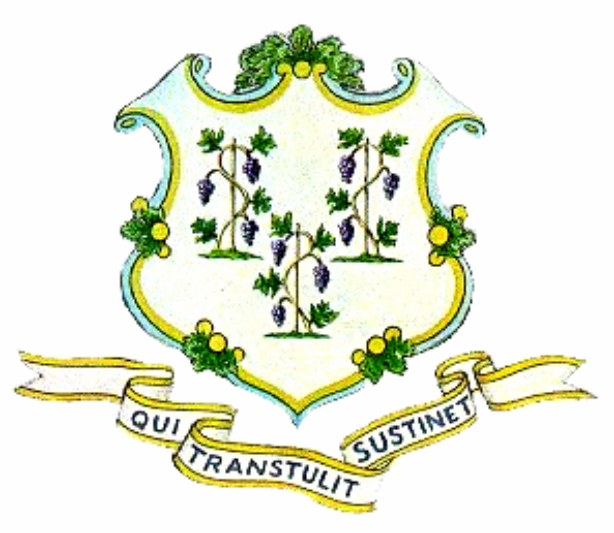
Health Insurance Portability and Accountability Act

State HIPAA Security Policy



State of Connecticut

Release 2.0
November 30th, 2004

Table of Contents

Executive Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities and covered components of hybrid entities to comply with 54 standards and implementation specifications regarding the protection of electronic protected health information (ePHI) and information technology (IT) resources that store, process, access, and/or transmit ePHI. The standards and implementation specifications are defined in the HIPAA regulations, 45 C.F.R. Subpart A of Part 160 and Subparts A and C of Part 164 (HIPAA Security Rule).

The Department of Information Technology (DOIT) is the state agency charged by state statute to develop and administer integrated policies and standards pertaining to information and telecommunication systems for all state agencies. *See* Conn. Gen. Stat. §§ 4d-1, *et seq*. As directed by the State Chief Information Officer (CIO), DOIT has established within it the IT Security Unit (ITSU). The ITSU is responsible for establishing and overseeing information security functions that must exist for all state agencies. These information security functions include developing and administering policies, security audits and assessments, security tools, security operations, security investigations, security awareness, and risk management pertaining to the potential loss or disclosure of IT assets and electronic information.

The ITSU, in collaboration with agencies, developed the State HIPAA Security policies and centralized procedures to be followed by those state agencies that are covered entities for the purpose of compliance with the HIPAA Security Rule. State HIPAA Security policies and centralized procedures will be administered by the ITSU. In addition to centralized procedures, decentralized (agency developed) procedures will be developed as directed by policy. A Business Associate Memorandum of Understanding between DOIT and each covered entity agency will be developed to establish responsibilities.

As of this revision date, the following state agencies have been identified as covered entities or hybrid entities.

1. Department of Administrative Services
2. Department of Children and Family
3. Department of Social Services
4. *Department of Public Health**
5. Department of Metal Retardation
6. Department of Mental Health and Addiction Services
7. *University of Connecticut**
8. University of Connecticut Health Center
9. Department of Veterans Affairs
10. Teachers Retirement Board

**For purposes of this policy the agency has been declared a "hybrid entity" wherein only the agency's covered components are subjected to State HIPAA Security Policies and Procedures.*

<u>Implementation and Enforcement</u>: The agency heads of the above-referenced covered entities, and their designees, along with the ITSU, are responsible for establishing, implementing, and enforcing State HIPAA Security policies and procedures. State HIPAA Security policies and procedures do not preempt any existing or similar laws or policies.

<u>Scope</u>: The State HIPAA policies and procedures apply to all ePHI and IT resources that store, process, have access to, and/or transmit ePHI held by the covered entities and covered components of hybrid entities.

Policy Definitions

For the purposes of the State HIPAA Security Policy and Procedures, the following terms have been defined.

