-HIPAA-team in order to audit the calls. Hence, it is strictly required for the users to use this facility only for the business purposes and not for any personal purposes.
   3. Analog phones shall be provided in the areas where it is required for business purposes. The analog phone extension shall be provided by the facilities team upon request and due approval from the operations manager.
4. Use of copier machines
   1. Photocopying machines are provided in the organization to facilitate photocopying of business related documents or papers.
   2. Accesses to Copier Machines are restricted to only Support Team (HR, Admin, Accounts & IT)
   3. HR will monitor no. of copies photocopies as against logins monthly.
5. Use of Printers
   1. Printers are provided for all operations considering the need for the same in organization's Business. Users shall take responsibilities in appropriate use adhering to the policy.
   2. Users shall not print any documents unless it is mandatory to print them.
   3. After printing, the user shall immediately collect the printed information from the printer.
   4. No printed information shall remain near the printer's unattended, giving unauthorized access to others.
   5. User shall drop in the bin (named "to be shredded") after using them. These bins are kept near the Printing Machines. Housekeeping team will collect the same and shall shred at end of the day.
   6. Any information above confidential classification mark and in electronic form shall be printed only after authorization from the operation manager.   
      Classification: The HIPAA Compliance Team shall periodically conduct physical inspections in the work areas to check policy adherence, record violations and take necessary actions to avoid the same in future.
6. Use of Fax Machines
   1. E-fax can be used for both outgoing and incoming fax services
   2. User shall send e-fax only for business purpose. User will send e-fax along with cover sheet only.
   3. Access to delete the "sent items" has been restricted for the users. AIG-HIPAA-Team will delete more than 1 week old sent items.
   4. Any misuse of the e-fax or breach of confidentiality of information through fax must be immediately reported to the respective Process head, Human resources and the HIPAA Compliance team by the person's in-charge.
   5. The HIPAA Compliance team along with Human resources shall take necessary actions to avoid such incidents from happening in the future. They may suggest improvements on the controls.
7. Use of Scanners
   1. The scanners are to be used strictly for official purposes only. Users cannot use organization's scanners to; Scan personal documents, photographs & other objectionable material.
   2. User shall save scanned document in their respective path. Scanned files should not be saved in local drives (PC connected to scanner) for security reason as this may allow other users to view the document. In case such scan files found in local drives, the same will be deleted on daily basis by Utilities.
   3. The HIPAA Compliance team shall have full rights to question users on the use of scanners during their periodical visits and in detection of personal usage or so; they may recommend the AIG-HIPAA-Team to withdraw this facility for ever.
8. File downloads, Backups, Maintenance
   1. Inventory of backup CDs shall be maintained by Utilities and inventory check shall be done in the first week of every month. Records of the same shall be maintained by Utilities.
   2. Additional backup CDs shall be provided based on Senior Management approval from concerned departments on returnable basis. Inventory of backup CDs for different departments shall be maintained as centralized system in Utilities.
   3. Formatting shall be done in case the item connected to data storage before its taken out of premise (both for returnable and non-returnable). Record shall be maintained on detail of formatting and shall be verified before it is sent out of premise.
   4. Gate Pass (Returnable) shall be used in case any Items/materials planned to send outside for repair or to complete any activity. Such Gate pass shall be approved only by Head Infra/Head HR.

## Enforcement through Access Control Lists

### Physical Security

Statement of Policy

Physical security involves the proper layout and design of facilities and the use of measures to delay and prevent unauthorized access to organization assets. It includes measures to detect attempted or actual unauthorized access, and activate an appropriate response. Physical security also provides measures to safeguard employees from violence

Purpose:

1. To ensure 100% HIPAA compliance at AIG i.e. –
   1. No Paper
   2. No Pen or Pencil
   3. No Pen drive, CD drive, Hard Drive
   4. No Mobile, Laptop
   5. No Camera
   6. No Any electronic items.
2. To ensure Security at AIG i.e.
   1. No Arms
   2. No Matchbox
   3. No Tobacco etc.

No materials taken from office Procedure

* + Compliance Officer is designated by the Admin/Management and he/she will manage the security of the systems.
  + Our personnel are screened for any data capture devices so that no sensitive information is compromised.
  + Round­the­clock security guards ensure that our buildings are totally secure.
  + We also use digital copies for exchanging data so that no paper printouts can change hands.

Standard Operating Procedures at AIG Business Solutions for Security Staff:

1. Frisking Means:

● Bag Check ­

○ Make the entry of the items on Employee’s Items register and ask to the employee to keep it to the other room or locker.

○ At the time of exit make sure the employee carry out only those items which are mention in the register and no office items.

○ If any Tobacco product found security guard has to ask to the employee to throw it outside of the office premises.

● Pocket Check­

○ Have all employees empty their pockets and show their inside out and check all the items.

● Waist and Socks­

○ Pat down waist and socks and check all items, if any unauthorized item found make the entry of item in register and keep it in locker.

○ At the time of exit make sure the employee carry out only those items which are mention in the register and no office items.

1. Whom to Frisk­

● Frisking is required for 100% employees including Chairman, Director, VP, AVP, Sr. Manager, Executives and all visitors.

1. Employee Entry SOP –

● Security guard will ensure the entry of employee only after the checking of AIG’s ID card. If the employee will not show the ID card then security guard has to inform Admin and only after the following steps the employee will get the permission to entry into the office:

○ That employee must call to their Reporting Manager and the Manager has to approve his entry.

○ After that, Admin will call to security and make the entry for employee.

* + - Security must enter the in time of employee in attendance register.
    - Frisking as per 1.
    - Employees must deposit their mobile to security guard at the time of entry.
    - Security guard must ensure the security of item which are deposited to security guard.
    - List of authorized person allowed for Mobile, laptops, Pen drive, and all other electronic items.

○ Director

○ Sr. Manager Billing

○ Manager Billing

○ IT

○ Admin

○ HR

○ Accounts

○ Recruiter

* + - No one can carry any electronic items or documents on the floor without the approval of Concern department head or Administration.
    - Security guard must make sure employees do not carry out any official documents or electronic items of office.

