VITL PRIVACY AND SECURITY POLICIES

VITL HIPAA Policy – HIPAA Regulation Guide

This document itemizes the HIPAA Security Rule safeguards and identifies the *VITL HIPAA Compliance Policies and Procedures* sections that pertain to each safeguard's requirements.

- Policy sections may have supporting procedures integrated into policy or defined in the companion *VITL HIPAA Procedures and Appendices* document.
- Regulatory language is paraphrased in some sections for ease of use.
- *Addressable* specifications are identified as such, otherwise all standards and safeguards are *Required* under the regulations.
- Policies are listed in order of relevance to each identified safeguard.

ADMINISTRATIVE SAFEGUARDS §164.308

§164.308(A)(1) SECURITY MANAGEMENT PROCESS

(i) Standard: ***Security Management Process.*** Implement policies and procedures to prevent, detect, contain, and correct security compliance violations.

Reference: Policy InfoSec 1; Policy InfoSec 1, section 1.12; Policy InfoSec 1, section 1.13; Policy InfoSec 4

(ii) Implementation Specifications:

(A) ***Risk Analysis.*** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI.

Reference: Policy InfoSec 1, section 1.3

(B) ***Risk Management.*** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Reference: Policy InfoSec 1, section 1.3

(C) ***Sanction Policy.*** Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures.

Reference: Policy InfoSec 1, section 1.10

(D) ***Information System Activity Review.*** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Reference: Policy InfoSec 1, section 1.6; Policy InfoSec 4

§164.308(A)(2) ASSIGNED SECURITY RESPONSIBILITY

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

Reference: Policy InfoSec 1, section 1.1

§164.308(A)(3) WORKFORCE SECURITY

(i) Standard: Implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic PHI, and prevent those workforce members who do not have access from obtaining access to electronic PHI.

Reference: Policy InfoSec 2, section 2.1; Policy InfoSec 3, section 1

(ii) Implementation Specifications:

(A) ***Authorization and/or supervision.*** Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed. (Addressable)

Reference: Policy InfoSec 2, section 2.1; Policy InfoSec 3, section 1

(B) ***Workforce Clearance Procedure.*** Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate. (Addressable)

Reference: Policy InfoSec 2, section 2.1; Policy InfoSec 3, section 1

(C) ***Termination Procedures.*** Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or when the workforce member no longer needs access to PHI. (Addressable)

Reference: Policy InfoSec 3, section 1

§164.308(A)(4) INFORMATION ACCESS MANAGEMENT

(i) Standard: Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the HIPAA Privacy rule**.**

Reference: Policy InfoSec 3

(ii) Implementation Specifications:

(A) Isolation of Clearinghouse function; not applicable to VITL.

(B) ***Access Authorization.*** Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism. (Addressable)

Reference: Policy InfoSec 3, section 1; Policy InfoSec 2, section 2.1; Policy InfoSec 2, section 2.2

(C) ***Access Establishment and Modification.*** Implement policies and procedures that, based upon your access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. (Addressable)

Reference: Policy InfoSec 3, section 1; Policy InfoSec 2, section 2.1; Policy InfoSec 1, section 1.6

§164.308(A)(5) SECURITY AWARENESS AND TRAINING

(i) Standard: Implement a security awareness and training program for all members of the workforce (including management).

Reference: Policy InfoSec 1, section 1.9

(ii) Implementation Specifications:

(A) ***Security Reminders.*** Provide the workforce periodic security updates. (Addressable)

(B) ***Protection from malicious software.*** Establish and provide training in procedures for guarding against, detecting, and reporting malicious software such as viruses, etc. (Addressable)

(C) ***Log-in monitoring.*** Establish and provide training in procedures for monitoring log in attempts and reporting discrepancies. (Addressable)

(D) *Password Management.* Establish and provide training in procedures for creating, changing, and safeguarding passwords. (Addressable)

Reference (for A-D): Policy InfoSec 1, section 1.9

§164.308(A)(6) SECURITY INCIDENT PROCEDURES

(i) Standard: Implement policies and procedures to address security incidents.

Reference: Policy InfoSec 4; Policy InfoSec 1, section 1.8; Policy InfoSec 2, section 2.6

(ii) Implementation Specification:

Response and Reporting. Implement policies and procedures to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Reference: Policy InfoSec 4; Policy InfoSec 1, section 1.8; Policy InfoSec 2, section 2.6

§164.308(A)(7) CONTINGENCY PLAN

(i) Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (i.e. fire, vandalism, system failure, natural disaster) that damages systems that contain electronic PHI.

Reference: Policy InfoSec 1, section 1.7

(ii) Implementation Specifications:

(A) *Data backup plan.* Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.

Reference: Policy InfoSec 1, section 1.7

(B) *Disaster Recovery Plan.* Establish (and implement as needed) procedures to restore any loss of data.

Reference: Policy InfoSec 1, section 1.7

(C) *Emergency Mode Operation Plan.* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

Reference: Policy InfoSec 1, section 1.7

(D) *Testing and revision procedures.* Implement procedures for periodic testing and revision of contingency plans. (Addressable)

Reference: Policy InfoSec 1, section 1.7

(E) *Applications and data criticality analysis.* Assess the relative criticality of specific applications and data in support of other contingency plan components. (Addressable)

Reference: Policy InfoSec 1, section 1.7

§164.308(A)(8) EVALUATION

Standard: Perform periodic technical and non-technical evaluations based on established security best practices and the HIPAA Security Rule, in response to environmental or operational changes affecting the security of electronic PHI, that establish the extent to which security policies and procedures meet the Security Rule requirements.

Reference: Policy InfoSec 1, section 1.4

§164.308(b) Business Associate Agreements

Standard: Document satisfactory assurances that any business associates will appropriately safeguard any electronic PHI and meet the requirements of the HIPAA Privacy and Security Rules.

Reference: Policy InfoSec 1, section 1.11

PHYSICAL SAFEGUARDS §164.310

§164.310(a) Facility Access Controls

(1) Standard: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Reference: Policy InfoSec 3, section 5

(2) Implementation Specifications:

(i) *Contingency operations.* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. (Addressable)

Reference: Policy InfoSec 1, section 1.7

(ii) *Facility security plan.* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. (Addressable)

Reference: Policy InfoSec 3, section 5

(iii) *Access control and validation procedures.* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. (Addressable)

Reference: Policy InfoSec 3, section 5

(iv) *Maintenance records.* Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks). (Addressable)

Reference: Policy InfoSec 3, section 5

§164.310(b) Workstation Use

Standard: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

Reference: Policy InfoSec 2, section 2.2; Policy InfoSec 2, section 2.3; Policy InfoSec 2, section 2.4; Policy InfoSec 2, section 2.5

§164.310(c) Workstation Security

Standard: Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.

Reference: Policy InfoSec 3, section 5

§164.310(D) DEVICE AND MEDIA CONTROLS

(1) Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.

Reference: Policy InfoSec 3, section 6; Policy InfoSec 3, section 7

(2) Implementation Specifications:

(i) *Disposal.* Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.

Reference: Policy InfoSec 3, section 7

(ii) Media re-use. Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

Reference: Policy InfoSec 3, section 7

(iii) *Accountability.* Maintain a record of the movements of hardware and electronic media and any person responsible therefore. (Addressable)

Reference: Policy InfoSec 3, section 6

(iv) *Data backup and storage.* Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment. (Addressable)

Reference: Policy InfoSec 1, section 1.7

TECHNICAL SAFEGUARDS §614.312

§164.312(A) TECHNICAL ACCESS CONTROL

(1) Standard: *Access Control.* Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been properly granted access rights.

Reference: Policy InfoSec 3; Policy InfoSec 1, section 1.5

(2) Implementation Specifications:

(i) *Unique user identification.* Assign a unique name and/or number for identifying and tracking user identity.