1. Access – The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
2. Access Control – The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use.
3. Access Control Mechanisms – Hardware, software, or firmware features and operating and management procedures in various combinations designed to permit authorized, and detect and prevent unauthorized access to a computer system.
4. Access Rights – Also called "permissions" or "privileges", these are the rights granted to users by the Agency. Access rights determine the actions users have been authorized to perform (e.g., read, write, execute, create and delete).
5. Agency – see covered entity.
6. Agency Security Official – The individual designated by the Agency who is responsible at that Agency for the development and implementation of the policies and procedures required by the HIPAA Security Rule.
7. Application – A computer program or set of programs that processes records for a specific function.
8. Application Controls – These refer to the transactions and data relating to computer-based applications whose purpose is to ensure the completeness and accuracy of records and the validity of the entries in the records. Applications controls may be manual or programmed, and the records and entries may result from both manual and programmed processing. Examples of application controls include, but are not limited to, data input validation, agreement of batch totals and encryption of data transmitted.
9. Audit – A methodological examination and review of an Agency's implementation of HIPAA Security Policies and Procedures.
10. Authentication – The corroboration that a person is the one claimed. Authentication is the act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data.
11. Backup – Exact copies of files and data, and the necessary equipment and procedures available for use in the event of a failure of applications or loss of data, if the originals are destroyed or systems are not functioning.
12. Business Associate – A person or organization that performs, or assists in the performance of a function or activity on behalf of a covered entity, any function or activity involving the use or disclosure of ePHI, or any other function or activity regulated by HIPAA, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services of ePHI.

13. Business Continuity Plan – Also known as contingency plan. A document describing how an organization responds to an event to ensure critical business functions continue without unacceptable delay or change.
14. Business Continuity Planning – Business continuity is the ability to maintain the constant availability of critical systems, applications, and information across the enterprise.
15. Centralized Procedures – Procedures that are developed and administered by the ITSU pertaining to the HIPAA Security Rule and that must be implemented by all Agencies.
16. CIO – State of Connecticut Chief Information Officer and the administrative head of the Department of Information Technology.
17. Covered Entity (CE) – A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. For purposes of these policies and procedures, covered entities include all the state agencies, or covered components of hybrid entities, listed in the Executive Summary.
18. Data Owners – Individuals employed by state agencies, who have been given the responsibility for the integrity, accurate reporting, and use of computerized data.
19. Decentralized Procedures – Procedures that are developed, administered and implemented by the Agencies that are Agency specific.
20. Department of Information Technology (DOIT) – The state agency that is responsible for developing and implementing policies and architecture pertaining to information and telecommunications system for state agencies.
21. Disaster Recovery Plan – A documented plan that provides detailed procedures to facilitate recovery of capabilities at an alternate site.
22. Disaster Recovery Planning – Disaster recovery refers to the immediate and temporary restoration of critical computing and network operations after a natural or man-made disaster within defined timeframes. An organization documents how it will respond to a disaster and resume the critical business functions within a predetermined period of time; minimize the amount of loss; and repair, or replace, the primary facility to resume data processing support.
23. Electronic Protected Health Information (ePHI) – Agency information that is individually identifiable health information that is transmitted by electronic media or maintained in electronic media.
24. Encryption – A technique (algorithmic process) used to transform plain intelligible text by coding the data so it is unintelligible to the reader.
25. Health Care Clearinghouse – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value added" networks and switches, that either processes or facilitates the processing of health information.
26. HIPAA – The Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder.
27. Hybrid Entity – A Hybrid Entity has programs or functions considered to be those of a Covered Entity; however the functions covered by HIPAA are not the agency's primary function or "dominant mission".

28. Information Security – Administrative, physical and technical controls that seek to maintain confidentiality, integrity and availability of information.

29. Information Technology (IT) Resources – IT resources are tools that allow access to electronic technological devices, or are electronic technological devices themselves that service information, access information or is the information itself stored electronically. These resources include all state-supplied computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices such as printers, scanners and cameras; pagers, radios, voice messaging, computer generated facsimile transmissions, copy machines, electronic communication including email and archived messages; electronic and removable media including CD-ROMs, tape, floppy and hard disks; external network access such as the Internet; software, including packaged and internally developed systems and applications; and all information and data stored on State equipment as well as any other equipment or communications that are considered IT resources by DOIT.