1. Break Time SOP (i.e. going in & out of the office during normal shift timing)
   * + The employee can go only with Ball frisking when he/she go out or come in at break times.
     + In Ball frisking there are 4 ball in a box 3 are of same color and 1 is of different color. If an employee pick the different color ball the security must frisk the employee.
     + If the employee pick the same color ball he can enter the premises without frisking.
     + Security guard must make sure that each employee punches in biometric attendance machine each entry or exit.
2. Employee Exit SOP –
   * + Security Guard has to check the employee bag for any such item:

○ Mouse

○ Pen Drive

○ Office Note Pad

○ Office Pen

○ Any other office’s electronic items and official documents

* + Frisk the employee and check that the employee is not carrying out any official items or document without approval of Administration.
  + Enter employee exit time in attendance register and make sure employee punch in biometric attendance machine.

1. Visitor Entry & Exit SOP­
   * Security must ask for the purpose of the visitor.
   * Security guard must give the Visitor register to the guest/visitor and make sure the visitor/Guest fill all the details as required.
   * He must inform the visitor that we are a data secure place just like an airport, so we need to check for any electronic items by emptying of the pockets, going through your bag.
   * Security guard must frisk the visitor/Guest
   * Security guard must issue a visitor pass to the Guest/visitor who carry mobile, laptop or any other electronic items, and mention the items in the visitor pass
   * The visitor pass will be signed back by concerned person whom visitor is meeting and has to be returned back to the security guard at the time of exit.
   * During Exit security guard will recheck the visitor.

## Entity Authentication procedures

Entity Authentication procedures to verify that the person or entity seeking access EPHI is the one claimed

### Password Policy

**Statement of Policy**

Passwords must be chosen, handled and used in a manner, which maximizes their effectiveness as an authentication control.

**Target Audience**

The target audience of this policy is the employees of the organization and any third parties who utilize passwords provided by the organization.

**Scope**

The scope of this policy pertains to all passwords within the environment that are issued by the organization or that are used on organization's owned or operated systems.

Explicitly out of scope for this policy are passwords used by staff for non­work related systems that are not used in any manner relating to the business of the organization and passwords used to access client network or systems.

**Procedure**

1. Password Policy Standards
   1. Password Complexity

The complexity of passwords shall be maintained by users and those generating passwords for users as per this table

1. Password Management Guidelines
   1. Password and User ID Allocation

The allocation of user IDs and passwords must be strictly controlled. User IDs and passwords are required as the principal means of validating a user's authority to access information services.

* 1. Only the AIG HIPAA Team is permitted to allocate initial passwords to user, who will be required to change it on first use before accesses to systems are granted.
  2. When new accounts are created, the AIG HIPAA Team member must assign unique password and it should be provided to user via phone or Process Manager.
  3. Users must acknowledge receipt of passwords to AIG HIPAA Team.
  4. Storage and Transmission

Passwords are automatically classified as CONFIDENTIAL and must be protected appropriately.

* + 1. If passwords are stored on hosts, they will be encrypted. Under no circumstances is password information to be stored in clear text on hosts, even if they do not relate to the host on which they are stored.
    2. Passwords and user details should not be written on paper bits and left on desks or stuck on monitor screens, keyboards etc
    3. Clear text passwords must never be embedded into application or user files, end user device emulator or file transfer set­ups, etc unless on a computer stored or operated in a proven secure area.
    4. Password files must be stored separately from the main application system data.
    5. A copy of all administrative passwords will be available with the head of AIG HIPAA Team group; the same is to be kept in a sealed envelope and will be opened in case of emergency or non­availability of AIG HIPAA Team personnel. This copy will be destroyed and replaced with the new one when the password changes occur.

1. Management system

An effective password management system will be used.

The organization's password management system will:

* 1. Enforce the use of individual passwords to maintain accountability
  2. Require users to select and change their own password
  3. Ensure passwords conform to the organization's standard
  4. Not to display passwords on the screen when being entered
  5. Prevent new staff from inheriting user IDs and passwords from their predecessors
  6. Log password reset requests, keeping details including the asset ID (for which the password was reset), the name of the resetting member and the time the reset was initiated
  7. Ensure that reset passwords comply with the organization's password standards
  8. Disable user access of all permanent staff, contractors or consultants immediately after they leave
  9. In case of AIG HIPAA Team managing or troubleshooting systems through the remote management utilities, they shall not ask for user passwords over phone, instead, they shall allow users to logon and then take control of the system.

1. Users must follow good practice when managing their user Ids and passwords.
   1. Good end user practices in the selection and use of passwords are essential.
   2. All users are required to adopt the following practices when setting and managing their password.
   3. Select passwords that conform to the AIG Business Solution Pvt. Ltd. HEALTHCARE BUSINESS SERVICES standard. Don't use a weak password just because it's easier to remember.
   4. Keep all passwords confidential
   5. Don't give your password to ANYONE. Don't give it to your manager, your spouse, your friend, the VC, your mother, or any other authority
   6. Don't write down your user ID or password: remember it. It's better to have your password reset when you have forgotten it than to have it stolen
   7. Change passwords whenever there is any indication of possible system or password compromise
   8. Change initial passwords a t the first logon
   9. Do not include passwords in any automated logon process, e.g. stored in a macro or function key
   10. You are responsible for ANY activity using your account user ID and password
   11. Don't let anyone observe you entering your password. Cover your keyboard when logging in if someone is watching you, or ask them to turn away
   12. If your password has been changed or reset and you didn't request it or change it, please let the Help desk know

It is the business owner's responsibility to ensure that all users have been instructed in the selection of secure passwords and their use.

## Policies and procedures to address security incidents

### Data Security

AIG Business Solution needs to gather and use certain information about individuals.

This can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards ­ and to comply with the law.

Purpose:

This data protection policy ensured AIG Business Solution

* Complies with data protection law and follow good practice
* Protects the rights of staff, customers and partners
* Is open about how it stores and processes individual’s data
* Protects itself from the risk of data breach

Procedure:

* All confidential information is restricted to computers i n which our personnel work on
* No one is given access to floppy and USB drives
* Process executives working on client data are denied access to emails
* High security firewalls and access logged computers restrict the movement of information and lock it down to the computer in which the personnel are working on. In cases, where the client requests that we work on their servers, we operate remotely through the customer's computer, nullifying the risk of data theft.
* Email access is restricted or banned for process executives working on a healthcare project when handling client data.
* All email Data will be encrypted.

### Anti­Virus Policy

Viruses and other malicious code represent a very real and frequent threat to organizations. Strong controls must be utilized to ensure that organization's systems and network remain free from such malicious content.