Reference: Policy InfoSec 3, section 1; Policy InfoSec 2, section 2.1

(ii) *Emergency Access Procedure.* Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.

Reference: Policy InfoSec 3, section 1

(iii) *Automatic Logoff.* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. (Addressable)

Reference: Policy InfoSec 1, section 1.5 Policy InfoSec 2, section 2.2; Policy InfoSec 2, section 2.4

(iv) *Encryption and decryption.* Implement a mechanism to encrypt and decrypt electronic PHI on systems. (Addressable)

Reference: Policy InfoSec 3, section 3; Policy InfoSec 2, section 2.4; Policy InfoSec 2, section 2.5

§164.312(b) Audit Controls

Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

Reference: Policy InfoSec 1, section 1.6

§164.312(c) Integrity

(1) Standard: ***Integrity.*** Implement policies and procedures to protect electronic PHI from improper alteration or destruction.

Reference: Policy InfoSec 3, section 4; Policy InfoSec 3, section 2; Policy InfoSec 1, section 1.5

(2) Implementation Specification:

Mechanism to authenticate electronic PHI. Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner. (Addressable)

Reference: Policy InfoSec 3, section 1; Policy InfoSec 3, section 4; Policy InfoSec 3, section 2; Policy InfoSec 1, section 1.5; Policy InfoSec 1, section 1.6

§164.312(d) Person or Entity Authentication

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

Reference: Policy InfoSec 3, section 1

§164.312(e) Transmission Security

(1) Standard: Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

Reference: Policy InfoSec 3, section 3; Policy InfoSec 3, section 4; Policy InfoSec 2, section 2.3; Policy InfoSec 2, section 2.5; Policy InfoSec 1, section 1.5

(2) Implementation Specifications:

(i) ***Integrity controls.*** Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of. (Addressable)

Reference: Policy InfoSec 3, section 3; Policy InfoSec 3, section 4; Policy InfoSec 1, section 1.5; Policy InfoSec 1, section 1.6

(ii) ***Encryption.*** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. (Addressable)

Reference: Policy InfoSec 3, section 3; Policy InfoSec 2, section 2.3; Policy InfoSec 2, section 2.5; Policy InfoSec 1, section 1.5

Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 1

Policy Title: Information Privacy and Security Management Process

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):	1/22/16
Next Review Date:	1/1/17

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 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 VITL network system which is comprised of 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 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, models, 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 the 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. Risk Assessment and Analysis, and Risk Management
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 Security Officer responsibility for all matters relating to the safeguarding of the privacy and security of personal or private information to the Chief Technology Officer (CTO). 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 HIPAA Security Officer will be the initial point of contact in any security compliance inquiry.

The HIPAA Security Officer will have oversight for:

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 and/or breaches.
f) Administration of user accounts, including additions, deletions, and modifications, and monitoring and controlling all access to data.
g) Ensuring that any security weaknesses discovered in the course of security incidents or security evaluations will be prioritized for correction and corrected.
h) Ensuring that analyses and documentation required by applicable standards and regulations, and/or OHCC's security policies and procedures, are carried out fully and completely.

The HIPAA Privacy Officer will be responsible for receiving any complaints about HIPAA compliance and will be the initial point of contact in any privacy compliance inquiry.

1.2 HIPAA Privacy Rule Compliance

VITL and its staff shall treat all PHI as confidential information and only access the minimum necessary 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 Risk Assessment and Analysis, and Risk Management

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 and Analysis and Assessment 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.

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:

- 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
- Platform Security
- 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. A list of approved software is maintained in Shared(S:)\it\vitl\Admin\LOG - Software Management.xlsx. All new software will be tested by appropriate personnel in order 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. Because the software is often provided in 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 Rackspace. 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.

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 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 must 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.

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:

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. Or 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

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.

Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 2

Policy Title: Information System User Policy

January 26, 2016

IDENT	INFOSEC2
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):	1/22/16
Next Review Date:	1/1/17

Information System User Policy

Purpose

The purpose of the Information System User Policy is to ensure the proper use of workstations, devices, and computing facilities by members of the VITL workforce to protect the security of personal or private information, as required by the HIPAA Privacy and Security Rules and other applicable regulations.

Compliance with the enclosed policies and directives will:

- Protect personal or private and other information contained within these systems.
- Protect the significant financial investment made in these systems.
- Protect VITL and its system users from unnecessary risk.

Scope

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, 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 the task being performed – not just to specific departments or job titles.

Policy

The computer systems at VITL are provided to employees to perform their jobs. As such, VITL reserves the right to determine appropriate use of the equipment and software that employees use. No employee is allowed to employ these resources for personal gain. It is the responsibility of VITL Leadership to monitor the appropriate behavior of their employees, with the guidance and support of IS.

It is the policy of VITL that all workforce members shall comply with the requirements of applicable privacy and security standards and regulations. Compliance shall be ensured through the use of measures such as training, security reminders, policies and procedures, sanctions for policy violations, and monitoring of workforce activities.

Employees who are granted access to the computer systems at VITL agree to abide by the policies guiding the appropriate use of these systems. Any employee found in violation of this policy will be subject to a security investigation and possible disciplinary action as described in the Corrective Action and Discipline Policy, up to and including termination. Some violations may also constitute a criminal offense and may result in legal action according to Federal and State laws.

This policy addresses a variety of issues computer, system, and network users must be aware of, as described in the following sections:

2.1. Gaining Access to Information Systems
2.2. Acceptable Use
2.3. The Internet and e-mail
2.4. Laptops, Portable Devices, and Removable Media
2.5. Remote Access or Use of Information
2.6. Information Security Incidents
2.7. Intimidating or Retaliatory Acts
2.8. Confidentiality Agreement

2.1 Gaining Access to Information Systems

VITL grants role-based access to the network as well as other systems, and the organization Intranet and the Internet at large. The purpose of this policy is to provide the minimum necessary access for employees to perform their job functions. Users may access only those computer systems and resources that are necessary to perform their job. The Privacy and Security Officer is responsible for managing the process for the provision of access and passwords. Procedures shall include Access of Information, Network Access Changes, and Password Management.

1) Access of Information

a) All workforce members working with personal or private information or working in areas where personal or private information is accessible shall be authorized to do.

b) Workforce members shall be subject to a clearance procedure before being allowed access to personal or private information; such clearance shall be appropriate to the level of sensitivity of the information being accessed and the level of access accorded to the workforce member. Background checks will be conducted under the guidance of Human Resources and legal counsel.

c) Network and system IDs and passwords are provided for individual use only and must not be shared with anyone. IT may track activity in the system related to an employee's logon ID and password. Use of a logon ID and password is the legal equivalent of a signature.

2) Network Access Changes

All requests for new employee/user access must be made at a minimum of 5 days prior to starting and must be made of the System Administrator by the employee's supervisor following an established process. The System Administrator shall be responsible for the administration of access controls to all VITL computer systems. The System Administrator will process adds, deletions, and changes upon receipt of a written or in-person request from the end user's supervisor. Request for access to ePHI must also be approved by the Security Officer. Deletions may be processed by an oral request prior to reception of the written request.

3) Password Management

Network passwords will adhere to the following policies:

a) Passwords will be managed according to procedures and specifications defined by the Security Officer.
b) Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person.
c) No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
d) Users should not use the "Remember Password" feature of internal applications; User many use approved password keeper applications for external web sites which do not contain ePHI;
e) Passwords must be changed every 180 days.
f) A user cannot reuse the last 6 passwords.
g) Passwords must be at least eight characters and contain three of these four characteristics: upper case letters, lower case letters, numbers, and special symbols.
h) Passwords can be changed no more frequently than every 5 days unless required by a security breach or as approved by the Security Officer.
i) Entry of five incorrect passwords results in account lockout. The counter resets to zero after 10 minutes if the account is not locked. The lockout period is 30 minutes.
j) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords. Long, personally memorable phrases are recommended.
k) A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
l) Passwords must not be disclosed under any conditions to other workforce members or individuals, including family members.

