

ID	SEC002
Type of Document:	Policy
Type of Policy:	Corporate
Sponsor's Dept:	Project Management Office
Title of Sponsor	Lauri Scharf
Title of Approving Official:	Board of Directors
Date Released (Published)	09/24/09
Next Review Date	09/23/11

SUBJECT: Information Security

PURPOSE:

The purpose of the VITL Information Security Policy is to ensure that appropriate technical, administrative, and physical safeguards are applied end-to-end in the VHIE, including VITL and participating health care providers.

DEFINITIONS

The “Vermont Health Information Exchange” (“VHIE”) shall mean the health information exchange network operated by VITL.

A “Participating Health Care Provider” shall mean a health care provider, including any health care organization meeting the definition of a health care facility as defined in 18 VSA § 9402(6), that has executed an effective VHIE Data Services and Participation Agreement with VITL.

“Protected Health Information” (“PHI”) shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR §160.103.

“Technical safeguards” shall mean “the technology and the policy and procedures for its use that protect electronic PHI and control access to it.”

POLICY

The policy draws upon industry-standard guidelines such as HIPAA Security Guidance and International Organization for Standardization (ISO) security practices. For VITL, the policy requires independent certification of security best practices at the “core” of the exchange. For Participating Health Care Providers, the policy requires that providers affirm compliance with the HIPAA Security Rule, and recommends a risk assessment process based on HIPAA requirements that allows providers to demonstrate the application of specific safeguards most appropriate to their size and function. End-to-end compliance with security practices is also enhanced by VITL-provided training, guidance, and technologies for automated compliance.

Ensuring Security of the Core Infrastructure

In a health information exchange, the core infrastructure includes the systems and personnel to operate the components at the center of the network. The core infrastructure shall be certified for compliance by at least one independent certifier of industry standard information security practices, such as the Electronic Healthcare Network Accreditation Commission (EHNAC). EHNAC is an independent, non-profit accrediting agency that evaluates an organization's ability to meet standards and best practices. EHNAC certification includes a rigorous set of requirements aimed at HIPAA transaction processors, clearinghouses, and data centers, in the areas of Privacy and Confidentiality, Technical Performance, Resources, and HIPAA Security. VITL shall publish and maintain core infrastructure certification information on its website.

Ensuring Security at the Participating Health Care Providers

Participating Health Care Providers, as HIPAA covered entities, must comply with HIPAA Security rules and HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information. This requires HIPAA Security practices to mitigate risk in three areas: Accessing Health Information, Storing Health Information, and Transmitting Health Information. Participating providers shall affirm compliance with the HIPAA Security Rule, including eight HIPAA-based practices listed in the Risk Assessment subsection below. VITL reserves the right to conduct a security audit of participating providers to demonstrate compliance.

Risk Assessment

Participating Health Care Providers are required by HIPAA Security Rule §164.308 (a)(ii)(A) to conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic PHI. Based on the HIPAA requirements and Security Guidance published by the Department of Health and Human Services, VITL recommends that the risk assessment should include, but not be limited to, the following practices across eight subject areas:

1. Security policy and organization. Each Participating Health Care Provider should designate a Privacy Officer and Security Officer, and maintain a written security policy made available to all personnel with access to PHI. Confidentiality agreements should be utilized for third-parties with PHI access. The Privacy Officer and Security Officer should hold regular meetings with the management of the organization. They should develop processes for writing incident reports, regularly reviewing logs, end-user management including account creation, and patient inquiries.
2. Asset management. Each Participating Health Care Provider should maintain an inventory of health information assets containing PHI or with access to PHI such as laptops, desktops, servers, and removable media. A custodian should be identified to maintain the inventory, and rules should be written into security policy for acceptable use of the assets.
3. Human resources. Each Participating Health Care Provider should consider the information security impacts for employees joining, moving and leaving the organization. Job descriptions should indicate who has responsibilities related to PHI, and contracts with employees and contractors should include reference to information security policies,

including information security-related disciplinary procedures. The Participating Health Care Provider should have procedures for removing access to PHI upon termination of employment or contract. The Participating Health Care Provider should promote information security awareness through education and training for employees.