Target Audience

The target audience f or this policy is all users of organization's computer and network systems.

Scope

The scope of this policy covers all staff, contractors and systems of organization

Responsibilities

1. Users
   1. Sensible handling of external content via any media including floppy disks, CD­ROMs or Internet delivery.
   2. Reporting virus alerts to AIG­ HIPAA­ Team
2. AIG ­HIPAA ­Team Responsible for:
   1. Ensuring currency of anti­virus controls.
   2. Ensuring adequacy of gateway controls.
   3. Reporting incidents to HIPAA Compliance team.
   4. Managing virus outbreaks

Procedure

1. Anti­virus Policy Standard
   1. Anti­virus controls are placed such that any foreign content entering the organization is scanned by at least One Antivirus software
   2. Gateway systems such as proxy servers and email server must scan all traffic for virus' either inbound or outbound.
   3. All servers must have real-time scanning enabled.
   4. All desktops must have real-time scanning enabled.
2. Foreign Media and Data Classification

All media and data from external sources must be scanned for malicious content before being introduced onto network file servers and systems.

1. Managing Virus outbreaks
   1. In the event of a virus outbreak, AIG­ HIPAA ­Team will be responsible for

coordinating efforts to control the situation.

* 1. Due to the large potential variation in impact of any such event, it is impractical to describe here all possible actions. However, when managing an incident, AIG ­HIPAA ­Team must be mindful of the cost to the business of any action or continued outbreak
  2. Potential controls utilized to reduce an outbreak and regain control of the environment include:
     1. Shutdown of nonessential services.
     2. Disabling entry and exit points for viruses into or from the network.
     3. Segregation of infected network sections.
     4. Disabling of services such as file sharing.
     5. Infected systems (as opposed to those systems simply containing a copy of the virus but not infected by it) must be re­built either from original media or from last known good backup.

1. Laptop and Remote Systems
   1. Laptop and remote systems pose an increased level of risk as they may not be able to receive direct updates via the central anti­virus update management system.
   2. Laptops must have anti­virus signatures automatically updated when connected to the network either directly or via remote access.
   3. Content from remote systems must be scanned before being allowed onto the network in accordance with the defense in depth principal under this policy.
2. Associated Procedures
   1. Users suspecting that his/her workstation has been infected by a computer virus must IMMEDIATELY POWER OFF the computer and notify AIG HIPAA Team to coordinate virus removal operations.
   2. The Users shall not turn off the anti­virus software installed on their systems at any given point.
   3. Suspicious e­mail messages (spam/virus) should be forwarded to itsupport@aigbusiness.in for investigation before they are opened.

### Firewall Policy

Firewalls form an important part of the I T Security architecture of AIG B usiness Solution Pvt. Ltd. Healthcare Business Services. Firewalls as such must be appropriately deployed and managed in order to ensure their ongoing usefulness as a control against attack.

Target Audience

The audience of this policy is AIG HIPAA Team

Scope

The scope of this policy extends to all firewalls in use by the organization.

Responsibility

AIG HIPAA Team is responsible for compliance of this policy

Procedure

1. Firewall Design
   1. Firewall has been designed based on the following aspects
      1. Risk & Threat Assessment
      2. Administration
      3. Monitoring
      4. Configuration Management
      5. IDS
   2. We shall allow the minimum access required through the firewall for the business purpose, i.e. it restricts to ports, protocols, IPs & networks etc.
   3. We deploy firewall rule sets based upon a default deny principle and rule and when failures occur must by default deny all.
2. Firewall Monitoring
   1. Firewall logs are monitored depending upon the risk and as and when required.
   2. Logs are reported to a centralized log host.
3. Remote Management
   1. Remote management of firewalls is performed via encrypted sessions, from restricted systems only.
4. Anti­virus

Where practical and where data capable of containing viruses or other malicious code traverses a firewall, anti­virus controls has been implemented in accordance with the Anti­virus Policy.

### Clear Desk and Screen Policy

Desks and Screens within the organization or controlled by the same must be cleared of any non-public domain classified information when not attended. This reduces the threat in the event of unauthorised access to a workspace.

Target Audience

The audience of this policy is anyone working within an environment controlled by the organization or working with information controlled by the organization, which is not public domain information.

Scope

The scope of this document extends to all desks, workspaces or screens containing or accessing information of the organization with a classification higher than Public Domain. This policy explicitly includes desks and screens used in work from home and telecommuting arrangements.

Responsibilities

1. Ensuring systems are configured to auto lock and display screen savers.
2. Ensuring organization's screen saver policy enabled at the domain level, which activates when there is no activity on the system for 5 minutes.

Procedure

1. Where a desk will be unattended for more than an hour, information of a classification higher than Public Domain must be removed and securely stored.
2. No Information related material must be left unattended on the desk or anywhere near the work area which would allow another person to access the material.
3. All computer systems must automatically lock the screen and screensaver is enabled when the system is not in use for more than 5 minutes.

## Activating and modifying accounts to laptops / workstations and EHR systems

## 

**Statement of Policy**

AIG Business Solution Pvt. Ltd. HEALTHCARE BUSINESS SERVICES shall follow a standard registration/de­registration/access control procedure for all the users who are to be allocated access to resources of the organization.

**Target Audience**

All the staff of the organization in general and AIG­ HIPAA ­Team along with Human Resources in specific.

**Scope**

All the users who shall be registered on domain server, mail server, intranet & data servers etc.