30. Information Technology Security Unit (ITSU) – The unit within DOIT under the direction of the CIO that is responsible for overall information security functions for the executive branch of State government. Information security functions include policy administration, security audits and assessments, security tools, security operations, security investigations, security awareness training, and risk management pertaining to the potential loss or unauthorized disclosure of IT resources and electronic information.

31. Logical Access Control – The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data.

32. Malicious Software – Software, for example, a virus, designed to damage or disrupt a system.

33. Password – A protected, generally computer-encrypted string of characters that authenticate an IT resource user to the IT resource.

34. Preventive Controls – Controls designed to prevent or restrict an error, omission or unauthorized intrusion to IT resources.

35. Risk Analysis – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of IT resources.

36. Risk Management – The process of identifying, measuring, controlling and minimizing or eliminating security risks that may negatively affect information systems.

37. Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

38. Unique User Identifier – A unique set of characters assigned to an individual for the purpose of identifying and tracking user identity.

39. Workforce Member (User of an Information Technology Resource) – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

1. HIPAA Administration Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to policies and procedures and documentation requirements and the appointment of a security official.

1.1. Agencies shall adopt and follow the State HIPAA policies and procedures.

1.2. The agency heads and their designees, along with the ITSU, are responsible for establishing, implementing, and enforcing State HIPAA Security policies and procedures. State HIPAA Security policies and procedures do not preempt any existing or similar laws or policies.

1.3. The State HIPAA policies and procedures apply to all ePHI and IT resources that store, process, have access to, and/or transmit ePHI held by the covered entities and covered components of hybrid entities.

1.4. The following policies shall be adopted and enforced as applicable.

1.4.1. HIPAA Administrative Policy

1.4.2. Security Awareness and Training Policy

1.4.3. Acceptable Use and Sanction Policy

1.4.4. Information Technology Access Policy

1.4.5. Information Technology Security Policy

1.4.6. Information Technology Activity Review and Logging Policy

1.4.7. Incident Response and Reporting Policy

1.4.8. Information Technology Resource Management Policy

1.4.9. Facility Security Policy

1.4.10. Business Continuity Planning & IT Disaster Recovery Policy

1.4.11. Risk Management and Audit Policy

1.4.12. Business Associate Contracts Policy

1.4.13. Isolating Health Care Clearinghouse Policy

1.5. Policies and procedures shall be reasonable and appropriate to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, taking into account the size, complexity, and capabilities of the Agency; the Agencies technical infrastructure, hardware, and software capabilities; the costs of security measures; and the probability and criticality of potential risks to ePHI.

1.6. Centralized procedures shall be developed by the ITSU for those procedures that are to be used by all agencies. Agencies shall develop decentralized procedures that must be specific to their state agency to define specific operational steps for policy compliance.

1.7. Guidelines that set forth "best practices" shall be developed by the ITSU for the purpose of assisting Agencies to comply with policies and procedures.

1.8. Policies, procedures, and guidelines shall be documented and stored, by the Agencies and the ITSU, in paper form or electronically.

1.9. HIPAA Security Rule policies and procedures and actions, activities or assessments required by the HIPAA Security Rule, including but not limited to, risk analysis, evaluations, and documentation related to security incidents and their outcomes, shall be maintained for six years from the creation date or the date when it last was in effect, whichever is later.

1.9.1. Documentation shall be made available to anyone responsible for implementing, managing, and auditing the procedures to which the documentation pertains.

1.9.2. Documentation shall be reviewed, updated and modified, as needed, if environmental or operational changes affect the security of ePHI.

1.10. The Agency shall identify a security official who is responsible, in conjunction with the ITSU, for the development and implementation of the policies and procedures required for compliance with the HIPAA Security Rule.

2. Security Awareness and Training Policy

Purpose: The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to implementing security awareness and training programs for the Workforce Members concerning the protection of ePHI and IT resources.

