



Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 1

Policy Title: Information Privacy and Security Management Process

August 13, 2018

IDENT	INFOSEC1
Type of Document:	Policy
Type of Policy:	Corporate
Sponsor's Dept:	Security
Title of Sponsor:	Security Officer
Title of Approving Official:	CEO
Date Released (Published):	8/13/2018
Next Review Date:	08/13/2019

Information Privacy and Security Management Process

Purpose

The purpose of this policy is to establish requirements for proper handling of Protected Health Information (PHI) through the adoption of an Information Privacy and Security Management Process for Vermont Information Technology Leaders (VITL). Such a process is required as a means of managing the privacy and security of PHI under the HIPAA Privacy Rule and HIPAA Security Rule §164.308(a)(1), and to comply with any other applicable information security regulations and protect the overall security of the organization. The process includes analysis and management of risks, implementation of secure systems and applications, the use of security incident procedures to learn from prior issues, information system usage audits and activity reviews, regular security evaluations and regulation compliance assessments, training for all staff using electronic information systems, and documentation of compliance activities.

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at VITL. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within VITL with policies and guidelines concerning the acceptable use of VITL technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

Scope

This policy document defines common security requirements for all VITL personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of VITL, entities in the private sector, in cases where VITL has a legal, contractual or fiduciary duty to protect said resources while in VITL custody. In the event of a conflict, the more restrictive measures apply. This policy covers the VITL network system which comprises various hardware, software, communication equipment and other devices designed to assist VITL in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any VITL domain or virtual local area network (VLAN), either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by VITL at its office locations or at remote locales.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all VITL employees or temporary workers at all locations and by contractors working with VITL as subcontractors.

Each of the policies defined in this document is applicable to any task being performed – not just to specific departments or job titles.

Policy

VITL shall establish procedures to create and maintain an Information Security Management Process to ensure the confidentiality, integrity, and availability of protected health information (PHI), payment cardholder information, other personal and private information as required by law or regulation, and essential business information. The policy and procedures include the following sections:

- 1.1. Assigned Privacy and Security Responsibility
- 1.2. HIPAA Privacy Rule Compliance
- 1.3.1 Risk Assessment and Analysis
- 1.3.2 Risk Governance and Acceptance
- 1.4. Information Security and Compliance Evaluation
- 1.5. Implementation of Secure Systems and Applications
- 1.6. Information System Usage Audits and Activity Reviews
- 1.7. Backup and Disaster Recovery
- 1.8. Information Security Incidents
- 1.9. Training
- 1.10. Sanctions for Policy Violations
- 1.11. Contracts with Third Parties
- 1.12. Documentation
- 1.13. Exceptions

1.1 Assigned Privacy and Security Responsibility

§164.530(a) of the HIPAA Privacy Rule, and §164.308(a)(2) of the HIPAA Security Rule each require the designation of a single individual with the responsibility for the development and implementation of the policies and procedures required for compliance.

VITL will assign the HIPAA Security Officer (referred to as Security Officer) responsibility for all matters relating to the security of personal or private information to the Director of Technology. The Security Officer may delegate activities to the Information Security Team (IST). This individual or team (as appropriate) will be responsible for ensuring that all personal or private information is protected against reasonably anticipated threats or hazards to the security and

integrity of the information, and against reasonably anticipated improper uses and disclosures. The Security Officer will be the initial point of contact in any security compliance inquiry. If the Director of Technology is unavailable, or temporarily unable, to fulfill the Security Officer role VITL senior leadership will assign the responsibility to an appropriate member of staff.

The Security Officer will have oversight for the following:

- a) Ensuring that all policies and procedures required under applicable standards and regulations are established and maintained over time.
- b) Monitoring the appropriate and consistent implementation of policies and procedures.
- c) Ensuring that all members of the workforce, contractors, and business associates are aware of and abide by the policies and procedures.
- d) Monitoring and analyzing security alerts and information and ensuring proper follow-up action.
- e) Investigation of information security incidents or breaches.
- f) Authorization of user accounts, including additions, deletions, and modifications, and monitoring and controlling access to data maintained by VITL.
- g) Ensuring that any security weaknesses discovered during security incidents investigation or security evaluations will be prioritized for correction and subsequently corrected.