**Responsibility**

AIG ­HIPAA ­Team, Process Manager, and HR

**Procedure**

1. User Creation
   1. Creation of User IDs for Domain servers, E­mail and Intranet etc. shall be handled only by the AIG ­HIPAA ­Team
   2. The new user IDs shall be created only after receiving the request from HR/Process Manager.
   3. The IDs shall be created in the following manner:
      1. The user ID shall have the FIRST and LAST NAME with point (.) in between e.g. if the username is Ashish Gupta where Ashish is the first name and Gupta is the last name, the User ID shall be created as Ashish.Gupta.
      2. In case of an existing user with the same ID, the new user ID shall be the First and Last Name without point (.) symbol in between.
      3. If the username is unusually long, the first name shall be truncated or the initials shall be used in place of first name.
      4. The same user ID shall be used across servers
   4. The users shall maintain their user Ids or login name and passwords confidential
2. Access Control
   1. The AIG­ HIPAA ­Team shall have access to allocate or modify user privileges on the servers.
   2. AIG­ HIPAA­ Team will provide/remove access to folders only based on communication from Process Manager. Request mail will be copied to concerned Process Manager & HR.
3. De­registration or Revoking of Rights
   1. The User IDs and rights shall be removed across servers once the user quits or ends his/her service with the organization.
   2. Revoking of rights for users shall be made by the AIG ­HIPAA­ Team once they receive the "EMPLOYEE EXIT PROCESSING FORM" filled by users with due approval from the respective process head / managers before reliving. This process shall be initiated from HR.
   3. In case of termination, the same "EMPLOYEE EXIT PROCESSING FORM" shall be used on the last day of his/her employment.
   4. In case an employee is absconding/uninformed leave more than 3 days, concerned process manager will report the problem to HR and a memo will be sent to the concerned employee. If there is no reply to memo or he/she has not joined the duty, second memo will be sent. Entry access and User ID deactivation shall be done at this time.
4. Associated Procedures
   1. The HR shall get the personal details filled by the candidate, then fill in the appropriate details in the HR section of the form and forward the form to the respective department / process head to fill in their details and later forward the form to the AIG HIPAA Team.
   2. AIG HIPAA Team staff create email id only from receipt of approval from IT Manager.
   3. The access is to be given only to the resources approved by the Department / process head.
   4. The forms shall be filed in records for future references.

## Policy and procedures that specify audit and accountability

### HIPAA Compliance Team

HIPAA Compliance Team is formed involving different functional areas. Below are the HIPAA Compliance Team members.

Kaushal Kumar ­ from IT

Karan Bhattal ­ from HR

Asheet Raj ­ from Admin

Mr. Ravindranath ­ from Billing Operation

Mr. Amit Gupta ­ from QA

HIPAA Compliance Team responsible for:

1.1. The compliance to this Policies and Procedures in their respective areas.

1.2. Participate in quarterly compliance audit

1.3. To work with concern area responsible based on audit findings in order to ensure corrective measure.

1. Audits will be done extensively in order to check the compliance of AIG Business Solution Pvt. Ltd. Healthcare Business Services Security Policies & Procedures (physical checks where appropriate).
2. HIPAA Compliance team will have watch on day to day compliance requirement and will do spot check at times.
3. Compliance and non­compliance (breaches) shall be recorded during the audit.
4. Management Review:

Audit findings shall be reviewed by top management on monthly basis. Top management will also review the corrective actions taken against the breaches.

In case corrective action is connected to top management assistance/support, the same will be discussed in the management meeting.

### Human Resources

1. All users must acknowledge and sign to the fact that they are aware of all IT Security policy documents and will adhere to this and other policies at all times.
2. Signatures of acceptance must be obtained before system access is granted to any user.
3. All staffs of the organization are encouraged to report violations of policies (violated by any staff) to the HIPAA Compliance team/HR. They shall send details of persons involved in violation, time of violation and resource subjected to violation. Their identification shall be maintained confidential.
4. Breaches may also be referred to relevant law enforcement or other authorities as appropriate by HR
5. Any breach of this policy is considered a serious occurrence. Breaches of this policy will generally be referred to Human Resources and disciplinary action may result.
6. Non­compliance or violation by the staff shall lead to serious decisions by the management, even leading to the termination of employment.

### HIPAA Training

1. Formal training of HIPAA will be conducted for the newcomers as part of induction training. HIPAA Policies and Procedures will take part a s part of training.
2. Applicable Legal and Regulatory Compliance Policy and its practices shall be communicated during the induction programs by HR.
3. HR will communicate to all process owners/Training dept. in case any amendments to the policy as and when it occurs.
4. Training dept. will plan Refresher Training Program on HIPPA Policy requirements to all employees once in 6 months. During this training program, all applicable organization's HIPAA Policies and Procedures will be refreshed. Refresher Training Program also contains current applicable Legal and Regulatory Compliance Policy and its practices in the company.
5. Training dept. will keep records on topics covered during training and tests on

effectiveness of training for future reference.

### Legal and Regulatory Compliance Policy

Statement of Policy

The staff, contractors or business associates, visitors and service providers of organization shall be bound by the laws and regulations that are applicable to the company.

Target Audience

All staff of the organization

Scope

Organization shall be bound by the following Laws / regulations / regulating bodies

HIPAA Compliance

Fair Debt Collection p ractice act OIG (office of inspector general)

Confidentiality and Non­disclosure agreements with clients

STPI (software technology Parks of India)

Indian Companies Act 1956

Intellectual property rights & Copyrights Act.

Other Statutory laws of India

Responsibilities

1. Process Managers

Responsible for:

* 1. Ensuring appropriate level of knowledge transfer to the staff on the compliances bound with processes.
  2. Conducting periodical refresher training programs on the compliance.

1. Staff Responsible for:

Strictly respecting and abiding with the compliance.

Procedure

* 1. Knowledge Transfer
     1. Knowledge transfer to staff, on the relevant regulations and its practices in organization shall happen during the induction programs.
     2. Staffs are encouraged to interact more with the trainers to get better

understanding on the applicable laws and the impacts in case of violations.

* 1. Confidentiality and Non­Disclosure Agreements (NDA)
     1. Signing of these documents shall be mandated to any staff during the joining formalities.
     2. Signing of Visitor site NDA shall be mandated to those who would have access to the internal information of the organization.
     3. Business Associate agreement as per HIPAA privacy rule requirement will be maintained for all the customers.
     4. Letter of Intent (LOI) shall be issued for the new contractors for the initial period of 6 months (evaluation period). NON­DISCLOSURE and NON­CIRCUMVENT

1. AGREEMENT shall be signed along with LOI.

Business Associate agreement shall be signed with contractors after 6 months based on performances. Good practices while handling confidential information. The staff involved in processing confidential information (e.g. PHI) shall follow the practices as instructed during the induction programs.

1. Reputation of organization and individuals

The staff shall understand that violations to the applicable laws shall have great impact on the organization's reputation as well as the individual's.

1. Statutory requirements

The legal, finance and HR departments shall look into the needs and periodically meet those needs, to ensure compliance with statutory requirements.