2.1. DOIT shall develop and implement a centralized security awareness and training program for the Agencies. Each Agency shall develop and implement their decentralized procedural content and provide awareness and training thereon.

2.1.1. Security awareness and training shall be conducted for the Agency's Workforce Members.

2.1.2. The Security awareness and training program shall be reasonable and appropriate to carry out the various functions of the workforce and shall include, for all members of the workforce, the following features.

2.1.2.1. Periodic security updates to serve as security reminders.

2.1.2.2. Procedures for monitoring log-in attempts and reporting discrepancies.

2.1.2.3. Procedures for creating, changing, and safeguarding passwords.

2.1.2.4. Procedures for guarding against, detecting, and reporting malicious software.

2.1.3. Training shall be conducted prior to the access and authorization of Workforce Members to ePHI.

2.2. As determined necessary by the ITSU and the Agency, Workforce Members shall receive additional HIPAA Security training and security reminders.

2.3. Centralized procedures for this policy shall be developed and implemented.

3. Acceptable Use and Sanction Policy

Purpose: The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the acceptable use of IT resources and ePHI, and sanctions for violations of the State HIPAA policies and procedures.

3.1. Workforce Members are responsible for the appropriate use and security of ePHI when using any IT resource authorized by the appropriate agency of the State of Connecticut.

3.1.1. Appropriate use includes using authorized IT resources, as assigned, in accordance with duties and responsibilities. Using IT resources in violation of policy, or any negligent or unlawful activity is considered inappropriate use.

3.1.2. Workforce Members shall be given a copy of the State HIPAA Security policies and procedures.

3.1.2.1. All such Workforce Members shall sign a statement of policy acknowledgement and compliance prior to authorization and access to ePHI.

3.1.2.1.1. A decentralized procedure shall be developed and implemented for workforce acknowledgement.

3.1.3. IT resources shall be protected from misuse, including, but not limited to: theft, unauthorized access, fraudulent manipulation and alternation of data, attempts to circumvent security controls, and any activity that could compromise the confidentiality, integrity, or availability of data.

3.1.4. Workforce Members shall not tamper with or disable any security devices, including but not limited to, virus protection software and login account controls.

3.1.5. Workforce Members are prohibited from introducing any unauthorized IT resources into the State's environment. Furthermore, the introduction of any IT resources that could disrupt any operations or compromise security is prohibited. Refer to §8.1.3 for authorizing IT resources.

3.1.6. Any IT resources assigned to or in the possession of a Workforce Member shall be returned to a designated individual at the Agency when it is determined by Agency management that the use of those resources is no longer necessary.

3.2. Workforce Members learning of or reasonably suspecting any violation of a State HIPAA Security policy shall immediately report to their supervisor and the Agency Security Official.

3.2.1. Once the Agency Security Official has received notification of a known or suspected State HIPAA Security policy violation, he or she shall report to the ITSU in accordance with §7, Incident Response and Reporting Policy.

3.2.2. All Workforce Members are to immediately report lost or stolen IT resources to their supervisors and the supervisors shall report to the Agency Security Official.

3.3. Workforce Members shall adhere to all of the State HIPAA Security policies and procedures.

3.3.1. Any Workforce Member who violates any of the State HIPAA policies or underlying procedures may be subject to discipline, up to and including suspension, employment or contract termination, civil and criminal action, and removal from State premises.

3.3.2. The absence of written policies, procedures, standards, or guidelines governing a specific issue does not relieve the Workforce Member from the responsibility for the appropriate use and security of IT resources.

3.3.3. Workforce Member sanctions for policy violations shall be determined by Agency management.

3.3.4. An authorized State of Connecticut official may monitor contents and usage at any time of any IT resources available to Workforce Members. Furthermore, within the scope of HIPAA audit and compliance activities, Workforce Members are afforded no privacy of IT resource use.

4. Information Technology Access Policy

Purpose: The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to authorizing and controlling access to ePHI and IT resources that store, process, have access to, and/or transmit ePHI.