The Security Officer will ensure that analyses and documentation, required by applicable standards and regulations, and VITL's security policies and procedures, are carried out fully and completely.

VITL will appoint the Director of Operation as the Privacy Officer; the Privacy Officer will be responsible for all matters relating to the privacy of personal or private information. The Privacy Officer oversees all activities related to the development, implementation and maintenance of VITL's policies and procedures covering the privacy and breach of patient health information. This person serves as the key compliance officer for all federal and state laws that apply to the privacy of patient information. The Privacy Officer may delegate their responsibilities to other qualified parties where necessary and appropriate. If the Director of Operations is unavailable, or temporarily unable, to fulfill the Privacy Officer role VITL senior leadership will assign the responsibility to an appropriate member of staff.

The Privacy Officer is tasked with the responsibility of ensuring that all VITL patient information privacy and breach policies and procedures, related to the privacy of, and access to, patient health information, are followed. Specific responsibilities include, but are not limited to the following:

- a) Develop policies and procedures for staff training related to the privacy, breach and identity theft, as necessary, of patient health information and protected health information.

- b) Define appropriate levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities.
- c) Oversee, direct, deliver and ensure the delivery of initial and ongoing privacy, breach, and identity theft training and orientation to all staff members.
- d) Serve as the contact person for patient complaints, reports of breaches and patient requests for information.
- e) Process any patient requests for access to and amendment of health information.
- f) Process all patient accounting requests.
- g) Ensure compliance with all applicable Privacy Rule, Breach Rule, and Red Flag Rules or Identity Theft Rules requirements and works with managers to ensure the company maintains appropriate privacy and confidentiality notices, forms and materials.
- h) Act as the single point of contact for any Privacy compliance inquiry
- i) Cooperate with the state and federal government agencies charged with compliance reviews, audits and investigations related to the privacy of patient information.

1.2 HIPAA Privacy Rule Compliance

VITL and its staff shall treat all PHI as confidential information and only access the minimum necessary information to perform their job functions. PHI shall not be used or disclosed in any way other than as indicated in the Business Associate Agreements as agreed to by VITL.

In the event that VITL does retain and manage data that are considered to be part of a patient's Designated Record Set in a medical record, VITL will develop policies and procedures to satisfy individual rights defined in the HIPAA Privacy Rule § 164.520-528, as necessary and appropriate.

In the event of any improper disclosures in violation of the HIPAA Privacy Rule, steps will be taken to limit and mitigate any harmful effects of such disclosures, per §164.530(f).

Policy on training and documentation of HIPAA Privacy Rule compliance is integrated with that for HIPAA Security and Breach Notification Rule compliance.

1.3.1 Risk Assessment and Analysis

VITL shall regularly, at least annually, evaluate its information security-related policies and procedures to ensure that they meet the requirements of the HIPAA Security and Breach Notification Rules (§164.300 *et seq.* and §164.400 *et seq.*). A compliance evaluation shall also be required whenever there is a change in environmental or operational conditions that may affect the security of electronic PHI.

VITL shall document risk analysis and assessment of PHI held by the organization regularly or upon significant changes to operations or the environment as required by HIPAA Security Rule §164.308(a)(1). Such procedures shall include the conduct of an accurate and thorough assessment of the potential risks and vulnerabilities to personal and private information held by the organization.

Risk analysis and assessment shall be carried out using a process that substantially conforms to the process defined in the National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (document available at <http://csrc.nist.gov/publications/nistpubs>) and any guidance issued by the US Department of Health and Human Services in support of HIPAA compliance and risk analysis.

Risks shall be mitigated and managed by VITL to the best of its abilities within reasonable and appropriate constraints of cost, staff ability, and hardware and software capabilities, according to a regularly developed and updated Risk Management plan based on the Risk Analysis.

Risk analysis and assessments shall be reviewed and updated whenever there are material changes in systems or operations controlled by VITL, or significant changes in the security environment in which VITL operates, or no less frequently than once every year. In addition to the risk analysis and assessment process, each system will additionally be reviewed to ensure its Security Categorization has not changed.

