Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 2

Policy Title: Information System User Policy

August 13, 2018

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):	08/13/18
Next Review Date:	08/13/19

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 achieve the following:

- 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, 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

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

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 Officers are 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 so.

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 either the Privacy Officer or Security Officer. Deletions may be processed by an oral request prior to reception of the written request.

3) Password Management

Network passwords apply to Windows logins only, and 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 (unencrypted) written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a secured record of a password, 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 may 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 characters: 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 that 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 for longer than one month, without the knowledge and approval of the appropriate department leader and the Security Officer.

c) Users must immediately 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 that may transmit or retain personal or private information must be subject to the following:

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) Management 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 from a manager. 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 that requires a secure login and password. The use of a public Wi-Fi connection is only allowed, if the connection to VITL systems is made through an encrypted VPN tunnel.

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

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

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

i) 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 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 that 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 include, but are 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 shall not be permitted to store PHI on phones, tablets, or other mobile devices without the approval of the Privacy and Security Officers, if an exception is granted the mobile device must support strong encryption, and the device must be locked with a password adhering to the same requirements as section 2.1.3. 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, Security Officer, and Security Analyst reserve the rights to refuse, by physical and non-physical means, the ability to connect portable devices to corporate and corporate-connected infrastructure. The System Administrator, Security Officer, or Security Analyst will engage in such action if they feel such equipment is being used in such a way that puts the company's systems, data, users, and patients at risk.

The Security Officer reserves the right to audit any portable device used for VITL business to ensure that it continues to conform to this policy. The Security Officer or 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 and approved by the Security Officer or Privacy Officer.
    - If an exception is required, and sensitive information must be stored on encrypted portable media, it should be clearly identified and stored in a secure location when not in active use.
- Do not connect VITL devices to non-VITL workstations except in the case of trusted VITL partners. An example of acceptable use is 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.

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.

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 Incident Response Team (IRT) 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) the following:

- 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.

Reviewed by: Privacy Officer

8/28/18
Date

Reviewed by: Security Officer

8/13/18
Date

Approved by: CEO

8/13/18
Date