4.1. Workforce clearance and authorization to access ePHI shall be performed for all Workforce Members prior to granting access requests to IT resources.

- 4.1.1. Access rights shall be granted based on business requirements.
- 4.1.2. Access rights shall be properly authorized and documented by the Agency.
- 4.1.3. Access rights shall be periodically audited as required by the ITSU and the Agency.
- 4.1.4. Access rights shall be reevaluated by the Agency when a Workforce Member's access requirements to ePHI change (e.g., job assignment change).
- 4.1.5. Access rights shall not exceed the minimum necessary for a Workforce Member's assigned duties.
- 4.1.6. Decentralized procedures shall be developed and implemented for authorizing Workforce Members and requirements in this subpart.

4.2. Modifications to Workforce Member's access to IT resources shall be properly authorized and processed in accordance with Policy §4.1.

4.3. Security configurations shall be maintained on IT resources to restrict access to ePHI to only those Workforce Members or software programs that have been granted access in accordance with Policy §4.1.

4.4. Workforce Members shall be assigned unique user identifiers (or login names) for the purposes of authenticating to IT resources.

- 4.4.1. Workforce Members shall not share assigned unique system identifiers (or login names) with any other person, unless for authorized support purposes.
- 4.4.2. Anonymous access, including the use of guest and public accounts, to any IT resource is prohibited.
- 4.4.3. Unique user identifiers (or login names) shall be used with a password for authentication to an IT resource.
  - 4.4.3.1. Passwords shall not be shared with any other person.
  - 4.4.3.2. The Agency shall establish authorization and Workforce Member verification controls for creating and modifying passwords.

4.4.3.3. Passwords shall be encrypted for storage and transmission whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.4.3.4. Passwords shall minimally contain six characters.

4.4.3.4.1. Password controls shall force a minimum six character password length whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.4.3.5. Passwords shall contain both alpha and numerical characters.

4.4.3.5.1. Password controls shall force the creation of strong passwords, which shall include the use of both alpha and numerical characters, whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.4.3.6. Passwords shall be changed every sixty days.

4.4.3.6.1. Password controls shall force periodic password changes every sixty days whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.4.3.7. Passwords shall not be reused for at least five cycles.

4.4.3.7.1. Password controls shall restrict the reuse of passwords for five cycles whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.4.3.8. Password controls shall lockout login accounts after three unsuccessful login attempts whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

4.5. Workforce Member access to IT resources shall be terminated when access is no longer necessary or when determined by management (including when the business relationship between the Workforce Member and agency is terminated).

4.5.1. The Workforce Member's direct supervisor shall be responsible for making appropriate and timely requests for IT resource account deactivation.

4.5.2. A formal termination process shall be used and shall include documentation and verification.

4.5.3. A decentralized procedure shall be developed and implemented for terminating Workforce Member access.

5. Information Technology Security Policy

Purpose: The purpose of this policy is to comply with the Security Rule's requirements pertaining to using mechanisms and controls to protect ePHI by securing IT resources that store, process, have access to, and/or transmit ePHI.

5.1. ePHI shall be protected by authentication controls on all IT resources.

5.1.1. Authentication controls shall minimally include a unique user logon and password combination that support the requirements in §4.3 and §4.4.

5.1.2. Additional authentication controls shall be added to IT resources whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

5.2. ePHI shall be encrypted while stored on IT resources whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

5.3. ePHI shall be encrypted while in transit across an open communications network.

5.3.1. Mail messages containing ePHI shall be encrypted and transmitted using the approved secure messaging product(s) determined by the ITSU.

5.3.1.1. A centralized procedure shall be developed and implemented for transmitting secure electronic messages.

5.3.2. Files containing ePHI shall be encrypted and transmitted using the approved secure file transfer product(s) determined by the ITSU.

