

# System Audit Control Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 5/5/05

---

## 1.0 Purpose

The purpose of these procedures is to establish hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems.

These procedures are governed by HIPAA Security Standard *164.312(b) Audit Controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

## 2.0 Definitions

**2.1 Workforce:** All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

## 3.0 Procedures

### 3.1 System Audit Controls

#### 3.2 File Servers

The following guidelines apply to system audit trails for files stored within established protected ("P") drives on ISU production file servers and for customer identified folders on hosted servers. The P drive is intended for ePHI and other files that may contain sensitive data.

##### 3.2.1 Audit Trail Content

Domain logon activity will be monitored through the Windows Security Event Log. The Security Event Log Tracks:

- File/directory access
- File/directory modification
- File/directory deletion
- Login name
- Date and time
- Login failures and successes

##### 3.2.2 Audit Trail Security

Audit logs containing any suspicious activity will be saved as csv files in a protected location only accessible by S/Med domain administrators. Logs will be burned to CD (or DVD, dependent upon size) on an annual basis and sent offsite for secure storage. Retention time for media will be six years. Due to limited system administrator resources, ISU will make a best effort to separate

---

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 03/18/2005

## System Audit Control Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 5/5/05

---

the duties of those who administer the access control functions from those who administer the audit trails.

### 3.2.3 Audit Trail Review Guidelines

Due to the low risk of unauthorized activity and the massive amount of data collected by the Security Event Log, the logging feature will be turned on once per week for a duration of 24 hours. The audit trails will be reviewed once per month.

### 3.2.4 Appropriate versus Inappropriate Activity

The review process will entail looking for suspicious login activity such as multiple login attempts from unknown domains, accounts and machines within a short duration of time. Five failed logons will automatically lock the account for a period of 10 minutes

### 3.2.5 Unexpected Activity

While conducting system audit reviews, system administrators will look for unexpected or suspicious activity such as performance problems, additional or unknown processes running, unexpected ports open, unexpected user log entries and changes to log files.

**3.2.6 Audit for access:** Once per year, the ISU will review with the Department Managers the access control list on file for the "P" drive.

## 3.3 Database Applications

All ISU proprietary or 3<sup>rd</sup> party database applications that utilize ePHI, receive application and/or database support by ISU, and are hosted by ISU will utilize MS SQL Server. ISU will purchase a 3<sup>rd</sup> party tool to perform system audits on SQL databases that contain ePHI. All 3<sup>rd</sup> party applications or departmental applications that are hosted by ISU, but do not receive applications and database support by ISU are the responsibility of the 3<sup>rd</sup> party vendor or the department. ISU is not responsible for system auditing on these systems.

Sections below to be updated by ISU DBA after more

---

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 03/18/2005

## System Audit Control Procedures

Revision B  
Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 5/5/05

---

information is known about 3<sup>rd</sup> party tool:

**3.3.1 Define Audit Trail Content:** Define the content of the audit trail. At a minimum, the audit trails should contain the following information:

- Type of event
- Date and time of occurrence
- User ID associated with event
- Program, command, or method used to initiate event
- Patient and data elements whose information was changed

**3.3.2 Define Audit Trail Security:** Design and implement sufficient security controls to protect audit trails from unauthorized access. Separate the duties of those who administer the access control functions from those who administer the audit trails, if possible.

**3.3.3 Define Audit Trails Review Guidelines:** Determine review methods and the frequency of audit trails, based upon the identified risks level.

**3.3.4 Define Appropriate Versus Inappropriate Activity:** Identify what is considered to be appropriate activity and inform the individuals responsible for reviewing audit trails to ensure that they can distinguish between appropriate and inappropriate activity

**3.3.5 Define Unexpected Activity:** While conducting system audit reviews, system administrators will look for unexpected or suspicious activity such as performance problems, additional or unknown processes running, unexpected ports open, unexpected user log entries and changes to log files.

# System Audit Control Procedures

Revision B

*Dean's Office*

Information Services Unit

Issue Date:

Last Revision: 5/5/05

---

## 4.0 Initiation and Control Reporting

---

### 4.0 Records & Documentation Control

---

---

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 03/18/2005

## System Audit Control Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 5/5/05

### 6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Audit Controls	<b>164.312(b)</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
Special Publication: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule – National Institute of Standards and Technology (NIST)	<b>SP 800-66</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
University of California Business and Finance Bulletin IS-3 Electronic Information Security	<b>IS-3</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a> or <a href="http://www.ucop.edu/ucophone/policies/bfb/is3.pdf">http://www.ucop.edu/ucophone/policies/bfb/is3.pdf</a>
Information Security and Confidentiality Policy (UCSF)	<b>650-16</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
Information Security and Confidentiality Policy (UCSF Medical Center)	<b>5.01.04</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
Security Management Procedures	<b>60.001</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>

### REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	03/04/05	Ken Jakobs	Initial Release
B	03/18/05	Ken Jakobs, Dan Yee and Barbara Heredia	Version 1.5 section 3.0 Procedures
C	04/11/05	Todd Lawrence	Converted to S/Med Template

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 03/18/2005