## IT Security Standards for Servers and Desktops

The following standards are required for all computers (servers and desktops):

**General Standards:**

* All servers must be registered tie AIG Business Solution IT Support.
* All servers must have a static IP. Static IP addresses can be requested through Network Services.
* Device registration: Any desktop computer and any network addressable device that connects to a campus network should be approved by and registered with the campus IT department. IT Support System shall maintain must maintain a current inventory of all desktops and servers. At a minimum, the inventory should contain the computer’s serial number, software and OEM license number of software preloaded through the manufacturer, the location, and who the computer is assigned to.
* IT Support System shall maintain develop, test, and maintain a disaster recovery and business continuity plan.
* IT Support System shall maintain backup and restore procedures.
  + - Run regular schedule backups of data. Backups should be stored off-site. If your department lacks this capability, ITS can provide these services.

**Data Security Standards:**

* + - IT Support System must determine and classify types of data stored on servers and desktops.
    - All servers and desktops containing sensitive or confidential data must have methods installed and enabled to protect data.
    - Access should be given only to those who require access to such data. That access should be only what is necessary (i.e., read, write, modify, etc.).
    - It is recommended that confidentiality agreements be signed and secured from users accessing data which needs to be protected from unauthorized access.

**Physical Security Standards:**

College and department servers must be located in a secure area with up-to-date documentation of who has access. Area should be one which is not public and only accessible by those who require access. Doors and windows must be locked when not in use. A log of who has keys to the area must be maintained. Keys must be collected from those who no longer need access to the area.

Servers should be located in a climate controlled environment.

Use of a UPS (Uninterruptable Power Supply) is recommended. It should have line conditioning for electrical and network cabling.

It is recommended that servers are cabled and locked to an immovable surface or stored in a cage that is locked. If desktops are located in a public area, they must be cabled and locked to an immovable surface.

Fire suppression services must be available (fire extinguishers).

**Logical Security Standards:**

* Operating systems and applications must be current with all service packs and patches. Anti-virus software must be installed and current with all recent signatures.
* Install and enable a firewall.
* Configure to allow only necessary/required traffic.
* Review logs regularly for inapprop0riate or unneeded access.
* Logs must be kept a minimum of thirty (30) days.
* Review the purpose of the server/desktop to only allow services, applications, and access as they pertain to the purpose. For example: If being used as a Web server, data, or data bases, should not be maintained on the same machine.
* Run only the services needed on the server.
* The services must be related to the role it is serving.
* Install only software and applications that are needed for the purpose of the machine.
* Use SFTP (Secure File Transfer Protocol) or SSH (Secure Shell) protocols.
* Disable Telnet and FTP (File Transfer Protocol) protocols.
* Disable all services that will not be used.
* Configure all services to log all connections and authentication information Assign appropriate person to review logs and report any unusual activity. Logs must be kept for a minimum period of thirty (30) days.

**User Account Standards:**

* + A unique login and password must be created for each user.
  + Password standards must conform to AIG Business Solution (P) Ltd. and AIG Business Solution (P) Ltd. policies and procedures.
  + The administrator/root account must be renamed and strong password created. Only the individual managing the server should have access to the administrator account.
  + It is recommended the server is not run in administrator mode. Administrator mode should be used only when necessary.
  + Force new users to change their password when their first login.
  + The guest account must be deleted or renamed and a strong password set.
  + Disable or delete old accounts/logins that belong to those who no longer need access.
  + For those who are terminated wither voluntarily or willfully, the accounts must be locked or deleted. If account is a shared account, the password must be changed each time someone is added to or leaves the group. Password should be changed on a regular basis for these accounts.

**Reassignment/Surplus of Electronic Equipment:**

* Colleges and departments shall use a secure deletion program that conforms to DOD standards to erase data from hard disks and media prior to reassignment, surplus, or disposal.
* Colleges and departments shall maintain changes to inventory.
* Operating system and any application software that was initially shipped with computer must be reassigned with computer.

Failure to follow established security standards can result in sanctions.

## Policy and procedures that specify physical and environmental safeguards used

### Physical Access Policy Standard

Human Resource is responsible for the adherence on this policy with the help of support services.

1. Segregation in Areas within the organization
   1. The areas within the organization have been segregated as under, depending

upon the sensitivity with respect to information security:

* + 1. Common Area
    2. Restricted Area
    3. Restricted Areas (Authorized Persons Only)
  1. The common areas are areas like corridors, cafeteria, reception etc. where staff of the organization, visitors and the contractors shall have access to. There shall be no restrictions in those areas.
  2. The restricted areas are the information processing (KPO), software development and other support activities shall be carried out in those areas. Access to those areas will be available to only those who work in that area.
  3. The high sensitive areas shall be marked as the 'Restricted Areas (Authorized Persons Only)". The Server rooms, UPS and Electrical rooms shall be treated as highly sensitive and access to these areas shall be given to AIG HIPAA Team staff, Facilities team and the Security supervisor only. However, temporary access shall be given to people who would carry out repair work during breakdowns and this shall be done with one member of the facilities team or security supervisor being present at the location.

1. Use of Physical Keys
   1. All physical keys of the organization shall be maintained by the Administration in a locked storage.
   2. Allocation of physical keys must be noted in the Key register by the Administration.

Physical keys should not be used for sensitive areas, such as computer rooms and UPS rooms, where a strong audit trail is required.

1. Mobile Phones Access
   1. Access to the mobile phone is restricted to limited employees. Employees whoever has access to mobile can carry only mobile without camera facility.
   2. Employees whoever authorized to carry mobile with camera has to put a tag on camera lens when he/she enter into restricted area or submit the mobile to security before entering into restricted area.
2. Access Card Usage
   1. Access cards showing appropriate identification must be visibly worn at all times.
   2. Allocation of Visitor passes must be recorded in the visitor register.
   3. Visitor passes must be collected when the visitor exit.
3. Granting of access
   1. Access must only be granted to those areas required by an individual for the course of their general daily duties.
   2. List of employees who are going to work in the week ends shall be provided by Process Manager to Admin. Security guard shall ensure that only listed employees enter the premise.
   3. Access to restricted area by any visitors shall be handled by receptionist/ Guard only after the permission of Admin.
4. Removal of access

Access must be removed from all users when no longer required as a part of their daily duties.

Classification: Access must be removed from resigning staff on their final day and access cards, keys etc. must be reclaimed.