2.2 Acceptable Use

Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, and for the care and security of any computer or hardware assigned to them.

Users shall not knowingly engage in any activity that may be potentially harmful to any portion of the network or its users. They shall also take the necessary precautions to protect any confidential or sensitive information from inappropriate or unauthorized access by others.

1) Use of Computing Resources

a) Company computer resources must be used in a manner that complies with company policies and State and Federal laws and regulations.

b) Uses shall not interfere with the proper functioning or the ability of others to make use of VITL's networks, computer systems, applications and data resources.

c) Use of VITL computer resources for personal gain is not permitted. Personal use of a limited nature is allowed but must not compromise the integrity of VITL's systems or workplace productivity.

d) Users are not permitted to connect any equipment to the corporate network without prior approval from the Security Officer. Users may connect equipment to the guest wireless network.

2) Access of Information

a) Workforce members may not access systems, files, documents, or other data of other users, or systems, files, documents, or other data to which they have not been properly granted access. Workforce members may not share their log-in or access codes or passwords with others.

b) Users leaving their work area should lock their computers (by logging off, using the ctrl-alt-delete or Windows-L key combination, or similar mechanism) to prevent use of their login by others. The Security Officer will implement an automatic password protected screen saver for all PCs connected to the network, which will activate after no more than 15 minutes of inactivity. In order to regain access to the computer, the user who is logged into that computer must enter their login id and password to unlock it. Staff may not take any action which would override this setting.

c) E-mail over the Internet shall not be used for the transmission of unencrypted protected health information that is part of VITL's operations.

d) Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate reason to access that information, to the extent practicable.

3) Hardware and Equipment

a) Only computer hardware and software owned by and installed by VITL is permitted to be connected to the network or installed on VITL equipment however employees may request an exception from the Security Officer. Only software that has been approved for corporate use by VITL may be installed on VITL equipment. Personal computers supplied by VITL are to be

used mainly for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by VITL for home use.

b) Computers and computer-related hardware belonging to VITL may not be removed from VITL premises without the knowledge and approval of the appropriate department leader and the Security Officer.

c) Users must notify the VITL System Administrator of any equipment that is missing or damaged.

d) Employees or business associates may not bring computers from outside VITL and connect them to the VITL network without prior approval from the Security Officer. Employees, business associates and other guests may connect computers to the VITL Guest Network without approval.

4) Technology Adoption

It is the policy of VITL to protect the security of personal and private information as new technologies and devices are adopted for use by the workforce, so that any technologies or devices used by the workforce do not jeopardize the security or personal or private information. Use of new technologies and devices such as modems, wireless network access points, personal digital assistants, smart phones and handheld computers that may transmit or retain personal or private information must be subject to:

a) Explicit management approval

b) Security procedures for the technology, including risk assessment

c) Maintenance of a list of all such devices and personnel with access

5) Software Copying, Downloading, and Installation

a) All software used on VITL computers must be licensed. Employees are required to read, sign, and adhere to VITL Confidentiality and Employee Non-Disclosure and Non-use Agreement.

b) The System Administrator will coordinate the acquisitions of commercial software, including those used for personal computers, related training courses, and manuals.

c) Software may not be downloaded and/or installed without prior approval. Approval of any new software shall include scanning for viruses or other malicious software. It is against company policy to install or run software requiring a license on any company computer without a valid license.

d) All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of VITL are the property of VITL unless covered by a contractual agreement.

6) Uploading, Copying, Backing Up, and Disposing Of Information

a) Workforce members may not upload information into VITL systems except as part of an established business process.

b) Workforce members may not copy information in VITL systems except as part of an established business process.

c) The confidentiality of any data copied or removed from VITL premises must be maintained. Refer to Sections 2.5 and 2.6 of this policy.

d) Any data files generated by a user must be stored on the network-based personal or group folder, so that they can be backed up nightly for safekeeping. Business-critical information not stored on a centralized file or application server must be backed up on a regular basis to protect against business interruption.

e) Business information will not be deleted or otherwise removed from VITL systems except as in accordance with defined information disposal procedures, and will not be deleted if it may be required for discovery proceedings related to a federal or civil lawsuit.

7) Wireless Networks

a) The use of non-VITL wireless networks for access to VITL systems shall be restricted to networks that are configured securely, utilizing at least the WPA2 encryption standard, and that require a secure login and password.

8) Instant Messaging and Texting

Instant Messaging and texting are not considered secure means of communication. Users are prohibited from including any confidential or protected health information in instant messages and text messages unless a secure communications technology approved by the HIPAA Security Officer is properly used.

9) Social Media

a) Employees must remember that the same basic policies apply to blogs and social networking sites as in other areas of their lives.

b) Follow all applicable VITL policies. For example, you must not share confidential or proprietary information about VITL and you must maintain patient privacy.

c) Write in the first person. Where your connection to VITL is apparent, make it clear that you are speaking for yourself and not on behalf of VITL.

d) If you communicate in the public Internet about VITL or VITL-related matters, disclose your connection with VITL and your role at VITL. Use good judgment and strive for accuracy in your communications; errors and omissions reflect poorly on VITL, and may result in liability for you or VITL.

e) Use a personal email address (not your VITL e-mail address) as your primary means of identification when writing personal views.

f) If your blog, posting or other online activities are inconsistent with, or would negatively impact VITL's reputation or brand, you should not refer to VITL, or identify your connection to VITL.

g) Be respectful and professional to fellow employees, business partners, competitors and patients. Avoid using unprofessional online personas.

h) Ensure that your blogging and social networking activity does not interfere with your work commitments.

i) Ask your supervisor if you have any questions about what is appropriate to include in your blog or social networking profile.

j) Guidelines for Official VITL Participation

• Some VITL staff may be interested in engaging in Internet conversations for work-related purposes, or may be asked by supervisors or leadership to participate, in support of VITL's organizational objectives.

• Use of external Web sites for work-related purposes (e.g. photo sharing through Flickr.com) must be first approved by the VITL Security Officer.

10) Unacceptable Use

Use of network, Internet, and e-mail services at VITL shall comply with all applicable law, all applicable VITL policy, and all VITL contracts. Employees must not use the Internet and e-mail for purposes that are illegal, immoral, unethical, harmful to the company, or nonproductive. The use of programs or connection to the Internet that compromises the privacy of users and/or damages the integrity of VITL computer system, data, or programs is forbidden. Examples of unacceptable use are:

• Illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, forgery, impersonation, and computer tampering (e.g., spreading viruses).

• Internet and e-mail services may not be used in any way that violates VITL policies, rules or administrative orders. Use of email services in a manner which is not consistent with the mission and educational purpose of VITL, misrepresents VITL or violates any VITL policy, is prohibited.

• Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive.

• Opening or forwarding any email attachments (executable files) from unknown sources and/or that may contain viruses.

• Sending or forwarding chain letters of other mass mailing communications.

• Downloading any data that is inappropriate or not VITL-specifically approved

• Sending communications anonymously

• Conducting a personal business using company resources.

• Product or business advertisements, and/or sales of goods for personal gain.

• Lobbying for a cause; political, religious, or otherwise.

• Communication containing ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on their race, sex, national origin, sexual orientation, age, disability, or religious or political beliefs

• Transmitting any content that is obscene, offensive, threatening, harassing, or fraudulent.

The following are among the prohibited activities:

• Crashing an information system. Deliberately crashing an information system is strictly prohibited unless specifically part of some VITL business function like system testing. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

• Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.

• Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer (“P2P”) or other malicious code into an information system.
Exception: Authorized information system support personnel, or others authorized by VITL Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
• Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. VITL has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
• Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on VITL computers must be approved by VITL.
• Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by VITL is strictly prohibited.

2.3 The Internet and e-Mail

Internet access is provided for VITL users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by VITL should be used judiciously. While seemingly trivial to a single user, the company-wide use of non-business Internet resources can consume a significant amount of Internet bandwidth, which is therefore not available for business uses.

As a productivity enhancement tool, VITL encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by VITL-owned communication software are considered the property of VITL – not the property of individual users. Consequently, this policy applies to all VITL employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

VITL provides resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services, which are intended for business purposes. However, limited personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:
    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of VITL information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.

c) Commercial use – Use of VITL information resources for personal or commercial profit is strictly prohibited.
d) Political Activities – All political activities are strictly prohibited on VITL premises. VITL encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using VITL assets or resources.
e) Harassment – VITL strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, VITL prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is NOT the policy of VITL to monitor the content of any electronic communication, VITL is responsible for servicing and protecting VITL's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

VITL reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as VITL policies.

Employees are reminded that VITL electronic communications systems are not encrypted by default. Email is subject to the Confidentiality policy and therefore should include only minimal confidential data. If confidential information must be sent over the Internet by electronic communications systems, encryption or similar technologies to protect the data (including authentication of the receiving party) must be employed. See the Security Officer or designee if assistance is needed to meet this requirement.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

2.4 Laptops, Portable Devices, and Removable Media

It is the responsibility of any staff member who is using PHI outside of VITL offices or connecting to the organizational network with a laptop, portable USB-based memory device, or via a personal digital assistant, smart phone, or other device to ensure that all components of his/her connection remain as secure as his/her network access within the office and to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied. Employees must take proper care to protect laptops, portable devices, and removable media from loss or damage, and must protect the confidentiality of any personal or private information held on such devices.

The System Administrator reserves the right to refuse, by physical and non-physical means, the ability to connect portable devices to corporate and corporate-connected infrastructure. The System Administrator will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and patients at risk.

The System Administrator reserves the right to audit any portable device used for VITL business to ensure that it continues to conform to this policy. The System Administrator will deny network access to any laptop that has not been properly configured.

The user of the portable device is responsible for physical and network security of the device whether they are onsite, at home, or on the road.

- Users must physically secure all portable devices that are used for VITL interests, whether personally- or company-owned.
- Such devices must not be accessed or used by unauthorized individuals.
- When off-site, equipment must be kept secure in locked buildings or vehicles and kept out of sight when unattended. If traveling by public carrier, equipment must be kept with the employee and cannot be checked as baggage.
- No sensitive data should ever be stored on portable media unless the data is maintained in an encrypted format.
- Do not connect VITL devices to non-VITL workstations except in the case of trusted VITL partners. Example: Data provided to auditors via USB drive during the course of an audit.
- Do not connect non-VITL devices to VITL workstations except in the case of trusted VITL partners.

Power-on passwords and encryption of stored personal or private information must be used, as possible and practicable. Passwords and other confidential data are not to be stored on portable devices or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and related flash-based supplemental storage media) unless encrypted using a

method approved by the Security Officer. NOTE THAT IF A PORTABLE DEVICE IS LOST OR STOLEN, INFORMATION NOT ENCRYPTED USING AN APPROVED METHOD IS CONSIDERED TO BE BREACHED AND MUST BE REPORTED UNDER STATE AND FEDERAL LAWS. THIS IS A VERY SERIOUS, EXPENSIVE PROCESS; ALL USERS MUST BE IN COMPLIANCE WITH ENCRYPTION REQUIREMENTS OR FACE SERIOUS DISCIPLINARY ACTION.

Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all VITL personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete. VITL network resources may be accessed only via an approved VPN connection, using approved hardware and software. Disabling a virus scanner or firewall is reason for termination.

The user of a portable device (whether VITL-owned or used for VITL data) agrees to immediately report to his/her director and VITL's Privacy and Security Officer the loss of any portable device, or any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

No matter what location, always lock the screen before walking away from a workstation. The data on the screen may be protected by HIPAA or may contain confidential information.

When an employee leaves VITL, all portable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to HIPAA requirements.

When no longer in productive use, all VITL laptops, workstations, portable devices or media, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All portable media must be returned to the Security Officer or appropriate personnel for data erasure when no longer in use.

2.5 Remote Access or Use of Information

Any personal or private information being accessed remotely shall be protected from improper access or modification in transit through encryption approved by the Security Officer and shall be subject to other sections of this policy. Strong cryptography and encryption techniques must be used to safeguard sensitive personal or private information during transmission over public networks. Personal or private information may not be sent via unencrypted e-mail. INFORMATION NOT ENCRYPTED USING AN APPROVED METHOD MAY BE CONSIDERED TO BE BREACHED AND REPORTABLE UNDER STATE AND FEDERAL LAWS. THIS IS A VERY SERIOUS, EXPENSIVE PROCESS; ALL USERS MUST BE IN COMPLIANCE WITH ENCRYPTION REQUIREMENTS OR FACE SERIOUS DISCIPLINARY ACTION.

Confidential information may not be maintained outside of VITL facilities without a valid business reason and approval by the employee's supervisor, and any such stored confidential information must be encrypted by a means that is approved by the Security Officer.

Computers used outside of VITL facilities by employees to access, store, or transmit confidential information must be used solely by the employee (not shared with other household members and not a public Internet access point) and must be configured with up-to-date virus protection, security patches, and firewall software. Independent verification of configuration of computers used by employees outside of VITL facilities may be requested by the Security Officer.

Wireless networks outside of VITL facilities used by employees for the transmission of any confidential information must be configured securely according to best practices so that any transmissions over the network are encrypted and access to the configuration of the network is protected. Independent verification of configuration of wireless networks used outside of VITL facilities may be requested by the Security Officer.

Any access or use of VITL information outside of VITL offices must be performed in an area and in such a way that onlookers and passers-by cannot see any PHI on the devices used.

Remote Data Security Protection

Data Backup: Use established backup procedures to preserve critical data – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate VITL personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to VITL: Transferring of data to VITL requires the use of an approved secure connection to ensure the confidentiality of the data being transmitted. Do not circumvent established procedures nor create your own method when transferring data to VITL.

External System Access: If you require access to an external system, contact your supervisor or department head. The Security Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-VITL Networks: Extreme care must be taken when connecting VITL equipment to a home or public network. Although VITL actively monitors its security status and maintains organization-wide protection policies to protect the data within all contracts, VITL has no ability to monitor or control the security procedures on non-VITL networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not

been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records displaying PHI around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside VITL: All external transfers of patient data must be associated with an official contract or appropriate Business Associate Agreement.

2.6 Information Security Incidents

All users must immediately report to their directors and VITL's Computer Security Incident Response Team (CSIRT) any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc., according to the **Information Security Incident Response Policy**. Incidents will be investigated and actions may be taken to prevent future similar incidents based on the results if the investigation. Persons reporting legitimate incidents will not be retaliated against by VITL or its management.

An incident may be any event that affects the confidentiality, integrity, or availability of personal or private information based in any electronic systems or networks. Reportable incidents may include known or suspected breaches of security, unusually slow or improper workstation or system operation, unusual or repeated system crashes, or other out-of-the-ordinary workstation or system behaviors.

Examples of information security incidents may include (but are not limited to):

- An employee or Contractor viewing Protected Information in a database the individual is not authorized to access under VITL policy.
- An employee or Contractor downloading software which is not permitted under the Information System User Policy
- Intrusion of a VITL system within which Patient Health Information resides by an unauthorized third party ("hacker"). This scenario requires the operant assumption that there was a probable loss of confidential patient information.
- An unauthorized third party ("hacker") using a falsified user name and password to gain access to Information Systems.
- An unauthorized third party seeking Information System access control or other information by pretending to be an individual authorized to obtain such information ("Social Engineering").
- An unauthorized third party ("hacker") who acquires access to any VITL system or device by any means or method.

