



IDENT	SEC004-01
Type of Document:	Procedure
Type of Policy:	Corporate
Sponsor's Dept:	PMO
Title of Sponsor:	VP
Title of Approving Official:	Chief Security Officer
Date Released (Published):	2/8/11
Next Review Date:	7/1/11

SUBJECT: Audit and Access Monitoring Procedures

PURPOSE:

Define procedures to comply with the VITL Policy on Auditing and Access Monitoring.

PROCEDURE

1. Audit Logs

- VITL will record audit entries with the following data elements as required by the VITL affinity domain policy:
 - i. For transactions sent to or from the VHIE, the audit system shall record:
 - 1. sending system or receiving system identifier
 - 2. sending user identifier
 - 3. date and time of event
 - 4. system component where the event occurred
 - 5. type of event or transaction
 - 6. outcome of the event (success or failure)
 - ii. For user access events, the audit system shall record:
 - 1. user identifier
 - 2. authentication details
 - 3. date and time of event
 - 4. system component where the event occurred
 - 5. type of event
 - 6. outcome of the event (success or failure)
 - iii. For granting/revoking access to the VHIE the audit system shall record:
 - 1. user identifier
 - 2. date and time of event
 - 3. system component where the event occurred
 - 4. type of event (authorization, etc.)

Revised: 2/7/2011



- iv. For archiving events:
 1. User identifier
 2. date and time of event
 3. system component where the event occurred
 4. outcome of the event (success or failure)
2. Audit reports
 - On the first of each month, the Chief Security Officer will review the following automatically generated report for 5% of audit records:
 - i. user accesses including successes and failures
 - ii. node authentications including successes and failures
 - iii. PHI accesses, updates, publications, and archiving by users and systems
 - On a quarterly basis, the Chief Security Officer will review audit reports to identify suspicious activity and opportunities for improvement.
3. Access monitoring
 - The Chief Security Officer will monitor Participant access to the VHIE at least monthly by reviewing the VHIE audit reports.
 - The Chief Security Officer will contact the Participant to review any suspicious activity. In case of a reportable event, the Chief Security Officer will generate a report (refer to procedure SEC005-1 for details).
4. Participant request for an audit report
 - The Security Officer will accept Participant requests for an audit report for events related to records that the Participant accessed in the VHIE.
 - The response will include an audit report that meets the criteria of a VITL Audit Request Form completed by the Participant.
 - The Security Officer will respond within thirty (30) days of receiving the VITL Audit Request Form using either the postal service or encrypted electronic mail.
 - The Security Officer will maintain a log of requests (recording the requestor, request date, nature of request, and date of response).
 - The Security Officer will retain the request form and the report at VITL.
5. Patient request for an audit report
 - The Chief Security Officer will respond to patient requests for an audit report for events related to the patient's data that any Participant provided to the VHIE.
 - The response will include an audit report that meets the criteria of a VITL Audit Request Form completed by the patient.
 - The patient must make an appointment to visit the Chief Security Officer at the VITL office during normal business hours, provide valid proof of identification that includes a photograph, and complete a VHIE Audit Request Form (SEC004-2).



- The Chief Security Officer will respond within thirty (30) days of receiving the VITL Audit Request Form.
- The Chief Security Officer will send the report to the location specified in the Form using either the postal service or encrypted electronic mail.
- The Security Officer will maintain a log of requests (recording the requestor, request date, nature of request, and date of response).

REVIEWERS

Sandy McDowell, VP of Operations

APPROVING OFFICIAL'S NAME

Lauri Scharf, Director of Technology