HIPAA Security Policies and Procedures

# Purpose

The purpose of this policy is to establish a Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Program.

The program defines and implements the security regulations (the “Security Rule”), as amended by the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, (“HITECH Act”) which require covered entities and business associates to protect the confidentiality, integrity and availability of ePHI.

#{company} is a business associate under HIPAA and, as such, is required to comply with the Security Rule.

# Scope

This policy applies to all people, processes and technologies that access, store and process PHI.

# Ownership

#{owner} is responsible for implementing and maintaining this policy. The #{owner} is responsible for facilitating HIPAA security training and oversight of its workforce members; facilitating investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA Security Rule; and implementing and maintaining all policies, procedures, and documentation related to #{company}’ HIPAA security compliance.

# Policy Statement

In accordance with the standards set forth in the HIPAA Security Rule, #{company} is committed to protecting the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, and/or transmits.

The HIPAA Security Policies and Procedures apply to workforce members (which includes employees, trainees, students, volunteers, etc.) as well as subcontractors and outside affiliates.

Failure to comply with the HIPAA Security Policies and Procedures or the HIPAA Privacy Policies and Procedures by workforce members may result in disciplinary action. In the case of a violation by subcontractors or outside affiliates, such violation may result in the termination of the subcontractor agreement or affiliation.

#{company} as a Business Associate or Subcontractor

#{company} may act as a Business Associate of a Covered Entity or Covered Entities and/or as a Subcontractor of a Business Associate or Business Associates. When #{company} is acting as a Subcontractor, references herein to “Business Associate” should be read as “Subcontractor,” and references to “Covered Entity” should be read as “Business Associate,” as appropriate and applicable.

Definition

“**ePHI**” means a subset of protected health information or PHI that is created, maintained, transmitted, or received by #{company} in electronic media and relates to: (1) the past, present, or future physical or mental health or condition of an individual; (2) the provision of health care to an individual; or (3) the past, present, or future payment for the provision of health care to an individual. Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

“**PHI**” stands for Protected Health Information and is any information that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

“**HIPAA**” stands for Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.

“**HITECH**” stands for Health Information Technology for Economic and Clinical Health Act (HITECH) and was signed into law on February 17, 2009 and addresses the privacy and security concerns associated with the ePHI.

“**Workforce members**” include employees, managers, senior executives, and as appropriate contractors.

“**Risk**”: The probability that the confidentiality, availability, and integrity of PHI, other confidential or proprietary electronic information, and other system assets will be affected by a threat or vulnerability.

#### General Rules:

Maintenance: §164.306

To ensure a reasonable and appropriate level of protection of ePHI, #{company} will review, modify and update (as needed) the security measures #{company} has implemented pursuant to the Security Rule on a regular basis to ensure compliance with current Security Rule requirements and operational standards.

The #{owner} shall periodically meet or correspond with the appropriate department or teams, as well as other appropriate persons, as necessary to ensure that the implemented safeguards are sufficient to protect the ePHI maintained by #{company} and to comply with regulatory requirements.

If security measures need to be modified or updated, the #{owner} shall work with the appropriate persons to ensure that the security measure is addressed and documented.

#### Administrative Safeguards:

Security Management Process: §164.308(a)(1)

Risk Analysis: §164.308(a)(1)(ii)(A)

Risk Management: §164.308(a)(1)(ii)(B)

*To use in conjunction with the Risk Management policy*

#{company} has assessed the potential risks to the confidentiality, integrity and availability of ePHI held by #{company} . #{company} will employ ongoing information security measures and management processes for all systems containing ePHI to prevent, detect, contain, and correct security violations in accordance with and pursuant to the #{company} Information Security Policies and Procedures. #{company}implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

* Ensure the confidentiality, integrity, and availability of all PHI the organization creates, receives, maintains, and/or transmits.
* Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
* Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required.
* Ensure compliance by the workforce.

#{company} conducts thorough analysis of all ePHI created, received, maintained and transmitted on or by its networks and systems on a periodic technical and non technical evaluation, ongoing basis to document the threats and vulnerabilities to stored and transmitted information. The risk analysis is conducted at least annually and takes into account the following factors:

* The size, complexity, and capabilities of the covered entity or business associate.
* The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
* The costs of security measures.
* The probability and criticality of potential risks to electronic protected health information.
* The relative criticality of specific application and data in support of other contingency plan components.