- An email or other communication purporting to be from an authorized party seeking Protected Information or information potentially useful in obtaining Information System access ("phishing").
- A software virus or worm ("malware") interfering with the functioning of personal computers which are part of an Information System and which may also result in a compromise of the infected system by a remote “hacker”, etc.

2.7 Intimidating or Retaliatory Acts

Any individual who provides assistance with HIPAA compliance and any HHS officials or investigations shall not be subjected to intimidation or retaliatory acts by VITL, per HIPAA Privacy Rule §164.530(g).

2.8 Confidentiality Agreement

Users of VITL information resources shall sign, as a condition for employment, a confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand and acknowledge that, if I breach any provision of this agreement, I may be subject to civil or criminal liability and/or disciplinary action consistent with applicable VITL policies, bargaining contracts and VITL processes.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing VITL information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

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 Security Management Process Policy

Information Security Incident Response Policy

HIPAA Privacy, Security, and Breach Notification Rules

Payment Card Industry Data Security Standard

Policy Review & Approval

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

Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 3

Policy Title: Information System Access Control Policy

January 26, 2016

IDENT	INFOSEC3
Type of Document:	Policy
Type of Policy:	Corporate
Sponsor's Dept:	IT
Title of Sponsor:	CTO
Title of Approving Official:	CEO
Date Released (Published):	01/28/16
Next Review Date:	01/01/16

Information System Access Control

Purpose

The purpose of the Information System Access Control Policy is to ensure that all users have only the appropriate access to electronic PHI, and that unnecessary or inappropriate access to electronic PHI is prevented, consistent with the requirements of the HIPAA Privacy Rule, and HIPAA Security Rule §164.308(a)(4), 310, and 312.

This document, along with guidelines/operating manuals, may be used to train new personnel in the defined operations, and used to ensure conformity among personnel performing those operations.

Scope

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, 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 the task being performed – not just to specific departments or job titles.

Policy

VITL shall require the implementation of technical procedures where practicable to limit access to electronic protected health information (PHI) and payment cardholder information to only those persons or software programs that have been properly granted access rights, and to ensure that the granting or modification of access to electronic personal and private information is consistent with the requirements of the HIPAA regulations and other applicable information security regulations. The policy and procedures include the sections following:

3.1. Authentication and Access

3.2. Perimeter Security

3.3. Data Encryption

3.4. Data Integrity

3.5. Physical Access Controls

3.6. Media Management

3.7. Media and Equipment Disposal

Also see the **Information System User Policy** for policy regarding password management (in the sections on **Gaining Access to Information Systems** and **Remote Access or Use of Information.)**

3.1 Authentication and Access

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

VITL shall institute documented procedures for granting and modifying access to electronic PHI and other confidential information to authorized persons within the bounds of the “minimum necessary” requirements of the HIPAA Privacy Rule and other applicable regulations, including HIPAA Security Rule §164.312(a) and §164.312(d). The organization shall institute procedures to establish, document, review, and modify a user’s right of access to a workstation, transaction, program, process or other mechanism.

Procedures will be developed for managing Network Connectivity, including Remote Access to and from VITL, Firewalls, Wireless Access Points, and Use of Personal Devices.

Access to Information

Rules for access to resources (including internal and external telecommunications and networks) are established by the information/application owner or manager responsible for the resources. Access is granted only by formal request. This request can only be initiated by the appropriate department head, and must be approved by the department head and the Security Officer or appropriate personnel.

Only VITL staff and contractors with a legitimate need will receive a user ID to access VITL systems. All requests for access by a non-employee (e.g., contractors, partners, etc.) shall be made by a VITL staff member by requesting access from the Security Officer.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the VITL network only upon the written approval of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Individual users shall have unique login IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Procedures shall be established to verify the identity of the person or entity seeking access to confidential information. Persons may be authenticated by the use of passwords, cards, tokens, keys, biometrics, or other means of personal identification approved by the Security Officer.

The login ID is locked or revoked in accordance with InfoSec policy 1 section 2.1.3.

Procedures shall be developed, if necessary, to ensure that electronic confidential information shall be accessible by approved personnel in an emergency situation in which normal access is not available.

Passwords

The Security Officer shall manage the process of password provision for all systems at VITL.

User IDs and passwords are required in order to gain access to all VITL networks and workstations. All passwords are restricted by a corporate-wide password policy (InfoSec policy 1 section 2.1.3).

Passwords shall not be shared with any party, must be kept confidential, and may not be written down on paper unless kept under lock and key, or stored within a file or database unless secured by encryption. Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

Reviews of Access Lists

No less than annually, the Security Officer shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect patient data.

All user login IDs are audited at least twice yearly and all inactive login IDs are revoked. The VITL Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

Termination of Access

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the Security Officer. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the Security Officer of employee's last scheduled work day so that their user

account(s) can be configured to expire. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as VITL equipment and property is returned to VITL prior to the employee leaving VITL on their final day of employment.

In the event of a termination or resignation of staff:

a) Supervisors must immediately notify Human Resources of any departures or terminations.

b) Supervisors must immediately notify the Security Officer of the termination of any user.

c) Human Resources will distribute a list of employee terminations to the Security Officer in advance of the departure of the employee, or immediately if advance notice is not possible.

d) According to HIPAA Security Rule §164.308(a)(3) and (4), workforce members whose right to access electronic confidential information is terminated or restricted shall have physical and/or system access privileges removed and shall surrender any keys, tokens, or other objects that allow access. In addition, combination locks and alarm system codes known by such workforce members shall have their combinations or access codes changed, according to a defined procedure.

e) Procedures shall identify the parties to be involved in termination activities, the steps to be taken in the process of termination or restriction of access, and the timing of termination activities, such as coordination of notice of termination with removal of access to systems and networks.

f) The manager and involved supervisors will immediately notify the Security Officer of any terminations or restrictions of access, so that access can be modified promptly. Such notifications must be followed up in writing or email to the Security Officer.

3.2 Perimeter Security

Perimeter security controls, such as firewalls, shall be used to protect the electronic confidential information held within VITL systems and allow access across the perimeter where appropriate, as required by HIPAA Security Rule §164.312(a) and §164.312(e). Such controls are required in order to allow permitted information flows and prohibit unauthorized or improper information flows into and out of the organization's computing networks and systems. In addition, this policy includes requirements for protection of the perimeter and the systems contained within the perimeter via anti-malware (anti-virus, anti-spam, and anti-keylogging) systems

A perimeter firewall is in place to separate VITL's internal networks from the public Internet and the DMZ. Only necessary protocols and their associated ports are open on the firewall. Refer to the network diagram for information on the logical layout of the network.

Any changes to the firewall configuration must be approved by the Security Officer. Change requests for the firewall must follow a defined, documented process.

Anti-virus software is installed on all VITL personal computers and servers. Virus update patterns are updated daily on the VITL servers and workstations. Virus update engines and data

files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date. Procedures are defined for implementation of anti-virus tools.

All data and program files that have been electronically transmitted to a VITL computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate VITL personnel for instructions for scanning files for viruses.

Every CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a VITL computer or network.

Computers shall never be "booted" from a CD-ROM, DVD or USB device received from an outside source. Users shall always remove any CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the CD-ROM, DVD or USB device is not "bootable."

VITL shall utilize appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.