5.3.2.1. A centralized procedure shall be developed and implemented for transmitting secure files.

5.3.3. All other ePHI transmissions, e.g. client/server connections, shall be encrypted using approved mechanisms, e.g. virtual private networks, whenever available and feasible, or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

5.4. ePHI integrity shall be sustained using approved mechanisms, e.g. hashing algorithms, electronic signatures and digital signatures, whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

5.5. IT resources shall be secured using physical safeguards for protection from unauthorized access.

5.5.1. Screen locks, e.g., session timeouts, auto logoff, with password controls shall be activated on IT resources, e.g. laptops, desktops, consoles.

5.5.2. Portable IT resources, e.g. laptops, shall be physically secured when not in use.

5.5.2.1. A decentralized procedure shall be developed and implemented for securing portable IT resources.

5.5.3. Virus protection shall be installed and activated on all IT resources where available. Additional mechanisms shall be implemented to further protect IT resources from malicious software whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

6. Information Technology Activity Review and Logging Policy

Purpose: The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to performing audits and logging functions for ePHI and IT resources that store, process, have access to, and/or transmit ePHI.

6.1. IT resources that store, access, or transmit ePHI shall electronically log activity into created log files.

6.1.1. Logging shall include system, application, database, and file activity whenever available or deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

6.1.2. Logging shall include creation, access, modification and deletion activity.

6.1.3. Log files shall be retained electronically for a period no less than 12 months.

6.1.4. Decentralized procedures shall be developed and implemented for logging activity.

6.2. IT resources and log files (defined in §6.1) shall be periodically examined for access control discrepancies, breaches, and policy violations.

6.2.1. System activity review cycles shall include review of audit logs, access reports, and security incident tracking reports, shall not exceed 30 days, and shall include daily exception reporting.

6.2.2. Decentralized procedures shall be developed and implemented for reviewing activity logs.

7. Incident Response & Reporting Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to the identification, response, mitigation and documentation of suspected or known security incidents involving ePHI and IT resources that store, process, have access to, and/or transmit ePHI.

7.1. Designated individuals shall be responsible for monitoring IT resources to identify suspected or known security incidents.

7.2. Workforce Members having knowledge of any suspected or known security incidents shall report this information to their supervisors and the supervisors shall notify the Agency Security Official. The Agency Security Official shall then immediately report to the ITSU.

7.3. Once the Agency has reported the incident or suspected incident to the ITSU, the ITSU shall immediately execute its incident response procedures.

7.4. Harmful effects of security incidents that are known to the Agency and/or ITSU shall be mitigated, to the extent practicable, by the ITSU, Agency, and any other designated agents, where appropriate.

7.5. Suspected and confirmed security incidents and their outcomes shall be documented.

7.6. Centralized incident response and reporting procedures shall be developed and implemented.

8. Information Technology Resource Management Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

8.1. There shall be a record of the movements of IT resources containing ePHI and the designated individual(s) responsible.

8.1.1. The movement of IT resources shall be authorized and logged by the Agency prior to the IT resources entering or leaving a facility.

8.1.2. The Agency shall be accountable for IT resources while in transit between facilities.

8.1.3. IT resources shall be authorized for use and access within a facility by the Agency.

8.1.4. The location of IT resources within a facility shall be documented, and internal movement of IT resources shall be tracked and logged.

8.2. IT resources containing ePHI shall be properly logged and disposed of when no longer used.

8.3. ePHI shall be removed from IT resources and electronic media before they are made available for reuse.

8.4. A retrievable, exact copy of ePHI, when needed, shall be created before any movement of IT resources.

8.5. Decentralized procedures for this policy shall be developed and implemented.

9. Facility Security Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to limiting physical access to a facility's ePHI and the facility or facilities in which they are housed, while ensuring that authorized access is allowed.

9.1. Facilities storing ePHI and IT resources shall maintain a facility security plan.

9.1.1. The facility security plan shall be implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. As appropriate, the facility security plan shall comply with all standards developed by the State of Connecticut Department of Public Works, as set forth in Chapter 60a, sections 4b-130 to 4b-136, inclusive and sections 4b-1 and 4b-52 of the Connecticut General Statutes.