The risk management program consists of regularly performed risk assessments, which identify and prioritize security and compliance gaps, and recommend additional security controls needed to mitigate the risk carried by the gaps for all systems containing ePHI to prevent, detect, contain, and correct security violations. The Risk Management process is based on the following steps:

* Risk Prioritization - Using information from the risk analysis, risks will be ranked on a scale based on the potential impact to information systems containing ePHI and the probability of occurrence.
* Control selection – Mitigating controls shall be selected that are the most appropriate security methods to mitigate or manage identified risks to critical information systems and ePHI.  Such selections will be based on the nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards.
* Assign risk ownership – Appropriate Workforce members will be identified and assigned responsibility for implementing and managing selected safeguards.
* Security method evaluation - Selected security safeguards will be regularly evaluated and revised as necessary.
* The results of each of the above steps will be formally documented and retained for 6 six years.

All documentation of risk management efforts, including decisions made on controls to implement as well as those to not implement, are documented and maintained for six years.

#### Administrative Safeguards:

Sanction Policy: §164.308(a)(1)(ii)(C)

#### Technical Safeguards:

Integrity and Mechanism to Authenticate Controls: §164.312 (1 and 2)

It is #{company} policy to train all members of its workforce on its HIPAA Security Policies and Procedures. Workforce members who violate the HIPAA Security Policies and Procedures may be subject to appropriate discipline, as determined by the #{owner}.

Violations include but are not limited to:

* Unintentional breach of privacy or security that may be caused by lack of knowledge, lack of judgment, or human error such as accessing information that you do not need to know to do your job, copying PHI without authorization
* Unintentional breach of privacy or security that may be caused by carelessness, such as leaving your computer unattended while logged into a sensitive system, discussing confidential information with an unauthorized person
* Failure to follow policies and procedures
* Deliberate or purposeful violation for personal gain such as making unauthorized changes to confidential data

In the event, that you as an employee of #{company} are responsible for a Violation of the HIPAA security policies, the following sanction guidelines would apply:

* Verbal reprimand
* Written reprimand kept in employee’s file
* Retraining on Privacy and/or HIPAA Awareness training
* Suspension of employee
* Termination of employment

#### Administrative Safeguards:

Information System Activity Review: §164.308(a)(1)(ii)(D)

Security Incident Procedures: §164.308(a)(6)(i and ii)

Evaluation: §164.308(a)(8)

#### Technical Safeguards:

Audit Controls: §164.312

*To use in conjunction with the Security Incident Response Plan Policy*

#{company} will review records of system activities to determine whether ePHI and the systems that maintain ePHI are properly safeguarded.

#{company} reserves the right to review and audit information on #{company}’ information systems at any time. #{company} information systems are provided for business purposes only, and all information stored or sent through such information systems is the property of #{company}. #{company} review information system activity for systems containing ePHI to identify possible operational or security concerns.

#{owner} oversees the identification, investigation, and response to suspected and known security concerns. The security incident response plan guide employees in the security incident response process that includes:

* Identification of what specific event would be considered a security concern and/or incident
* Identification of workforce members’ role and responsibilities regarding security incidents
* Management involvement regarding security incidents
* Workforce members or roles to which the incident response policies and procedures are to be disseminated
* Coordination of security concerns and/or incidents among business associates
* Identifies what steps should be taken in response to a security incident
* The frequency to review and update current security incident policies and procedures

Security Incidents that result in a “breach of PHI” will be handled in accordance with the Breach Notification Policy and Procedure.

#{company}.’s procedures for handling security incidents are documented in its Security Incident Management Policy. The purpose of this policy is to establish requirements and plans for reporting and responding to security incidents impacting #{company}.’s corporate or customer systems.

#### Administrative Safeguards:

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

Job Description and Responsibilities: §164.308(a)(3)

*To use in conjunction with the Information Security Policy*

The #{owner} is responsible for overseeing all ongoing activities related to the development, implementation, maintenance of, and adherence to #{company} policies and procedures related to the security of ePHI, in compliance with federal and state laws and #{company}’ Security Rule Policies and Procedures. The #{owner} will work with individuals involved with #{company}’ information technology (“**IT**”) to maintain appropriate security measures.