3.3 Data Encryption

Where indicated by a formal Risk Analysis or as required under applicable regulations, confidential information at rest shall be encrypted to prevent access or use by unauthorized personnel, as required by HIPAA Security Rule §164.312(a)(1)(iv). Confidential information residing on easily movable devices such as laptops, smart phones, memory sticks and other portable electronic devices must be encrypted. In order to avoid reportable information security breaches under the HIPAA Breach Notification regulations at §164.400 *et seq.*, any encryption used must meet the requirements specified in guidance provided by the US Department of Health and Human Services (HHS), available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html .

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, VITL shall establish the criteria in conjunction with the Security Officer or appropriate personnel. VITL employs several methods of secure data transmission.

Confidential information may not be sent from a workstation by any method except as part of an approved business process. Electronically or physically transmitted personal or private information must be protected from unauthorized access or modification, as required by HIPAA Security Rule §164.312(e), and the HIPAA Security Rule Guidance on the Remote Access and Use of PHI issued December 28, 2006, available at http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal.pdf

Procedures shall be defined for the means to implement encryption to secure PHI and other private information at rest and in transit.

3.4 Data Integrity

VITL shall implement and maintain appropriate electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner, to protect VITL's PHI from improper alteration or destruction. Integrity is assured through the use of strict access controls including authentication and authorization, encryption, use of anti-malware tools, good software deployment and change management procedures, and reviews and audits of security and system activity. Thorough backup and recovery procedures protect against the loss of PHI.

3.5 Physical Access Controls

It is the policy of VITL to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, VITL strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it.

It is VITL's commitment to provide the appropriate resources and guidance to ensure that all physical access to workstations and systems is approved, tracked, monitored and reviewed to support the security of the overall computing environment.

VITL shall establish procedures to limit or enable, as appropriate, physical access to files, systems, and devices containing personal or private information, as required by HIPAA Security Rule §164.310(a), §164.310(c), and §164.310(d). Areas and facilities housing network and/or computer server systems, network switches, and patch panels shall be secured so that such devices contained therein are inaccessible to unauthorized personnel.

Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate business or healthcare reason to access that information, to the extent practicable.

The physical security of the premises will be reviewed regularly, and appropriate alarm and/or surveillance technology will be utilized, both for monitoring entry and exit during business hours, and for securing the premises after hours.

Any unrecognized person in a restricted office location should be challenged as to their right to be there. In some situations, non-VITL personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.

Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

3.6 Media Management

Media included within the scope of this policy includes, but is not limited to, hard drives, solid state memory, flash drives, smart phones, digital storage cards, DVDs, CD-ROMs, and USB memory devices.

The purpose of this policy is to guide VITL employees/contractors in the proper use of portable media when a legitimate business requirement exists to transfer data to and from VITL networks. Every workstation or server that has been used by either VITL employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from portable media to protect sensitive VITL data. Since portable media by their very design are easily lost, care and protection of these devices must be addressed.

The use of portable media in various formats is common practice within VITL. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of VITL networks. Portable media received from an external source could potentially pose a threat to VITL networks. Sensitive data includes all human resource data, financial data, VITL proprietary information, and PHI protected by HIPAA.

There shall be procedures to record the movement of hardware and electronic media containing electronic confidential information into, out of, and within organization facilities, to ensure that all devices used by VITL to access or retain electronic confidential information are known and locatable, and that any portable hardware or media retaining electronic confidential information are in the care of known responsible parties.

Procedures shall include Physical Security of Media, Distribution and Movement of Media, Inventory of Media, Transportation Offsite, and Accountability.

3.7 Media and Equipment Disposal

Media included within the scope of this policy includes, but is not limited to, hard drives, solid state memory, flash drives, smart phones, digital storage cards, DVDs, CD-ROMs, and USB memory devices.

The disposal or reuse for another purpose of any hardware or electronic media containing confidential information, including all forms and types, such as computers, servers, portable devices, copiers, and multifunction machines, shall include the destruction of any such confidential information before ultimate disposal or reallocation to a new use outside of VITL. The destruction of electronic confidential information shall be carried out by physical or electronic means that ensures the actual destruction of the information.

In order to avoid reportable information security breaches under the HIPAA Breach Notification regulations at §164.400 *et seq.*, any and all disposal methods used must meet the requirements specified in guidance provided by the US Department of Health and Human Services (HHS),

available at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

All paper which contains sensitive information that is no longer needed must be shredded before being disposed of. All employees working from home, or other non-VITL work environment, MUST have direct access to a shredder.

All electronic media being disposed of must be sanitized or destroyed in accordance with HIPAA-compliant procedures. Do not throw any media containing sensitive, protected information in the trash. Return all portable media to your supervisor.

As the older VITL computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- For spare parts.
- On an emergency replacement basis.
- For testing new software.
- As backups for other production equipment.
- To provide a second machine for personnel who travel on a regular basis.
- To provide a second machine for personnel who often work from home.
- On occasion, VITL may sell a machine to an employee after wiping it of all data and resetting it to factory defaults.

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Procedures shall be developed for the Destruction of Media.

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 User Policy

Information Security Management Process Policy

Information Security Incident Response Policy

HIPAA Privacy, Security, and Breach Notification Rules

Payment Card Industry Data Security Standard

Policy Review and Approval

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

Michael L. Gagnon	
Reviewed by: Privacy and Security Officer	January 26, 2016 Date
Approved by: CEO	Date

Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 4

Policy Title: Information Security Incident Response

January 26, 2016

IDENT	INFOSEC4
Type of Document:	Policy
Type of Policy:	Corporate
Sponsor's Dept:	Security
Title of Sponsor:	Security Officer
Title of Approving Official:	Security Officer
Date Released (Published):	1/26/16
Next Review Date:	1/1/17

Information Security Incident Response

Purpose

The purpose of the Information Security Incident Response Policy is to help assure the confidentiality, integrity, and availability of Protected Information held by VITL, including but not limited to protected health information as defined by Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA), and assure the operational integrity of VITL's information systems, through the definition of a process for recognizing, reporting, and responding to information security incidents.

Information Security Incident Response Policy provides the guidance necessary to evaluate a situation in the face of unusual circumstances in order to determine if an information security incident is or has been taking place, and provide the steps to follow to handle any incidents properly, including the proper handling of any breaches of information security.

This document, along with guidelines/operating manuals, may be used to train new personnel in the defined operations, and used to ensure conformity among personnel performing those operations. Every policy and procedure document and its content are designed to be consistent with overall Corporate VITL management objectives.

Scope

The scope of this policy is limited to the confidential electronic data (PHI, credit card data, or other personal information under state and federal laws) that is handled, stored and/ or produced by VITL. This policy applies to employees, clients, vendors, and contractors including all personnel affiliated with third parties.

Policy

VITL shall have in place 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 and breaches may be reported and handled promptly, using an orderly process known to all workforce members, according to HIPAA Security Rule §164.308(a)(6).

Procedures shall identify:

1. How to determine what qualifies as an “incident” (including the indication of alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems)
2. How to report incidents (including the designation of to whom incidents and alerts must be reported on a 24/7 basis)
3. The steps to take in investigating
4. The roles and responsibilities of the response team
5. The steps to be taken and information to be included when documenting incidents
6. The steps to be taken to mitigate the effects of incidents (where possible and/or allowed by law)
7. Steps to be taken to provide business recovery and continuity, including the use of adequate backup procedures
8. Who may release information about the incident and the procedures for doing so
9. To which entities incidents involving breaches must be reported, such as payment card information Acquirers and card associations, consumers, and relevant Local, State, or Federal agencies
10. Who shall be authorized to release a system following investigation?
11. How a follow-up analysis should be performed and who should participate.

Information Security Incident Response Team members shall be provided appropriate training.

The incident response plan shall be reviewed regularly, tested at least annually, and modified as appropriate according to lessons learned and to incorporate current security best practices.