1. Entry and Exit Doors
   1. All doors must be self-closing either electronically or via mechanical closing mechanisms.
   2. Bio­metric access system is provided to all employees. Employees should provide their thumb impression to enter in the operational areas.
   3. The exit shall be only through swiping of access cards or finger print.
2. Frisking and Personal belongings
   1. Staff working in information processing & development areas shall leave behind their personal belongings (like bags, CDs, USB drives etc.) in locked storage provided before entry.
   2. Bag frisking shall be conducted randomly by the security personnel for all staff of the organization. The staff shall co­operate with them during this activity.
   3. The contractors on duty shall be subjected to frisking on a daily basis by the security personnel.
   4. The security on detecting any official material (books, manuals, CDs etc.) being carried out, shall inform the Admin and HIPAA COMPLIANCE team immediately and shall allow entry / exit only after written approval from them.
3. Security Guards
   1. Trained and specialized Security guards are appointed at the facility through an outsourced agency.
   2. The Security guards who are under the control of Admin, admin is responsible for the physical security of the organization's facilities.
   3. A register shall be maintained by the Admin, which would record the details of the security personnel on duty, their in time, out time etc.
   4. A checklist of tasks to be carried out by security guards shall be provided by the Admin. The security personnel on duty shall follow the checklist and shall sign the same every day, confirming that he has carried out his routine checks on a daily basis. This record shall be maintained and monitored by the Admin.
   5. The security guards shall be provided with details of key contacts of the

organization whom they shall contact in case of incidents like theft, fire etc.

1. Contractors on duty
   1. Housekeeping / Pantry staff
   2. Canteen staff
   3. FMS staff
   4. Security staff
   5. The housekeeping staff shall be under the control of the Admin.
   6. All activities of housekeeping staff shall be monitored by their supervisors and the

supervisors shall report to the Admin on a daily basis all information about the staff on duty, their working hours, their activities etc.

* 1. The Housekeeping staff shall not have entry to the restricted areas (authorized persons only) areas of the facility and in case of any work to be carried out through them in the sensitive areas, the Admin shall be physically present till the completion of the work.
  2. The canteen staff shall have access only to the common areas and in­case of their service requirements in restricted areas; they shall be accompanied by the security guard.

1. Interviews
   1. The training team shall provide enough rooms to conduct interviews or tests outside the operational areas.
   2. The interview facility shall have enough number of computers required for testing purposes. The computers shall be installed with test data and the applications required to be tested upon. The interview candidates at any cost shall not have access to live systems, data or the network of the organization.
   3. The interviews shall be held with prior information and consent of the Human resources and Admin.
   4. All candidates appearing for interview shall enter their details in the interview register maintained by the Human resources, which shall be made available at the reception during interviews.
   5. In case the candidates have to be brought inside the operation areas, they shall be escorted by the respective interviewer and it shall be the responsibility of interviewer to make sure the candidate has no access to any internal information till the time he is escorted back to the common area.
2. Visitors
   1. Staff who would expect their visitors shall inform the front office about the same in advance.
   2. Visitors shall enter their details (their name, their company, person to visit, purpose of visit etc.) in the visitor’s log book maintained at the reception. This log shall be reviewed periodically by the Admin for its consistency.
   3. Every visitor shall be given a Visitor's ID card and the visitor shall wear the same till he is present in the premises.
   4. The Training team shall provide discussion / meeting rooms outside operational areas. The staff shall hold discussions or meetings only in these rooms.
   5. In case the visitor needs to enter the restricted areas, receptionist shall contact person to whom the visitor wants to meet. Based on approval, the visitor shall be allowed and he/she shall be escorted personally by the person whom he visits or by security guard and they shall be escorted back to the reception area after the meeting is complete. A register shall be maintained by receptionist on details of visitors entered in the restricted area.
   6. While the visitor enters operational area, the receptionist shall insist that the visitor leaves behind his belongings (like laptops, CDs, USB Drives, Camera phones, bags etc.) at the storage facility available a t the proctor.
   7. If the purpose of visit is dependent on laptops or other gadgets, the visitor shall declare all gadgets carried by him and the purpose of carrying them in the visitors' log book. The receptionist or the security shall verify the same physically. Confirmation to carry such items shall be confirmed by receptionist with HR.
   8. The above process will be followed in case canteen staff enters in the restricted areas.

## E­mail Policy (HIPAA)

Statement of Policy

E­Mail is provided to all staff primarily for work related purposes and in order to carry out effective and faster communication, both internal and external to the organization.

Target Audience

The Audience of this policy is all staff and users of the organization's E­mail Facility.

Scope

The scope of this document includes all users accessing the E­mail via systems (both internal and external) controlled by Organization's AIG HIPAA Team.

Responsibilities

1. Users of Email Systems Responsible for:
   1. Ensuring appropriateness of email content.
   2. Using email in accordance with this and the E­mail Usage Guidelines.
   3. Ensure body of the e­mail does not contain PHI data.
   4. Ensue PHI data are in the attached file with password protected
   5. Ensure email signature must have Disclaimer info

1. AIG HIPAA Team Staff Responsible for:
   1. Creating E­mail Id's as per the organization's new user creation standards.
   2. Providing email content filtering to block sensitive information, offensive text and unauthorized attachments.
   3. Monitoring the E­mail traffic and the logs generated by content filtering tools.
   4. Reporting incidents of blocked content to Management/IT Manager

Procedure

* Communicate via e­mail as attachment with Password Protected
* Email must be encrypted before sending.
* Email must not be used for generation of unsolicited commercial email or SPAM. Internal generation or origination of such content will result in disciplinary action and may result in dismissal and/or legal action.
* Email is provided for the primary purpose of conducting the business of the organization.
* The management of the organization doesn't promise privacy of e­mails to its users as it may be required to access the mails/contents of mails by the AIG HIPAA Team during
  1. Backing up emails

○ Archiving mails

○ Troubleshooting e­mail related problems

○ Retrieval of old or archived mails and

○ Periodical maintenance of mail server

○ Legal requirements

* All incoming and outgoing messages must be scanned at the email gateway and ensured to be clear of all known viruses and malicious code. Messages containing viruses or malicious code must be quarantined
* Desktops must also include email anti­virus filtering. Such filtering must use a different anti­virus product (If possible) to the gateway control.
* Attachments
  1. Attachment should be password protected as it contains PHI

○ Messages containing attachment must not be sent to more than ten (10) recipients.