1.3.2 Risk Governance and Acceptance

VITL holds a quarterly risk governance meeting to discuss emerging and potential threats, and how they could apply to the organization; VITL holds additional ad hoc risk governance meetings when a specific threat emerges, and the threat needs to be addressed before the next scheduled meeting. The risk governance meeting must include the Security Officer, Privacy Officer, and the Security Analyst; the meetings may include, by request, subject matter experts who can provide guidance regarding the likelihood a threat may be exploited and the potential impact. There are three primary goals of the risk governance meeting:

1. Determine the severity of new threats by comparing the likelihood the threat will be exploited, with the negative impact to the organization if the threat is successfully exploited.
2. Determine the cost of resources (monetary and time) required to mitigate the risk of an exploited threat and then compare the resultant cost to any privacy or security benefits gained by mitigating the risk.
 - a. There may be multiple cost benefit analysis results for different mitigation options.
3. One of the following two outcomes must be reached for each threat event discussed:
 - a. Provide a recommendation that the risk of threat exploitation should be accepted, along with the reasoning for the recommendation.
 - b. Determine that VITL will mitigate the risk.

If the outcome of the meeting is to recommend that VITL accept the risk, then a presentation of the discussion and reasoning for the recommendation will be made to VITL's senior leadership by the Security or Privacy Officer. If senior leadership can reach a unanimous decision to accept the risk, the threat and associated risks will be documented as acceptable and no mitigation efforts will proceed. When a risk is accepted by VITL senior leadership, an agenda item will be added to the monthly Plan of Actions and Milestones (POA&M) review meeting, the threat, associated risks, and VITL's acceptance of the risk will be presented to the Agency of Digital Services (ADS) representative for additional comment.

If the ADS representatives disagree with the VITL decision to accept the risk, the risk will be added to the POA&M for tracking and resolution.

If the outcome of the meeting is that VITL will mitigate the risk, then an item will be opened on the POA&M to document mitigation plans and progress.

The risk will be considered mitigated by VITL when marked complete on the POA&M and approved by the Security Officer. The risk mitigation will then be reviewed by VITL's third-party security assessment provider, or the State of Vermont Agency of Digital Services.

1.4 Information Security and Compliance Evaluation

VITL shall develop procedures to establish regular, periodic evaluations of the information security-related technical measures, policies, and procedures in place at the organization to ensure that they continue to meet the requirements of HIPAA Security Rule §164.308(a)(8). The period of review shall be at least annual and determined according to the organization's information systems risk analysis and consideration of best practices. Evaluations shall be documented for regulatory compliance and to provide direction to the organization in the execution of its security management process and plans.

VITL shall regularly evaluate its information security-related policies and procedures to ensure that they meet the requirements of the HIPAA Security and Breach Notification Rules (§164.300 *et seq.* and §164.400 *et seq.*). The period of review shall be determined according to the organization's information systems risk analysis and consideration of standard security practices, or at least annually. A compliance evaluation shall also be required whenever there is a change in environmental or operational conditions that may affect the security of electronic PHI.

1.5 Implementation of Secure Systems and Applications

It is the policy of VITL to implement and maintain systems and applications using secure best practices, whether developed in-house or procured from an external vendor. Procedures shall be developed to address the following:

- Documentation Requirements
- Default Passwords and Parameters
- Password Suppression and Account Lockout
- Automatic Logoff
- Wireless Access
- Configuration Standards
- Administrative Access
- Patch Management
- Vulnerability Management
- Software Development Practices
- Change Control
- Web-based Software and Applications
- Application Security
- Application Backup and Restoration
- Security Configuration for Desktop and Laptop Computers.

VITL shall have procedures to track changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information (“ePHI”). Change tracking allows the Information Technology (“IT”) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Only software created by VITL application staff, if applicable, or software approved by the Security Officer or appropriate personnel will be used on VITL computers and networks. All new software will be tested by appropriate personnel to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes software procured directly from commercial sources as well as shareware and freeware.