Reporting Security Incidents

1) Any incident that affects physical facilities, computer systems, network services or the confidentiality, integrity, or availability of personal or private information based in any electronic systems or networks shall be reported to members of the Information Security Incident Response Team and the Security Officer. The person receiving the report shall document the particulars that are reported and immediately notify the Information Security Incident Response Team (ISIRT) leader, and the Security Officer.

2) Reportable incidents may include known or suspected breaches of security, unusually slow or improper workstation or system operation, unusual or repeated system crashes, or other out-of-the-ordinary workstation or system behaviors. Examples of information security incidents may include (but are not limited to):

- An employee or Contractor viewing Protected Information in a system or database that the individual is not authorized to access under VITL policy.
- An employee or Contractor downloading software which is not permitted under the Information System User Policy
- Intrusion of a VITL system by an unauthorized third party (“hacker”) within which Patient Health Information resides. This scenario requires the operant assumption that there was a probable loss of confidential patient information.
- An unauthorized third party ("hacker") using a falsified user name and password to gain access to Information Systems.

• An unauthorized third party seeking Information System access control or other information by pretending to be an individual authorized to obtain such information ("Social Engineering").

• An unauthorized third party ("hacker") who acquires access to any VITL system or device by any means or method.

• An email or other communication purporting to be from an authorized party seeking Protected Information or information potentially useful in obtaining Information System access ("phishing").

• A software virus or worm ("malware") interfering with the functioning of personal computers which are part of an Information System and which may also result in a compromise of the infected system by a remote “hacker”, etc.

3) The ISIRT team will review the initial report to determine if this is a new incident, new information about an existing incident, or some other kind of service or information request. Information about new or existing incidents will be retained and acted upon as appropriate.

Security Incident Prioritization

The ISIRT leader will determine the priority of the incident according to its impact:

1) Critical: A Critical level event is an event that can cause significant damage, corruption, or loss (compromise) of confidential, critical and/or strategic organization and patient information. The event can result in potential damage and liability to the organization and to its public image and may degrade client and community confidence concerning its services. Risks of critical incidents include exposure to criminal penalties; exposure to major financial losses; potential threat to life, health or public safety; major damage to reputation or operations. Examples of critical incidents may include:

• Known or potential theft or loss of confidential VITL or Protected Health Information

• Disruption of or denial of service attacks of Critical Systems, including clinical decision-support applications, financial reporting systems, and electronic medical records information

• Unauthorized access to security administrator applications or information

• All unauthorized computer intrusions, malware infections, any attacks against the IT infrastructure, etc.

2) Moderate: A Moderate level event is an event that may cause damage, corruption, or loss of replaceable information without compromise or may have a moderate impact on the organizations operations or reputation or may result in legal liability to the organization. Risks of moderate level incidents include exposure to minor financial losses or minor damage to reputation or operations. Examples of moderate level events may:

• An employee viewing the confidential information of a fellow employee without authorization

• A “hacked” VITL system is used in attacks on other non-VITL systems and organizations

• A worm causes fraudulent mass emailing from infected systems

- A website is defaced
- Misuse or abuse of authorized access
- Accidental intrusion
- Confined virus infection
- Unauthorized access
- Unusual system performance or behavior
- System crashes
- Installation of unauthorized software
- Unexplained access privilege changes
- Unusual after-hour activities, etc.

3) Minor: A Minor level event is an event that causes inconvenience, aggravation, and/or minor costs associated with recovery, unintentional actions at the user or administrator level, or unintentional damage or minor loss of recoverable information. The event will have little, if any, material impact on the organization's operations or reputation. Risks of minor level events include exposure to minimal financial losses, or minimal or no damage to reputation or operations. Examples of minor level events may include:

- A "Phishing" email is received
- An employee accesses prohibited websites
- Sharing of passwords that does not result in unauthorized access
- Policy or procedural violations, etc.

4) Suspicious Activities: Suspicious Activities include observations that indicate possibility of past, current or threatened security incident, but that may be consistent with authorized or non-harmful activities. Examples of Suspicious Activities include:

- Access logs show limited number of unsuccessful attempts by authorized user
- An employee loiters near restricted work area beyond his authorization
- A user returns to workstation to find new application started without his/her authorization, etc.

Response to Security Incident Reports

1) All Critical incidents must be investigated and documented as incidents. Moderate or Minor incidents will be minimally investigated and documented as incidents but will receive full investigation and documentation if it is deemed that the incident is unusual and can be learned from so that similar incidents may be prevented in the future. Suspicious Activity incidents do not need detailed investigation and documentation as security incidents. However, Suspicious Activity incidents may be elevated to a higher level by the ISIRT team, depending on the incident.

2) The ISIRT leader will notify appropriate persons, such as the Security Officer, or CEO.

3) Information concerning a computer security incident shall be considered confidential and may not be released to individuals not directly involved with the incident and any investigation or response without permission from the Security Officer, or CEO.

Public Response to a Security Incident

1) The ISIRT leader will notify the CEO in cases where an incident may have repercussions that need public announcement or response to inquiry by the public, a staff member, a resident, a client, an individual whose information was held by a client, or a family member of an individual whose information was held by a client.

2) Any announcements to the public or responses to questions from the public about information security incidents shall be made only by the CEO or his designee. The person making such announcements and responses will be advised by the ISIRT leader.

The Information Security Incident Response Team (ISIRT)

1) The ISIRT shall be responsible for responding to all Critical and/or otherwise material security incidents, and shall develop procedures and delegate responsibilities for responding to lesser priority incidents.

2) The ISIRT shall include the Security Analyst, the Security Officer, the Human Resources Manager and the CEO. The ISIRT will be chaired by the Security Officer.

3) The ISIRT is responsible for developing and maintaining incident response procedures, and for leading and coordinating responses to incidents.

4) The ISIRT shall maintain relationships with and contact information for law enforcement agencies, Internet service providers, third party contractors, outside legal counsel, and any other technology experts deemed appropriate or helpful.

Investigating Security Incidents

1) Security Incident investigations shall be managed by the ISIRT leader, who shall call in assistance from other VITL staff and consultants as necessary to understand the incident, terminate the incident, mitigate any negative effects of an incident, and document the incident and its handling.

2) The owners of any accounts compromised will be notified appropriately so as to maintain confidentiality of the incident pending review by the ISIRT. Once forensic evidence is preserved and review is made possible by the ISIRT, account owners should change their passwords and scrutinize the integrity of the information in affected accounts, providing relevant information about the existence of any security violations to the ISIRT leader or other investigating officer.

3) Any workstations or systems affected by a Security Incident shall be removed from service if it is deemed that doing so will help preserve evidence that may assist in determining the cause or source of the incident, or would help prevent any escalation of the incident. The ISIRT team will refer to detailed incident response procedures and act appropriately.

4) Workstations or systems will be examined as appropriate to determine not only the cause of an incident and parties involved, but also what actions may be taken in the future to prevent similar incidents. Usage logs and system access audit tools, as well as any other appropriate forensic tools or activities, will be used as possible and appropriate to provide relevant information during investigation.

5) Information gathered in the investigation of security incidents shall be developed and preserved to the greatest extent possible as potential evidence admissible in court in the event it is needed in legal proceedings. Individuals and entities which may be liable for harm caused by the incident shall be identified.

6) The ISIRT leader will contact other appropriate responsible individuals or departments, as appropriate in the course of the investigation.

7) In investigating an incident, the investigators shall endeavor to get the global picture of all the events that occurred coincident to the incident, and distinguish observations from any assumptions, hearsay, or hypothesis about the incident.

