

# AHS Audit and Accountability Standard

---

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Audit and Accountability ( AU-1, AU-2, AU-2(4), AU-3, AU-3(1), AU-4, AU-5, AU-6, AU-6(1), AU-7, AU-7(1), AU-8, AU-9, AU-10, AU-11, AU-12, IRS Publication 1075) Controls.

## Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
8/4/2013	1.0	Created Document	Jim St. Clair
8/5/2013	2.0	Document revised for AHS standards	Jack Green
10/08/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

### PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Audit and Accountability (AU-1, AU-2, AU-2(4), AU-3, AU-3(1), AU-4, AU-5, AU-6, AU-6(1), AU-7, AU-7(1), AU-8, AU-9, AU-10, AU-11, AU-12, IRS Publication 1075) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

### SCOPE

The scope of this standard includes the VHC and its constituent systems only.

### STANDARD

#### **Auditing Events**

1. Prior to the introduction of a new system at the VHC, the System Administrator must ensure the system is auditable.
  - System audits must track the following information:
    - i. Any system administration activity that takes place
    - ii. When the system server is started or shut down
    - iii. Any system services that are loaded/unloaded
    - iv. Any software installation or removal
    - v. A log of every user who accesses the system and logs on
    - vi. Any account creation, modification, or deactivation
  - The System Administrator maintains the event logs. The event logs are accessible by the VHC Security and Privacy Manager in the event reporting and/or analysis is required.
2. Audit logs will be produced for the following systems:
  - Desktop and Laptop computers
  - File, print, web, firewall, or terminal servers
  - Network components such as wireless routers or switches

3. Audit logs for desktops are maintained by the VHC IT staff in accordance with state and federal rules and regulations per AU-2 policy and controls.

### **Audit Record Content**

1. The following information is captured in all audit logs for each information system:
  - Date and timestamp of when the event took place
  - The component of the system in which the event occurred
  - The event source
  - The event type
  - The event outcome
  - Any security relevant actions that were processed
2. Systems containing or processing FTI data must also capture the following information in the Audit Logs:
  - All creation, modification, and deletion of objects including files, directories, and user accounts
  - All creation, modification, and deletion of user accounts and group accounts
  - All creation, modification, and deletion of user account and group account privileges.
  - All access, modification, deletion, and copying of FTI data.
    - i. Must uniquely identify the user making the request.
    - ii. Also applies to database or database tables embedded in or residing outside of the applications.
  - All identification and authorization attempts.
  - All Successful and Unsuccessful authorization attempts.
  - All changes to logical access control authorities (rights, permissions...).
  - All system changes with the potential to compromise the integrity of auditing policies, auditing configuration, and audit records generation.
  - Enabling and disabling audit report generation services.
  - Command line changes, batch file changes, and queries made regarding information components (Operating System, Application, Database...)
3. Audit logs from systems containing or processing FTI data must be handled as if they may contain FTI data.
4. The execution of all privileged commands or operations must be captured, including but not limited to administration logon, administration logoff, system shutdowns, system reboots, system component failure.

### **Audit Log Storage**

1. The System Administrator must ensure enough storage capacity is provisioned for saving all audit logs and follow the process (if required) for the archival of audit logs that are older than 90 days.

2. Archives of audit logs are retained and accessible.
  - Archives of audit logs regarding request for FTI and the response provided must be maintained for a minimal of 5 years.
  - Archives of audit logs for system containing or processing FTI data must be retained for a minimal of 6 years.
  - All other system must retain the audit log archives for a minimal of 1 year

### **Audit failure events**

1. Each VHC information system will automatically alert the System Administrator in the event of an audit log failure.
  - This notification should be distributed via E-mail to allow easy access to the notification in the event the System Administrator is not on site.
2. The information system must also ensure in the event storage capacity has been reached, that any new audit logs overwrite the oldest existing audit log on the system.
3. Systems containing or processing FTI data shall retain the audit log over system shutting down and restarting, stopping and starting the audit report generation without overwriting the oldest information.

### **Review, analysis, and reporting of audit logs**

1. The System Administrators for each VHC Information System must review and analyze on a weekly basis the audit logs in their systems for the following:
  - Unusual or inappropriate activity
  - Ensure audit log functionality
2. In the event unusual or inappropriate activity is identified, it must be reviewed with the Security and Privacy Manager immediately.
3. For each VHC Information System, the System Administrator is liable to perform the following regarding audit logs:
  - Review audit logs created for critical systems daily.
  - Review and compare audit logs on for firewalls, routers, or any other network devices with logs on critical systems daily to validate if any incidents have occurred.
  - Review PII access and extracts monthly.
  - Review audit logs on all other systems on a weekly basis.
  - Inspect Administrator groups for unauthorized administrator accounts on a bi-weekly basis.
  - Perform manual review of audit records at least once every 30 days.
4. All audit logs for all system logons and logoffs must be reviewed weekly by the System Administrator of that specific VHC Information System.

5. Any new system introduced must also include a training session for the System Administrator to ensure log management responsibilities can be performed.
6. All audit findings must be reported by the System Administrator to the Security and Privacy Manager.
7. Any incidents identified by the System Administrator or Security and Privacy Manager must be immediately reported to the VHC ISO.

### **Audit Report Generation and Reduction**

1. Each VHC Information System will provide the ability for the System Administrator to perform report generation to support real-time audit review, analysis, and reporting while ensuring the original audit records are not altered.

### **Audit Protection**

1. System Administrators must ensure that all access to audit logs is limited only to the Security and Privacy Manager, authorized users, or other system administrators as necessary.
2. System Administrators must encrypt all audit logs which contain data deemed sensitive (PII, FTI).
3. Inspection Reports, including corrective action must be retained for a minimal of 3 years (PII).

### **IMPORTANT INFORMATION**

These procedures can be found at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>