

ID	SEC004
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: Auditing and Access Monitoring

PURPOSE:

The purpose of the policy is to insure that the security and confidentiality of patient data is protected.

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.

“Unsecured Protected Health Information” means PHI that has not been secured through the use of a technology or methodology standard as provided by federal law.

“Audit” means an individual’s act of reviewing and examining records of activity related to the records of access and use of the VHIE by participating health care providers.

“Audit Logs” means system generated reports based on logging and recording transactions sent and received, access records (including denied access), and other information related to tracking use and access by Participating Health Care Providers in the VHIE.

POLICY

1. Audit logs shall be generated by the VHIE, by the Participating Health Care Providers’ EHR systems, and by other computer software and systems that communicate with the VHIE to access, store and communicate personal health information about individuals who have opted in to the VHIE.

2. Audit logs accessible by Privacy Officers of Participating Health Care Providers shall be restricted to records of access by the Participating Health Care Provider.
3. VHIE Audit logs shall be reviewed on a routine basis by the VITL Privacy Officer and by the Privacy Officer of Participating Health Care Providers. Any suspicious activity discovered by VITL shall be reported to the Participating Health Care Provider and VITL shall generate a Reportable Event report. Any suspicious activity discovered by a Participating Health Care Provider shall be reported to VITL; VITL shall generate a Reportable Event report as per the VITL Privacy and Security Events Policy. The VITL Privacy Officer shall specifically review audit logs to detect intrusion attempts and patterns of access to the VHIE.
4. VHIE Audit logs shall be reviewed by VITL and Participating Health Care Provider as needed to follow up on inquiries from providers and patients regarding accesses and use of the VHIE.
5. As per the Policy on Information Security, Participating Health Care Providers are expected to create secure audit logs whenever PHI is accessed, created, updated, or archived via an EHR or other information system. Audit logging shall be implemented at all times and procedures for analyzing audit logs shall be provided and used by the provider.

VHIE Audit Logs

A secure audit log shall be created whenever PHI is accessed, created, updated, or archived via the exchange. Audit logging shall be implemented at all times, and procedures for analyzing audit trails shall be used by the VITL Privacy Officer and Participating Health Care Provider Privacy Officers.

VITL Privacy Officer and Participating Health Care Provider Privacy Officers shall be provided with facilities for analyzing logs and audit trails that:

- allow the identification of all VHIE users who have accessed or modified a given subject of care's PHI in the VHIE over a given period of time, and
- allow the identification of all subjects of care whose PHI has been accessed or modified by a given VHIE user over a given period of time.

Audit logs shall be secure and tamper-proof. Access to system audit log analyzing tools and audit logs shall be safeguarded to prevent misuse or compromise.

For transactions sent to or from the VHIE, the audit system shall record:

- sender identifier
- date and time of event
- system component where the event occurred
- type of event or transaction
- outcome of the event (success or failure)

For user access events, the audit system shall record:

- user identifier
- date and time of event
- system component where the event occurred
- type of event
- outcome of the event (success or failure)

For granting/revoking access to the VHIE the audit system shall record:

- user identifier
- date and time of event
- system component where the event occurred
- type of event (authorization, revocation, password change)
- outcome of the event

All access and transaction logs shall be kept for six years.

Patient Request for Audit Report

An individual may request an audit report of access to his or her PHI on the VHIE, for a period no longer than three years prior to the date of request, by contacting VITL's Privacy Officer. VITL shall provide the requested Audit Report within 30 calendar days, and it shall provide the following information pursuant to 45 CFR § 164.528(b):

1. The date of disclosure;
2. The name of the Participating Health Care Provider and/or user or other person who received the protected health information and, if known, the address of such entity or person;
3. A brief description of the protected health information disclosed; and
4. A brief statement of the purpose of the disclosure.

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.

RELATED POLICIES

n/a

REFERENCES

n/a

REVIEWERS

VITL

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