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Security Officer or appropriate personnel; approval by the Security Officer or appropriate personnel may only apply to a specific version of the software. Whenever possible when downloading shareware or freeware the downloaded file should be integrity checked through hash verification, if possible. Since shareware and freeware are often provided through an open distribution environment, special precautions must be taken before it is installed on VITL computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage VITL hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

1.6 Information System Usage Audits and Activity Reviews

VITL implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information (“ePHI”). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

VITL is committed to routinely auditing users’ activities in order to regularly assess potential risks and vulnerabilities to ePHI in its possession. As such, VITL has established a secure drive location where all ePHI must be stored for routine VITL operations. ePHI also is stored at Medicity (our HIE vendor) and within the VITL data management infrastructure hosted by TechVault. VITL will regularly assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

The list of exceptions and their purpose for storing PHI on the designated drive are as follows:

- 1.) Audit and security logs that contain PHI events do not need to be exclusively stored on the P:\ drive, they can also exist on specifically identified security systems with additional access control and hardening.

- 2.) PHI can be present in Salesforce (MyVITL) tickets to facilitate communications between VITL and partner organizations, where exchange of PHI is required for troubleshooting or other business needs. PHI cannot be present in the subject field of Salesforce tickets.
- 3.) Offsite backups stored in the Azure cloud contain encrypted PHI, these files must be stored offsite to provide full disaster recovery capability.

VITL shall conduct, on a periodic basis or as related to an incident or other event or activity, reviews and audits of information access, system usage, and internal security controls, according to HIPAA Security Rule §164.308(a)(1)(ii)(D), §164.312(b), and §164.312(c).

Such controls may include, for example: logs produced by firewall or system monitoring applications, access reports and other documentation provided by application programs in use, system security status reports, incident tracking systems and procedures, and sign-in logs for service personnel.

VITL shall establish a process for conducting, on a periodic basis, at least annually, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. VITL shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Such reviews of information system activity shall be sufficient to discover and facilitate investigations into information security incidents, ensure data have not been modified inappropriately, and provide information for input to the organization's security management process, in order to determine the effectiveness of security procedures and controls, and to discover and mitigate security issues that may not be fully addressed by the existing procedures or controls. The level of detail to be audited will be determined according to the organization's risk analysis and set as part of the overall information security management process.

As systems are modified and expanded, abilities to audit access in greater detail shall be pursued where practicable and according to the determination of the organization's risk analysis and any risk mitigation plan in place.

Procedures shall be identified to establish qualifications of the reviewer, the scope of audits and logging, the report format for review findings, and the frequency of reviews of various types.

1.7 Backup and Disaster Recovery

It is the policy of VITL to prepare for contingencies and ensure an appropriate response to emergencies or other occurrences that may damage systems that contain electronic confidential information, such as protected health information (PHI), and maintain usable copies of electronically held confidential information for use in such responses if appropriate, as required by HIPAA Security Rule §164.308(a)(7), and by other applicable state or federal regulations. Information not required to be maintained shall be disposed of according to defined procedures.

Contingency plans must take into account the criticality of applications/systems and data, and the effects of short-term interruptions (such as brief power or system failures) and long-term disruptions (such as a loss of facilities or epidemic).

Procedures shall be established sufficient to restore lost or damaged data with a useful duplicate, including the definition of which file systems to back up, frequency of backups and media rotation, off-site storage requirements, documentation and labeling of storage media, and regular testing of backed up data to ensure adequacy.

Backup and restoration procedures for electronic media and information systems containing critical data must be tested according to the frequency and practices as established in the Individual System Backup Plans.

VITL management shall maintain a detailed Disaster Recovery Policy (DRP). This plan addresses the hardware and software configurations and detailed recovery procedures. Plans and procedures shall be sufficient to ensure the restoration of lost data and system access, including a full range of information and activities needed to assure that the Plan and its implementation will be effective.

Plans and procedures shall be sufficient to enable the organization to continue secure operations while operating in an emergency situation as practicable, including the identification of crisis management team members, facilities for operation of a command center, a process for acquiring personnel with the necessary skill sets to supplement staff in an emergency, alternate locations for data processing and related work, health and safety issues, and procedures to enable access to electronic information systems as necessary.