9.2. Facility management shall control and validate a person's access to facilities based on his or here role or function, including visitor control, and there shall be control of access to software programs for testing and revision.

9.2.1. Workforce Members shall be authorized for entry by facility management.

9.2.1.1. Entry records shall be maintained by facility management.

9.2.1.2. Entry records shall include the Workforce Member's job function.

9.2.2. Visitors to the facility shall be authorized for entry by an authorized Workforce Member or other authorized personnel.

9.2.2.1. Visitors shall sign in with facility management, accompanied by an authorized signature from facility management or their designee.

9.2.2.2. Facility management shall provide visitors with a name ID tag at the time of arrival and visitors shall display a name ID tag at all times while in the facility.

9.3. Facility management shall maintain exterior and interior access controls.

9.3.1. Access controls may include a combination of physical locks, electronic ID badges, and cipher locks.

9.3.2. Facility management shall implement additional exterior and interior access controls whenever deemed necessary by the risk analysis or evaluation in accordance with §11, Risk Management and Audit Policy.

9.4. Facility modifications to physical security shall be authorized and recorded by facility management, in consultation with the Agency and ITSU.

9.5. Decentralized procedures for this policy shall be developed and implemented.

10. Business Continuity Planning & IT Disaster Recovery Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to responding to an emergency or other occurrence that damages systems that contain ePHI.

10.1. A contingency plan shall be developed, and implemented as needed, for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages IT resources that contain ePHI.

10.1.1. An application and data criticality analysis shall be developed and maintained to assess the relative criticality of specific applications and data in support of the contingency plan components.

10.1.2. Facility access procedures shall be developed and maintained for access to support recovery efforts.

10.1.3. Contingency plan testing and revision procedures shall be developed and executed for verifying recovery capabilities.

10.2. A data backup plan shall be established and implemented to create and maintain retrievable exact copies of ePHI.

10.3. Emergency access procedures shall be established and implemented for the retrieval of ePHI during an emergency.

10.4. A disaster recovery plan shall be established and implemented to restore any loss of data in the event of a disaster.

10.4.1. Disaster recovery plan testing and revision procedures shall be developed and executed for verifying recover capabilities.

10.5. An emergency mode operations plan shall be developed and implemented to protect ePHI during emergency operations of business processes.

10.6. Decentralized procedures for this policy shall be developed and implemented.

11. Risk Management and Audit Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to the assessment of potential risks and vulnerabilities to the security of ePHI, the reduction of such risks and vulnerabilities, and the evaluation of the agency's compliance with the State HIPAA Security policies and procedures.

11.1. The ITSU and Agency Security Official shall conduct an evaluation of Agency compliance with technical and non-technical HIPAA standards.

11.1.1. Technical and non-technical evaluations shall be conducted when there is an environmental or operational change that possibly affects the security (confidentiality, integrity, or availability) of ePHI.

11.1.2. Results of non-compliance shall be remediated as soon as practicable, depending on specific circumstances and the acceptability of the risk determined by the ITSU and Agency.

11.1.3. Results of all technical and non-technical evaluations shall be securely stored using authorized mechanisms determined by the ITSU.

11.1.4. A centralized procedure shall be developed and implemented for performing evaluations.

11.2. The ITSU and Agency Security Official shall approve a risk analysis methodology to perform an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

11.2.1. The ITSU and Agency Security Official shall conduct an accurate and thorough risk analysis, based on the approved methodology, prior to the initial HIPAA Security Rule compliance date and maintain a routine schedule for assessment updates.

11.2.2. The risk analysis shall be used to determine reasonable and appropriate levels of risk acceptance and compliance.

11.2.3. Non-compliance and unacceptable risks shall be mitigated to a reasonable and appropriate level defined by the Data Owners of ePHI. ITSU and the Agency will implement security measures sufficient to reduce unacceptable risks.