In addition to the above responsibilities, the #{owner} is responsible for implementing the following in respect to HIPAA:

* serving as a liaison to individuals involved with IT with regard to maintaining the confidentiality, integrity, and availability of ePHI
* implementing and maintaining all policies, procedures, and documentation related to HIPAA security compliance
* monitoring compliance with HIPAA Security Policies and Procedures
* facilitating HIPAA security training and oversight of its workforce members development on HIPAA security policies and procedures
* implementing separation of duties to address the potential abuse of authorized privileges by ensuring that each job description include clear roles and responsibilities
* performing periodic security risk assessment
* performing ongoing performance of technical and non technical evaluations
* assisting with security audits.
* oversee the security incident process through the identification, investigation, and response to suspected and known Security Incidents
* maintaining current knowledge of applicable federal and state laws relating to the security of ePHI.
* cooperating with OCR and other oversight agencies.
* acting as a point of contact in the event of a reported security violation.
* managing complaints relating to security of ePHI.
* oversee the sanctions policy and its implementation
* facilitating investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA Security Rule
* coordinating with Privacy Officer and/or legal counsel, as applicable, to manage Business Associate contracts and respond appropriately if problems arise.
* maintaining documentation required by the Security Rule; including maintaining policies and procedures in compliance records management requirements, or for six (6) years from creation, or the last “effective date”, whichever date is later.

#### Administrative Safeguards:

Workforce Security: §164.308(a)(3)(i)

Authorization and/or Supervision: §164.308(a)(3)(ii)(A)

Workforce Clearance Procedures: §164.308(a)(3)(ii)(B)

Termination Procedures: §164.308(a)(3)(ii)(C)

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

Access Authorization: §164.308(a)(4)(ii)(B)

Wireless Access Authorization: §164.308(a)(4)

Access Establishment and Modification: §164.308(a)(4)(ii)(C)

Facility Access Controls: §164.310(a)

Maintenance Records: §164.310(A)(2)(iv)

Log-in Monitoring: §164.308(a)(5)(ii)(C)

#### Technical Safeguards:

Access Control: §164.312(a)(1) and §164.312(a)(2)(i)-(iii)

Person or Entity Authentication: §164.312(d)

*To use in conjunction with the Access Control Policy and Physical Security Policy*

#{company} will ensure that workforce members have appropriate access to ePHI and will limit workforce members who do not require access to ePHI for their job responsibilities from obtaining access to ePHI. #{company} grants access to ePHI on a “need to know” basis. Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI must be provided with a unique username and password. #{company} will verify and authenticate that a person or entity seeking access to ePHI is the person or entity claimed by using a unique identifier for each user, along with a corresponding password.

 The access controls include, but are not limited to the following:

* #{owner} will assign appropriate levels of security access to different workforce members based on their job responsibilities according to the access control policy
* Only those workforce members with a need for access to ePHI will be granted such access. Any requests for ePHI access modifications will be submitted to the appropriate team.
* #{owner} will monitor access levels and make adjustments as appropriate, including but not limited to when a workforce member’s job responsibilities change.
* Authentication is required for all systems that maintain or access ePHI and actions performed on the system with their user ID will be monitored
* Password policies are documented and enforced
* BYOD usage is monitored
* When a workforce member’s employment or other arrangement ends, or access to ePHI is no longer appropriate, [company] will promptly terminate that workforce member’s access to ePHI.
* Appropriate measures will be implemented to protect the security of ePHI housed in a facility and #{owner} will limit physical access to its electronic information systems and the facility in which they are housed.
* #{owner} will review audit logs of access to all systems containing ePHI regularly that are capable of audit trail, to determine whether access has been appropriate
* #{owner} will periodically review the list of approved users to ensure that the appropriate level of access has been granted to each workforce member and system access to workforce members who have left #{company} have been terminated
* Access to ePHI through the use of portable devices, remote access, or removable media is limited to authorized users based on their roles and responsibilities
* Login timeout are defined and unsuccessful login attempts are monitored and investigated
* Systems are configured to automatically log-off after a defined period of inactivity

#{company}’s full access control practices are documented in its Access Control Policy. The purpose of this policy is to establish the principles and guidelines for controlling access to systems owned by #{company}.

