Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 3

Policy Title: Information System Access Control Policy

August 13, 2018

IDENT	INFOSEC3
Type of Document:	Policy
Type of Policy:	Corporate
Sponsor's Dept:	IT
Title of Sponsor:	Security Officer
Title of Approving Official:	CEO
Date Released (Published):	08/13/18
Next Review Date:	08/13/19

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, digital documents, 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 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 InfoSec2 – Information System User policy section 2.1.3.

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

Passwords

The Security Officer shall manage the process of password provisioning 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 (InfoSec2 – Information System User policy 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 may be stored electronically, only 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 and software 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 VITL-employed contractors, at which time login IDs are revoked.

Local Administrator Access

Users who are granted Local Administrator access are limited to accessing only the laptop provisioned to them. Local Administrator accounts are setup as an elevated permission to the

default login as a form of least privilege. Users with Local Administrator accounts should not logon to windows interactively. There are exceptions for developers and administrators who have a business need to gain elevated access to systems other than their laptop.

Exceptions to the local administrator policy can be found here -- \\vitl.local\files\SHARED\Security\Group Policy\Group Policy Exceptions

Termination of Access

Upon notice of termination of an employee, whether voluntary or involuntary, the employee's supervisor or department head shall promptly notify the Security Officer. If the employee's termination is voluntary and employee provides notice, the 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, or before, 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 advanced 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 "demilitarized zone" (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 the following URL: https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.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 available at https://www.hhs.gov/hipaa/for-professionals/security/index.html

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.

VITL personnel are tasked with the following responsibilities:

- Identify, report and work to correct system flaws with subject matter experts.
- Test software and firmware updates
- Install security-relevant updates to software and hardware within reasonable timeframes
- Periodically review existing configurations for flaw remediation purposes.

VITL Information systems will be configured with malicious code protection software (anti-virus or anti-malware).

- Anti-malware software will be configured to update automatically whenever new releases are available
- Anti-malware software will be configured to scan real time information as it flows into or out of the system, in addition to periodically running full scans of all files stored on the system
- Anti-malware will be configured to alert Competitive Computing (C2) and System Administrators in the event a file is removed or quarantined.
- The System administrator, and security team will periodically review files flagged during anti-malware scanning to identify false positives, updates to the anti-malware software will be discussed to ensure information confidentiality is maintained while reducing user issues related to information availability.

The VITL network and attached systems will be monitored for potential attacks and unauthorized connections. Critical systems will be monitored through third party intrusion detection services, as well as internal audit log review. Moderate and low risk systems will

additionally be monitored by internal log review. Internal system event logs will be aggregated to a centralized logging server and authorization protections will be put in place to ensure unauthorized access to logs is blocked.

The System Administrator, Security Analyst, Security Officer, and Privacy Officer will subscribe to some form of security newsletter, alerts, advisories or directives from industry recognized sources (US-CERT, Cynergistek, SANS etc.)

VITL personnel with permissions to install software will employ hash-based integrity verification tools, when possible, to detect unauthorized changes to software.

To the extent that it is available user and administrative documentation for new systems and software shall be saved to the relevant shared drive folder.

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; at the discretion of both the Privacy and Security Officers, non-VITL personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times. Documentation of contractors who do not need to be accompanied will be represented by the Privacy and Security Officers on the check in sheet maintained at the front desk.

Employees who are working with vendors or maintenance personnel onsite are required to verify the visitor's identity; either by referring to an established list of known employees or technicians provided by the partner organization to VITL; alternatively, identity can be verified by comparing company issued ID cards against government issued ID cards. If the vendor or maintenance person providing services to VITL or VITL systems brings any tools onsite (physical or electronic) to perform their job; the tools will be examined by a VITL employee to the best of their ability prior to granting access to VITL systems or Infrastructure.

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, printers 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. In order to protect against accidental loss of portable media, all removable USB drives must be encrypted before windows will grant write access to users. There are two exceptions to the removable media encryption requirement documented here -- \\vitl.local\files\SHARED\Security\Group Policy\Group Policy Exceptions\Removable Media Encryption.docx

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, printers, 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.

To electronically destroy confidential information, a multi-pass (at least three passes) or "DoD" style wipe will be employed. To physically destroy media a third-party equipment disposal company will be contacted to provide certified destruction services. If any media storage devices owned by VITL are destroyed intentionally during the equipment disposal process without a member of the VITL Technology team physically present, a certificate of destruction including the date, time and serial number of destroyed storage device must be obtained

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: https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html

All paper that contains sensitive information and 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 if they have access to both PHI and a printer.

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

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

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.

Reviewed by: Privacy Officer	Date 8/30/18
Reviewed by: Security Officer	Date 8/29/18
Approved by: CEO	Date August 29, 2018