Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Policy Number: InfoSec 4

Policy Title: Information Security Incident Response

August 13, 2018

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

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 (PHI) as defined by Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA). This policy assures the operational integrity of VITL's information systems, through the definition of a process for recognizing, reporting, and responding to information security incidents.

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

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 the following:

1. How to determine what qualifies as an “incident” (including the indication of alerts from intrusion detection, intrusion prevention, and audit log 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 forensics acquisition hold on 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. Training could take the form of reviews of actual incidents after they are resolved, or discussions of entirely hypothetical incidents in a tabletop discussion format.

The incident response plan shall be reviewed regularly, tested at least bi-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 a member of the Incident Response Team (IRT). The person receiving the report shall document the particulars that are reported; and provide the initial report to the Privacy Officer or Security Officer for priority determination

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) the following:

- 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 that is not permitted under the Information System User Policy
- Intrusion of a VITL system by an unauthorized third party (“hacker”) within which PHI or other sensitive 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 IRT 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 Security Officer or Privacy Officer will determine the severity 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 the following:

- 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 organization's 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 include the following:

- 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
- Production 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 the following:

- 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) Interruption: An interruption event is an event that disrupts operations for a limited amount of time, with no loss of information. This classification of event must not have a material impact on the organization's operations or reputation. Examples of Interruption events may include the following:

- Inability to access a non-critical resource on a temporary basis
- A system configured for redundant operation is unavailable during failover

- A resource is unavailable during scheduled maintenance, or planned downtime.

5) 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 the following:

- 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 following the Incident Response/Disaster Recovery (IRT001) Procedure. Moderate or Minor incidents will be investigated and documented as incidents, so that similar incidents may be prevented in the future. Interruption events do not need to be documented or investigated – but will still be documented by request of the Security Officer or System Administrator, for trend analysis. Suspicious Activity incidents do not need detailed investigation and documentation as security incidents. Suspicious Activity incidents may be elevated to a higher level by any IRT team, depending on the incident.

2) The member of the IRT receiving the potential incident report will be required to notify appropriate remaining members of the IRT, in order to properly categorize and prioritize the event.

3) Information concerning a Critical or Moderate 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 CEO or an acting representative identified by the CEO, may be required to notify media outlets 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 do so with the advice of the IRT.

The Incident Response Team (IRT)

1) The IRT shall be responsible for responding to all Critical and/or otherwise material security incidents. The IRT shall develop procedures and delegate the responsibilities for responding to low priority incidents as needed.

2) The Incident Response Team shall include the following:

1. CEO
2. COO
3. Security Officer
4. Privacy Officer
5. Security Analyst
6. System Administrator
7. Director of Client Services

And may include as necessary by request:

8. System subject matter experts
9. Human resources manager

3) Each member of the IRT shall have an alternate defined, in order to fill in if the primary member is unavailable. In some cases the alternate may be an existing member of the IRT who will adopt a new role.

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

5) The IRT 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 Security Officer, 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 to maintain confidentiality of the incident pending review by the IRT. Once any required evidence is acquired and preserved, such that review is made possible by the IRT, account owners should change their passwords and scrutinize the integrity of the information in affected accounts. The relevant information from the account owners review will be provided to the IRT for examination and analysis.

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 root cause or source of the incident. Workstations and Systems shall be removed from service if it is deemed that doing so would help prevent any escalation of the incident. The IRT 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) If outside assistance is required to investigate or mitigate an incident VITL will contact our legal consultants: Primmer, Piper Eggleston & Cramer and Cybersecurity Insurance provider AIG for recommended third party forensics experts.

6) Information gathered in the investigation of security incidents shall be documented 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. Evidence and documentation shall be maintained for at least 7 years.

7) The IRT will contact other appropriate responsible individuals or departments, as needed during the course of the investigation.

8) When 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.

9) Security incidents shall be categorized as best as possible by the IRT for documentation purposes; some examples of common incident types are 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.

10) If an incident appears to have been related to illegal activity, or is classified as a security breach, the following should be notified by the Security Officer, or CEO:

- Vermont State Police
- FBI
- US Secret Service

11) In cases where civil or criminal charges may be involved, the Security Officer, CEO, and legal counsel will take any legal action required.

12) 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.

13) The IRT 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 IRT 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 five (5) 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 IRT 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 leadership will consider the appeal and decide 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
- IRT001 – Incident Response and Disaster Recovery Procedure

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.