1.8 Information Security Incidents

VITL shall have in place an **Information Security Incident Response Policy**, including procedures for the reporting, processing, and response to suspected or known information security incidents, in order to investigate, mitigate, and document such incidents, so that security violations may be reported and handled promptly, using an orderly process known to all workforce members, according to the HIPAA Breach Notification Rule and HIPAA Security Rule §164.308(a)(6).

Refer to the **Information Security Incident Response Policy** for policy and procedure details.

1.9 Training

VITL shall establish an Information Privacy and Security Awareness and Training Program for the purpose of ensuring that all workforce members, including management, are aware of the organization's security policies and procedures and general principles of information security, as required by the HIPAA Privacy Rule, and HIPAA Security Rule §164.308(a)(5). Training must be provided to new staff before access to PHI is permitted and will additionally be provided to all staff at least annually. Procedures shall include definition of when training is to occur and for whom, what training content will be provided, documentation, and acknowledgement.

Training regarding VITL policies and procedures will be provided to all new staff members during the onboarding and orientation process.

Training on various privacy and security topics will be provided to all staff members during monthly staff meetings. Staff meeting training attendance and presentation slides will be documented in the [Training folder on the Security Share](#)

While employed by VITL, members of staff may be requested by their director to undergo specialized training in a specific role or system. These specialized forms of training will be documented within the [Specialized Training folder of the Security Share](#)

1.10 Sanctions for Policy Violations

As appropriate, any member of the workforce who does not comply with the security policies and procedures of VITL, or who otherwise misuses or misappropriates personal or private information will be subject to disciplinary action according to the organization's disciplinary procedures. Workforce members in violation of security policies and procedures may be subject to the following:

1. A verbal warning
2. Notice of disciplinary action placed in personnel files
3. Removal of system privileges
4. Termination of employment and/or contract penalties
5. Civil or criminal penalties which may include notifying law enforcement officials and regulatory accreditation and licensure organizations
6. Other sanctions as identified in the organization's disciplinary procedures.

Disciplinary and sanction procedures shall be defined by VITL management.

1.11 Contracts with Third Parties

VITL shall enter into written agreements with any entities that use or disclose personal or private information on behalf of the organization, in order to require the protection of the security of any and all such information as required by HIPAA Privacy Rule §164.502 and HIPAA Security Rule §164.308(b). Such agreements shall be contractual, and, in the case of protected health information, shall be Business Associate Contracts designed to meet the requirements of HIPAA Security Rule §164.308(b) and §164.314(a), and HIPAA Privacy Rule §164.502(e) and §164.504(e), and shall incorporate the required elements listed within §164.504(e)(2), including any amendments. HIPAA Business Associate Contracts shall be approved by VITL legal counsel.

1.12 Documentation

VITL shall document any policies and procedures implemented under the requirements of the HIPAA Privacy, Security, and Breach Notification Rules and other applicable information security regulations. VITL shall also document any actions, activities, and assessments

required to be performed under applicable HIPAA regulations or under the requirements of policies enacted in support of such regulations.

Documentation shall be in electronic or paper format and shall be maintained for at least six years from the date of issue or the date of last effect, whichever is later. Documentation shall be periodically reviewed and updated as needed or in response to environmental or operational changes affecting the security of electronic confidential information.

1.13 Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use that do not comply, but near-term future systems will, and are planned for;
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, Directors must develop a written explanation of the compliance issue and a plan for coming into compliance with VITL's information security policies in a reasonable amount of time. Explanations and plans must be submitted to the Privacy and Security Officers for review and must be approved by them.

Enforcement

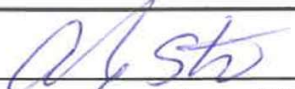

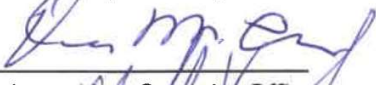



Any employee, vendor, client, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

References

- Information System Access Control Policy
- Information System User Policy
- Information Security Incident Response Policy
- HIPAA Privacy, Security, and Breach Notification Rules

Policy Review & Approval

VITL management performs a periodic review of this policy as defined in this policy. Based on the review, VITL management may change this policy to reflect its intentions and compliance requirements.

 _____ Reviewed by: Privacy Officer	 _____ Date
 _____ Reviewed by: Security Officer	 _____ Date
 _____ Approved by: CEO	 _____ Date