1.1.1. Disclaimer

All the mails sent out of the organization's network shall be attached with the disclaimer note as under:

“Information contained and transmitted by this e­mail is confidential and proprietary to AIG Business Solution and its affiliates and is intended for use only by the recipient. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e­mail is strictly prohibited and you are requested to delete this e­mail immediately and notify the originator. AIG Business Solution does not enter into any agreement with any party by e­mail. Any views expressed by an individual do not necessarily reflect the view of AIG Business Solution. AIG Business Solution is not responsible for the consequences of any actions taken on the basis of information provided, through this email.”

# 

## Internet Policy

Statement of Policy

Use of Internet Access is provided to staffs primarily for work related purposes. Special consideration must be made to confidentiality of the organization's information when using the Internet.

The Internet usage shall strictly adhere to the Internet Usage Guidelines and any violations may even lead to disciplinary actions by the management.

Target Audience

The Audience of this policy is all staff and users of the organization's Internet Facility.

Scope

The scope of this document includes all users accessing the internet via systems controlled by the organization's AIG HIPAA Team.

Specifically, out of scope for this policy is the method in which systems may be connected to the Internet. This can be found in the External Links Policy document.

Responsibilities

1. Users of Internet Access

Responsible for:

Using discretion in which Internet sites are accessed by the user.

1. AIG HIPAA Team

Responsible for:

* 1. Pro Providing Internet content filtering in accordance with this policy
  2. Reporting incidents of blocked content to Compliance Team / Management

Procedure

1. Internet Use Policy Standard
   1. There are three types access given to employees of the organization.
      1. L1 Group

Directors and IT belonging to this group having full access to all the sites.

* + 1. L2 Group

Employees (HR, Accounts, Admin, Recruitment) belonging to this group having restricted access of site (including pornographic, social media, and Medical Billing Apps.)

* + 1. L3 Group

Employees belong to this group having all site access except restricted access (like mail, pornographic, Job portal, Multimedia, Social Media etc.) Access to this group shall be given to Managers and below.

* + 1. L4 Group

Employees belong to this group having access to those websites which is essential for Business Requirement.

Access to this group shall be given based on approvals from Business Heads/ Senior Managers. This access shall be given based on business requirements.

* 1. Content Filtering
     1. Internet traffic into organization's networks and systems must be subjected to content filtering.
     2. Content that must be blocked includes:

Certain sites shall not be blocked for specific operations.

* + 1. Where access to a site or contents is blocked, HIPAA Compliance team must be informed.
  1. Personal Use

Internet Access is provided for the primary purpose of conducting the business of the organization.

* 1. Content Filtering server

All Internet access to organization's networks and systems must be provided via an authenticated, content filtering server.

* 1. Anti­virus protection

All Internet content must be scanned at the Content Filtering server and ensured to be clear of all known viruses and malicious code.

* 1. Technology Support Services (AIG HIPAA Team) Staff

**AIG HIPAA Team staff may download Executable content via the Internet if it is required for their general duties. Such content must be independently scanned for malicious content by an anti­virus package other than the package being used on the proxy/content filtering server.**

### Document Control

This is a controlled document by QA. Any additions and deletions will be reviewed by HIPAA Compliance Team before incorporate.

Based on this HIPAA Security Policies and Procedures, next level documents like Operating Procedures for Operations, HR, Physical Security, IT, Utilities, Training & Engineering have been prepared separately. Revision statuses for these documents are maintained separately.

Current version of HIPAA Security Policies and Procedures, related Operating Procedures and formats are placed in the path \\fileserver\AIG Policies PDF files.

Revisions status of this HIPAA Policy manual ­

|  |  |  |
| --- | --- | --- |
| Name | Version | Release Date |
| AIG Security Policies and Procedure | 1 | 01­01­2016 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | L1 | L2 | L3 | L4 |
|  | Member | Director, IT | HR,Accounts,A dmin, Recruitment | Sr. Manager, Manager | Billing user,  TL, QA |
| General Rights | Printing | Y | Y | N | N |
| USB/CD | Y | Y | N | N |
| Software (Modify) | Y | N | N | N |
| Print Screen | Y | Y | Y | N |
| Shared Drive (Full/Limited) | Y | Limited | Limited | Limited |
| Admin Password | Y | N | N | N |
| Applicatio  n /  Software Rights | Chrome | Y | Y | Y | Y |
| Softphone | Y | N | Y | Y |
| MS Office | Y | Y | Y | Y |
| PDF | Y | Y | Y | Y |
| Skype | Y | Y | Y | N |
| Local Messanger | Y | Y | Y | Y |
| Team Viewer | Y | Y | Y | N |
| Prime Clinical | Y | N | Y | Y |
| URL  Rights | Sharepoint | Y | N | Y | Y |
| Laserfiche | Y | N | Y | Y |
| eBridge | Y | N | Y | Y |
| eFax | Y | Y | Y | Y |
| Exenta | Y | Y | Y | Y |
| Healthcare | Y | Y | Y | Y |
| Social Media | Y | Y | N | N |
| AIG Local Email | Y | Y | Y | Y |
| Gmail | Y | Y | Y | N |
| Other Email | Y | Y | N | N |
| Online Banking | Y | Y | N | N |
| Prohance | Y | N | N | N |
| Education | Y | Y | Y | N |
| eCommerce/Shopping | Y | N | N | N |
| Naukri / Job portal | Y | Y | N | N |
| Informatics | Y | Y | Y | Y |
|  | Youtube / Multimedia | Y | Y | N | N |
| News | Y | Y | N | N |
| Security | CCTV Access | Y | Admin | N | N |
| Biometric Report Access | Y | HR, Admin | N | N |

## Glossary

The terms and definitions used in this resource document have been obtained from congressional legislation, executive orders, and commonly accepted glossaries of security terminology, including that of the National Institute of Standards and Technology (NIST) Special Publication 800-53: *Recommended Security Controls for Federal Information Systems*.