8) Security incidents should be categorized as one or more of the following:

- Denial of Service – an event that prevents or impairs the authorized use of networks, systems, or applications
- Malicious Code – a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- Unauthorized Access – logical or physical access without permission to a network, system, application, data, or other resource
- Inappropriate Usage – a person violates acceptable computing policies
- Breach – a breach of EPHI on the VITL network or VHIE
- Phishing/Social Engineering – an unauthorized attempt by someone masquerading as a legitimate party to elicit information from a staff member that may be used in attempts to compromise the security of systems or accounts.

9) If an incident appears to have been related to illegal activity, or is a security breach of significant scope, the following should be notified by the Security Officer, or CEO:

- Vermont State Police
- FBI
- US Secret Service.

10) In cases where civil or criminal charges may be involved, the ISIRT leader will work with the Security Officer, CEO, and legal counsel to take any legal action required.

11) The Human Resources department should be involved in any incident investigation that may involve improper activities by employees. Human Resources will be notified by the Security Officer, or CEO.

12) The ISIRT shall develop additional procedures to define more detailed steps to be taken in the investigation of and response to various types and priorities of incidents (including response times), and to define the roles of various ISIRT team members during an investigation or response.

Reporting Breaches of Confidential Information

1) Per the HIPAA Breach Notification Rule §164.400 *et seq.*, all breaches of protected health information (PHI) must be reported promptly to the individual, unless A) the PHI is encrypted using processes meeting the requirements of guidance published by HHS, or failing that, B) the disclosure is one of the three exceptions to the definition of a breach, as described by HHS, at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html or, failing that, C) a risk assessment determines that there is a low probability of disclosure of PHI.

2) If a disclosure that may be a breach is unencrypted by HHS standards and does not meet one of the three exceptions for reporting as a breach, the disclosure must be treated as a breach unless a risk assessment indicates there is a low probability of disclosure of the PHI involved. In order to determine if there is a low probability of disclosure, the risk assessment must consider four factors: 1) The nature of the information (how detailed, how much identifying information, sensitivity, including the potential for "adverse impact" to the individual?), 2) to whom it was released (was it another healthcare provider?), 3) whether or not it was actually accessed, used, or disclosed (was it discarded without reading?), and how the incident was mitigated (are there assurances that the information disclosed cannot be further used, disclosed, or retained?).

3) VITL will notify the Participating Health Care Provider(s) whose patient information was subject to the unauthorized acquisition, access, use or disclosure no later than ten (10) business days following the discovery of the Breach. Such notification will include the time and date of the Breach discovery and the identification of each individual whose PHI is involved.

4) In cases involving a Participating Health Care Provider, the Participating Health Care Provider, and/or VITL at the Participating Health Care Provider's request, shall notify, without unreasonable delay and in no case later than 60 days from the discovery of the Breach, each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the Breach. Notification shall be provided in writing to each affected individual or next of kin if deceased, by first class mail, or, if specified by the individual, by electronic mail. If the affected Participating Health Care Provider or VITL

concludes that there may be imminent misuse of an individual's PHI, notice shall also be provided by telephone contact or other means, as appropriate.

In the case in which there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual, electronic) notification to the individual, a substitute form of notice shall be provided. In the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, the involved Participating Health Care Provider will provide notice by arranging for a conspicuous posting on the home pages of the Web site, if available, of the Participating Health Care Provider involved and of VITL and/or notice in major print or broadcast media where the individuals affected by the breach likely reside. Such a notice in media or web postings will include a toll-free phone number to either the Participating Health Care Provider and/or VITL, as mutually agreed upon, where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

5) Breaches of PHI involving more than 500 individuals must be reported to HHS at the same time the breach is reported to the individual. Breaches involving fewer than 500 individuals must be reported to HHS within 60 days of the end of the calendar year in which they occurred.

6) Breaches of PHI must be reported to individuals, HHS, and the public according to the requirements of HIPAA Breach Notification Rule §164.400 *et seq.* and any other applicable regulation. See http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html for details.

7) As of January 1, 2007, Vermont Act 162, subchapter 2 requires notification of a Vermont resident if there has been unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of their personal information.

8) "Personal Information" under this Vermont law is first name or initial, and last name, and one or more of the following in unprotected form: (1) Social Security Number, (2) Driver's license number or non-driver ID card number, or (3) Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account, and does not include publicly available information lawfully made available to the general public from federal, state, or local government records.

9) Notice under the Vermont law must be given in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of any law enforcement agency.

10) Notice under Vermont law must meet the requirements of the law and any related regulations put forth by the Vermont Department of Financial Regulation, including providing a Toll-Free Telephone Number for contact, a description of what happened in general terms, what kind of information was involved, what's been done to mitigate the breach, and advice for consumers as to how they can mitigate damage from the breach. Notice may be waived by the

Vermont Department of Financial Regulation if the client can show that misuse of the information is not reasonably possible.

11) Any breaches that may be reportable under law are critical incidents that require involvement by VITL counsel and senior management to ensure that the Federal and State laws are followed correctly in the provision of various notices and reports to agencies. Note that Breaches of individual information may also be subject to the laws of the state of residence of the individual outside of Vermont.

12) If a law enforcement official determines that a notification required under this Policy would impede a criminal investigation or cause damage to national security, such notification shall be delayed in the same manner as provided under section 164.412 of title 45, Code of Federal Regulations.

Documenting Security Incidents

1) Security Incidents, breaches, and any risk assessments performed to determine whether or not an incident is a reportable breach will be documented according to the Documentation Procedures identified in the **Information Security Management Process Policy**. Incidents must be included in the analysis conducted as part of any Compliance Evaluation Procedures or Usage Audit and Activity Review Procedures, as appropriate.

2) Information gathered in the investigation of Security Incidents shall be developed and preserved to the greatest extent possible as potential evidence admissible in court in case it is needed in legal proceedings. Whenever possible, any individuals or entities that may be liable for harm caused by the incident shall be identified, and the ISIRT may seek to have damages quantified for possible use in administrative or legal proceedings.

Enforcement

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

Mitigation, Corrective Action and Sanctions

Upon receiving a report or being notified of a Reportable Event involving a Participating Health Care Provider, VITL will work with the Participating Health Care Provider(s) to develop a mutually acceptable mitigation and correction plan.

If it is determined by VITL's Security Officer that a Reportable Event or a Breach has occurred involving the VHIE, VITL may impose on the offender one or more sanctions, consistent with the violation. Depending on the circumstances, sanctions may be on an individual level or an organizational level. Sanctions for an unintentional violation may include, but are not limited to: verbal warnings; written warnings; suspension of VHIE access privileges; and revocation of VHIE access privileges. Sanctions for an intentional violation may include, but are not limited to: immediate suspension of VHIE access; revocation of VHIE access; a complaint filed with the violator's professional licensing board, if the violator is professionally licensed; information turned over to a prosecutor for criminal prosecution; and potential other legal action.

Appeals

Offenders may appeal sanctions to VITL. All appeals must be filed in writing, and received at VITL's business offices within 10 business days of the sanction being imposed. VITL staff will consider the appeal and make a determination of whether to continue the sanction within 10 business days of receiving the written appeal. VITL will provide the party filing the appeal with a written notice of its decision within 10 business days of making the decision. Sanctions will remain in effect while the appeal is being considered.

If the appeal is denied, and the appealing party believes there has been an error, it may file a request with VITL for an external review. Such requests must be made in writing within 30 calendar days of the appeal being denied. VITL will refer the case to an independent party, which will review the evidence and make a recommendation to VITL's board of directors, which will make the final decision.

References

Information System User Policy

Information Security Management Process Policy

Information System Access Control Policy

HIPAA Privacy, Security, and Breach Notification Rules

Payment Card Industry Data Security Standard

Policy Review & Approval

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

Michael L. Gagnon	
Reviewed by: Privacy and Security Officer	January 26, 2016 Date
Approved by: CEO	Date