4. Physical and environmental security. Each Participating Health Care Provider should take reasonable steps to protect computer facilities and equipment containing or with access to PHI. Depending on the size of the organization, this may include establishing secure areas and deploying physical security measures for these areas. Where IT equipment is used off-premises, the organization should have policies for remote use of laptops or home computers. Procedures for secure disposal of IT equipment should be followed.

5. Communications and operations management. Each Participating Health Care Provider should take responsibility for the management of technical security controls in its systems and networks that are used to access PHI. The Participating Health Care Provider or its contractors should have documented operating procedures and formal change control process for implementing changes to systems or networks. Controls to prevent, detect, and respond to malicious software and network intrusion should be deployed. When stored on portable media, PHI should be tracked, and encrypted or protected from theft. A secure audit log should be created whenever PHI is accessed, created, updated, or archived. The auditing should be implemented at all times, and procedures for analyzing audit logs should be followed.

6. Access control. Each Participating Health Care Provider should take measures to limit access to networks, systems, applications, functions and data to authorized personnel. An access control policy should be established including password management procedures.

7. Information systems acquisition, development and maintenance. The Participating Health Care Provider should take steps to ensure that security is built into EHR and other clinical systems that store electronic PHI.

8. Information security incident management. Each Participating Health Care Provider should anticipate and respond appropriately to privacy and security related events such as breaches. Policies should be established for response to such events.

Secure Audit Logs

In addition to the audit logs kept by the provider for its own records, VITL shall maintain a comprehensive set of audit logs detailing accesses to the exchange. VITL audit policies, as described in the Auditing and Access Monitoring Policy, include regular review of audit logs by the VITL Privacy Officer as well as delegated review of selected logs by the Participating Health Care Provider Privacy Officer. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches, are described in the VITL Privacy and Security Events Policy.

Detailed Guidelines and Training

No security policy can be successfully implemented without a training component. The Participating Health Care Provider Privacy Officer will be required to attend an online

security training session sponsored by VITL. All VHIE end-users must submit a written acknowledgement of security and privacy policies. VITL may also sponsor optional annual supplemental security training for all interested users. In addition to this policy document, VITL shall periodically publish guidelines to assist with the implementation of the ISO best practices defined above.

Affinity Domain Policy

As described in the Vermont Health Information Technology Plan, the VHIE is designed to be compatible with the Integrating the Healthcare Enterprise (IHE) architecture. IHE provides technical frameworks for the use of existing standards, reducing variability in their implementation. The integration profiles that make up IHE technical frameworks specify how standards should be used to achieve specific needs within the framework. VITL shall publish and maintain on its website a detailed IHE Affinity Domain Interoperability Policy Agreement which will include technical details for statewide standard interoperability requirements and specifications including standard content, identification schemes, vocabularies, actors, and transactions to be supported by the VHIE. These Cross-Enterprise Document Sharing (XDS) profile extensions are being defined statewide in Vermont and shall be followed by all VHIE participants within the state. They will include further details in the following areas related to technical security, including:

- Authorization
- Role Management
- Definition of Functional and Structure Roles
- Identity Management Policy and Authentication of Users
- Attestation and Delegation Policy
- Node Authentication Requirements

Technologies for Automated Compliance

VITL shall utilize technologies for automated compliance with security policies where practical. For example, VITL may implement an automated system which would require the existence of a current antivirus software on the end-user's terminal before access is granted to the exchange. VITL may employ automated intrusion detection systems, and may request that Participating Health Care Providers deploy similar software or participate in the application of these systems.

Procedures for Non-compliance

Procedures for non-compliance, including sanctions, are described in the Privacy and Security Events Policy.

APPLICABILITY:

This policy applies to all persons and organizations connected to the VHIE.

MONITORING PLAN

The VITL Chief Security Officer is responsible for monitoring the plan.

VITL

RELATED POLICIES

Auditing and Access Monitoring Policy
Privacy and Security Events Policy

REFERENCES

[Identified in the policy.]

REVIEWERS

Lauri Scharf, Director of Technology
VITL Board of Directors

SPONSOR'S NAME

Lauri Scharf, Director of Technology

APPROVING OFFICIAL'S NAME

VITL Board of Directors