|  |  |
| --- | --- |
| **Administrative Safeguards** | Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity’s workforce in relation to protecting the information. |
| **Addressable** | As applied to an implementation specification of the Health Insurance Portability  Accountability Act of 1996 (HIPAA), describing a measure that is mandatory for all HIPAA-covered entities unless the entity concludes the measure is not “reasonable and appropriate” after conducting a required analysis. The covered entity may still be required to implement an equivalent measure if the equivalent measure is “reasonable and appropriate” and achieves the same end as the addressable implementation specification. |
| **Affiliated Covered Entities** | Legally, separated covered entities that are under common ownership or control that have all designated themselves as single affiliated covered entities for the purposes of the Privacy and Security Rule (more precisely, those parts of the Rules appearing at 45 C.F.R., Part 160, Subparts C and E). |
| **Availability** | The property that data or information is accessible and usable on demand by an authorized person.  Ensuring timely and reliable access and use of information. (NDIS SB 800-53) |
| **Authorized User** | Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the AIG Business Solution (P) Ltd. These resources are extended to accomplish tasks related to the individual’s status with AIG Business Solution (P) Ltd. or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the AIG Business Solution (P) Ltd. or and AIG Business Solution (P) Ltd. institution. For the purpose of this policy, no attempt is made to differentiate among users by the user’s group. These policies treat all users similarly, whether student, faculty, staff or other authorized user in terms of expectations of the user’s conduct. |
| **Business Associate** | An entity dependent of a HIPAA-covered entity that handles individually identifiable health information received from or provided to the covered entity. For examples of the kinds of activities conducted by business associates, as well as certain exceptions to the definition, see Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82798. |

|  |  |
| --- | --- |
| **Computer Security Contingency** | An event with the potential to disrupt computer operations, thereby, disrupting critical mission and business functions. Examples include a power outage, hardware failure, fire. Flood, or storm. If the event is very destructive, it is often called a disaster. |
| **Confidentiality** | The property that data or information is not made available or disclosed to unauthorized persons or processes.  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST SB800-53) |
| **Contingency** | See **Computer Security Contingency.** |
| **Controls** | See **Security Controls**. |
| **Countermeasures** | Synonymous with security controls and safeguards.  Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. |
| **Covered Entities** | Entities that must comply with any or all of the HIPAA Rules in this document, including certain providers, health plans, and health care clearinghouses that are regulated by the HIPAA Security Rule and/or the HIPA Privacy Rule. |
| **Electronic Protected Health**  **Information (EPHI)** | Individually identifiable health information (IIHI) that is transmitted or maintained electronically. EPHI excluded information transmitted or maintained in media that are not electronic. Some other categories of information include “IIHI” are excluded by EPHI such as some education and employment records. |
| **Final Rule** | The version of the specific requirements for compliance with a statute published by the agency empowered to do so by the relevant statute. Final Rules are published after a public comment period and are usually redrafted to account for issues identified by these public comments. The Final Security and Privacy Rules set compliance deadlines, after which they are effective and enforceable. |
| **Health Care Clearinghouse** | A public or private entity that processes or facilitates the processing of health information received from another entity to or from a standard format. |
| **Health Care Provider** | A provider of medical or health services and any other person who furnishes, bills, or is paid for health care in the normal course of business. |
| **Health Information** | Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and relates to the past, present or future physical or mental health or condition of an individual; the provision or health care to an individual; or the past, present or future payment of the provision of health care to an individual. |
| **Health Plan** | An individual or group plan that provides or pays the cost of medical care. |
| **Hybrid Entity** | A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that has designated one or more of it components as health care components in accordance with 45 C.F.R. section. |
| **Impact** | See **Potential Impact**. |
| **Implementation Specification** | Specification requirements or instructions for implementing a standard. |
| **Incident** | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information system process, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (NIST SB 800-53) |
| **Individually Identifiable Health**  **Information (IIHI)** | Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse, and related to the past, present, or future physical or mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. |
| **Information Security** | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, integrity, and availability. |
| **Information System** | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| **Information Technology** | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchanges, transmission, or reception of data or information. |
| **Integrity** | The property that data or information has not been altered or destroyed in an unauthorized manner.  Guarding against improper information mortification or destruction, and includes ensuring information non-repudiation and authenticity. (NISC SB 800-53) |
| **Management Controls** | The security controls (i.e., safeguards and countermeasures) for an information system that focuses on the management of risk and the management of the information security system. Actions that are performed primarily to support management decisions with regard to information system security. |
| **Measures** | See **Security Controls** |
| **Mitigate** | See **Risk Mitigation** |
| **Operational Controls** | The security controls (i.e., safeguards and countermeasures) for an information system that are primarily implemented and executed by people (as opposed to the information system). |
| **Potential Impact** | The loss of confidentiality, integrity, or availability of a breach could be expected to have, such as: 1) a limited adverse effect; 2) a serious adverse effect; or 3) a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (NIST SB 800-53) |
| **Physical Safeguards** | Physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural environmental hazards, and unauthorized instruction. |
| **Proposed Rule** | Proposed requirements for compliance with a statute that is published for public comment by the agency empowered to do so by the relevant statute. Proposed rules are not binding (i.e., complying with a proposed rule). |
| **Protected Health Information** | Individually identifiable health information that is transmitted or maintained electronically or by using any other medium. Some categories of information included in the “IIHI” are not considered to EPHI, such as some educational and employment records. |
| **Required** | Mandatory—as applied to HIPA implementation specifications—for all covered entities to comply with HIPAA Rules. |

## Abbreviation

|  |  |
| --- | --- |
| **CFR** | Code of Federal Regulation |
| **CIO** | Chief Information Officer |
| **CMMS** | Centers for Medicare and Medicaid Services |
| **CSD** | Computer Security Division |
| **PHI** | Protected Health Information |
| **EPHI** | Electronic Protected Health Information |
| **HHS** | Department of Health and Human Services |
| **ID** | Identification |
| **IIHI** | Individually Identifiable Health Information |
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **NIST** | National Institute of Standards and Technology |
| **SIRT** | Security Incident Response Team |
| **SP** | Special Publication |
| **USC** | United States Code |

This appendix lists acronyms used within this document.

Because of the length of the HIPAA Security Rule, go to the following website for complete information:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html>

Date

1. Adapted from 68 Federal Register 8380, February 20, 2003 (Appendix A to Subpart C or Part 164—Security Standards: Matrix [↑](#footnote-ref-1)
2. Sunny Rathore, IT Security Officer has been appointed for the HIPAA Privacy and Security Rules [↑](#footnote-ref-2)
3. The definition of a workstation is an electronic computing device, i.e., desktop, laptop, or other device that performs similar functions, including the electronic media in its immediate environment. This latter statement extends the definition of workstation to a wider range of computer input and output devices - unintelligence and intelligent computer terminals, personal digital assistants, other wireless devices, diagnostic equipment, etc. [↑](#footnote-ref-3)