#### Administrative Safeguards:

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

Security Reminders: §164.308(a)(5)(ii)(A)

Protection from Malicious Software: §164.308(a)(5)(ii)(B)

*To use in conjunction with the Information Security Policy*

#{company} will ensure security awareness through a training program for all of its workforce members, including periodic reminders, virus protection, log-in monitoring, and password management. All workforce members are required to complete [Security Awareness and/or HIPAA] Training at onboarding and annually thereafter. In addition, they may be asked to complete further training as dictated by operational or environmental changes.

Changes that might lead to adjustment of the training program include:

* A security incident retrospective determining that additional training is required
* Adoption of new technology by the company
* Material changes in organizational policies
* Material changes in HIPAA security policies
* Change in the entity’s information system

To help ensure compliance with appropriate security standards, #{company} provides workforce members with periodic security updates.

#### Administrative Safeguards:

Protection from Malicious Software: §164.308(a)(5)(ii)(B)

System Use and Security: §164.310(b) and(C)

*To use in conjunction with the Asset Management Policy*

 #{company}will guard against, detect, and report any malicious software activity. #{company} has implemented the following safeguards to secure ePHI in #{company} ’s workstations:

* #{owner} will provide notice to workforce members of any threats related to malicious software
* An anti-malware and anti-spam protection is implemented at information system entry/exit points for the network and on all devices
* Workstations should only be used for authorized business purposes.
* When possible, workstations should be placed in secure areas.
* Users must take actions to prevent unauthorized viewing, such as privacy screens, minimizing sessions, closing laptops, etc.
* All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.
* Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.
* Automated Logoff- users must automatically log off the workstations and systems after [5] minutes of inactivity.
* [company] will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.
* Any portable device that contains PHI must be encrypted.
* A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
* To ensure that Workstations that may be used to send, receive, store or Access ePHI are only used in a secure and legitimate manner, all Workforce members must comply with [company] Acceptable Use policy.

#{company}’s workstation controls policy is documented in the Acceptable Use and Asset Management Policies. The purpose of this policy is to establish workstations controls and provide guidelines for their implementation.

#### Administrative Safeguards:

Contingency Plan: §164.308(a)(7)(i)

Applications and Data Criticality Analysis:§164.308(a)(7)(ii)

Data Back-Up Plan: §164.308(a)(7)(ii)(A)

Disaster Recovery Plan: §164.308(a)(7)(ii)(B)

Emergency Mode Operation Plan: §164.308(a)(7)(ii)(C)

BC/DR Testing and Revision Procedures: §164.308(a)(7)(ii)(D)

*To use in conjunction with the Business Continuity and Backup Policy*

Contingency

#{company} will respond promptly to any emergency or other occurrence that disrupts or damages the systems that contain ePHI to ensure that #{company} has access to ePHI when it is needed. The contingency plan must include:

* A data backup plan
* A disaster recovery plan and/or emergency mode

All ePHI necessary for #{company} ’ day-to-day operations is maintained by information systems owned by or licensed to #{company} and/or its customers or Business Associates. #{company} has prioritized a list of specific applications and data containing ePHI for restoration purposes and in the event that the #{company} s’ information systems become temporarily unavailable, #{company} ’ operations, including the security of ePHI, will be conducted pursuant to #{company} ’ Emergency Mode Operation Plan and Disaster Recovery Plan.

The Emergency Mode Operation Plan and Disaster Recovery Plan is tested at least annually through scenario-based walkthrough to avoid disruption or through live tests.

#{company}’s business continuity plan is documented in the Business Continuity Policy. The purpose of this policy is to establish requirements and plans to recover #{company} operations following a disruption due to causes such as natural disaster, loss of access to premises, pandemic, or malicious activity from external or internal sources.

Backup

All ePHI shall be stored on network servers in order to be automatically backed up by the system. ePHI should not be saved on the local drives of personal computers. If a Business Associate or backup service is used, a written contract is required to ensure that the contractor will safeguard the ePHI in an appropriate manner.

Employees are required and trained to save all files containing ePHI to a network server to ensure the ePHI is backed-up routinely by #{company} network servers.