11.2.4. Results of all risk analysis shall be securely stored using authorized mechanisms determined by the ITSU.

11.2.5. A centralized procedure shall be developed and implemented for performing risk analysis.

11.3. The ITSU shall approve and execute an audit program for the purposes of measuring Agency compliance with State HIPAA Security Policies.

12. Business Associate Contracts Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements pertaining to contracts with business associates.

12.1. When the business associate **is** a government organization:

12.1.1. An approved Memorandum of Understanding (MOU) shall exist with the business associate prior to that business associate creating, receiving, maintaining, or transmitting ePHI on the covered entities behalf.

12.1.1.1. The MOU shall require the business associate to implement administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the covered entity.

12.1.1.2. The MOU shall require the business associate to ensure that any agent, including a subcontractor, to whom it provides this information, agrees to implement reasonable and appropriate safeguards to protect it.

12.1.1.3. The MOU shall require the business associate to report to the covered entity any security incident of which it becomes aware.

12.1.1.3.1. In the event of a suspected or known security incident, the covered entity shall execute incident response and reporting procedures in accordance with Policy §7.3.

12.1.1.4. The MOU shall require the business associate to make its policies and procedures, and documentation required by the HIPAA Security Rule relating to such safeguards, available to the covered entity and/or the Secretary of Health and Human Services for purposes of determining the covered entity's compliance with the HIPAA Security Rule.

12.1.1.5. The MOU shall require the business associate to comply with any state law that is more stringent than the HIPAA security rule.

12.2. When the business associate **is not** a government organization:

12.2.1. The covered entity shall perform ITSU-approved due diligence procedures prior to the authorization of the business associate to create, receive, maintain, or transmit ePHI on the covered entities behalf.

12.2.2. An approved contract shall exist with the business associate prior to that business associate creating, receiving, maintaining, or transmitting ePHI on the covered entities behalf.

12.2.2.1. The contract shall require the business associate to implement administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity, as required under HIPAA.

12.2.2.2. The contract shall require the business associate to ensure that any agent, including a subcontractor, to whom it provides this information, agrees to implement reasonable and appropriate safeguards to protect it.

12.2.2.3. The contract shall require the business associate to report to the covered entity any suspected or known security incident of which it becomes aware.

12.2.2.3.1. In the event of a suspected or known security incident, the covered entity shall execute incident response and reporting procedures in accordance with Policy §7.3.

12.2.2.4. The contract shall require the business associate to make its policies and procedures, and documentation required by the HIPAA Security Rule relating to such safeguards, available to the covered entity and/or the Secretary of Health and Human Services for purposes of determining the covered entity's compliance with the HIPAA security rule.

12.2.2.5. The contract shall allow the covered entity to immediately terminate the contract if the covered entity determines that the business associate has violated a material term of the contract.

12.2.2.6. The contract shall require the business associate to comply with any state law that is more stringent than the HIPAA Security Rule.

13. Isolating Health Care Clearinghouse Policy

Purpose: The purpose of the policy is to comply with the HIPAA Security Rule's requirements that pertain to health care clearinghouses that are part of a larger entity for protecting ePHI and information technology (IT) resources that store, process, have access to, and/or transmit ePHI.

13.1. A health care clearinghouse, that is part of a larger organization, shall implement policies and procedures, and measures to protect the ePHI and IT resources from unauthorized access by the larger organization.

13.1.1. The health care clearinghouse shall physically segregate its business functions that involve the use of ePHI from the larger organization.

13.1.2. The health care clearinghouse shall electronically isolate its ePHI and IT resources from Workforce Members who perform other functions within the larger organization.

13.2. Healthcare clearinghouse management shall periodically test the above-referenced segregation and isolation measures.

13.3. ITSU shall periodically audit the above-referenced segregation and isolation measures.

13.4. Health care clearinghouse management shall incorporate revisions to protective measures according to test and audit results.

13.5. Health care clearinghouse management shall maintain a written record of all measures and revisions adopted to protect ePHI and IT resources.

13.6. Decentralized procedures for this policy shall be developed and implemented.