#{company}‘s backup procedures are documented in its Backup Policy. The purpose of this policy is to institute the necessary controls to mitigate the accidental loss of #{company} data. These controls assume that events such as accidental data corruption, deletion, or destruction will occur, and mitigate the impact of such events by maintaining reliable backup copies from which data can be readily restored.

#### Administrative Safeguards:

Business Associate Contracts: §164.308(b)

#{company} will ensure that all subcontractor Business Associates who create, maintain, access, receive, or transmit ePHI on behalf of #{company} have executed a Business Associate Agreement that complies with the requirements outlined in 45 CFR Part 164 and the HITECH Act.

## Vendor BAA Agreements

*(new control) Business Associate Agreements are signed with vendors that process or are given access to PHI by #{company}.*

#{company} signs Business Associate Agreements (BAA) with all third-party vendors or subcontractors that store, process, transmit or receive ePHI on behalf of #{company} that complies with the requirements outlined in 45 CFR Part 164 and the HITECH Act.

 BAAs are only required when the systems powered by that vendor are classified as Customer Confidential as per the Data Classification Policy. #{company} maintains a combined list of all third-party vendors or subcontractor business associates and notifies Sub-BAs when regulations require amendments to the Business Associate Agreement.

The BAA includes the security and confidentiality commitments made by both parties.

Copies of all signed Business Associate Agreements are maintained for a period of at least six (6) years from the date when last in effect.

The BAA includes the security and confidentiality commitments made by both parties.

#### Physical Safeguards:

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

Disposal: §164.310(d)(2)(i)

Media Re-use: §164.310(d)(2)(ii)

Accountability: §164.310(d)(2)(iii)

Data Backup and Storage: §164.310(d)(2)(iv)

*To use in conjunction with the Data Retention & Disposal and Backup Policy*

#{company} maintains an inventory of all devices and systems containing ePHI. #{owner} is responsible for ensuring that the data backup processes function appropriately according to the backup policy.

#{owner} is responsible for overseeing the movement of all epHI outside of#{company}’s facilities. #{company} will remove ePHI from electronic media before it is available for reuse and to the extent disposal of such information is permitted or required by applicable law, #{company} will properly dispose of the ePHI and, if necessary, the hardware or electronic media on which it is stored.

#### Technical Safeguards:

Transmission Security: §164.312 (1 and 2)

##

*To use in conjunction with the Encryption Policy*

#{company} will guard against unauthorized access to ePHI being transmitted over an electronic communications network by using integrity controls, encryption technology, and other procedures as required under the Security Rule. Encryption will be utilized when:

* Transmitting ePHI to outside entities
* Stored on Portable Devices and Media
* Sent via Email or messaging systems
* Sent over wireless networks

Encryption practices are documented in #{company}’s Encryption Policy. The purpose of this policy is to establish practices for protecting #{company} data in the event of unauthorized access through the use of encryption. The policy describes the different components that can be configured to utilize encryption, the algorithm that must be used for each, and how encryption keys should be managed.

#### Documentation: §164.316(b)(1)

### Creation

#{company}’s management team is responsible for creating policies and supporting any relevant requirements and activities through sufficient staffing and budget allocation. The management team is also responsible for ensuring that #{company}’s staff is trained to understand and remain familiar with all relevant policies, and for keeping policies available for review both internally and externally by customers and partners.

### Reviews

#{owner} is responsible for ensuring all #{company} information security policies are reviewed at least annually by #{company} management, and re-approved or updated as necessary.

Existing policies may be updated and new policies may be created for reasons including:

* Complying with applicable laws and regulations
* Complying with new requirements for certification and governance by the company or its customers
* Addressing new threats
* Technological or business requirements

### Retention

To comply with the Health Insurance Portability and Accountability Act (HIPAA), policies and procedures are retained for six years from the date of its creation to the date when it was last in effect, whichever is later.

Current and previous versions of #{company}’s policies and procedures are stored in its compliance management tool, Kintent and are made available to those persons responsible for implementing the procedures to which the documentation pertains. In addition, these policies are reviewed and updated annually or in response to environmental or operational changes affecting the security of ePHI.

# Related Controls

* Vendor BAA Agreements