Audit and Accountability Policy

Policy 8	POL-AU	Effective Date	12/17/15	Review Date	12/17/15	Version	1.0

Table of Contents

I. PURPOSE

The University of Chicago Medical Center and the Biological Sciences Division of The University of Chicago (the "**Organizations**") protects information that is the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the "**Security Obligations**"); such information is called "**Protected Information**." This policy sets forth the security requirements that will support the Organizations' ability: (i) to review key auditable events to verify the appropriateness of access to Information Systems, and the Data they contain; and (ii) to assist the Organizations' in detecting, containing and correcting security violations.

II. SCOPE

This policy applies to Information System Owners and IT Custodians who manage Information Systems for the Organizations.

III. POLICY

This policy defines methods that must exist in order for the Organizations to (i) create, protect, and retain Information System logging audit records (e.g. firewall logs, system event logs, etc.) including user access audit records; (ii) regularly review, analyze and investigate unlawful, unauthorized, or otherwise inappropriate Information System activity; and (iii) ensure that the

actions of individual Information System users can be uniquely traced to those users so they can be held accountable for their actions.

Capitalized terms used in this policy are defined in the glossary attached. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

IV. PROCEDURES

1. Information System Owners must maintain and document technical procedures that meet the Risk Controls set forth below when managing audit logging of Information Systems within their control.
    a. These technical procedures must account for enabling the user access audit logging functionality as well as ensuring user access audit logging reviews is occurring on a periodic basis.
    b. The documentation of these technical procedures must be retained for a period of six (6) years.
    c. In the event of a Security Incident with an Information System, then the audit logging records will be maintained by the CISOs for six (6) years.

2. IT Custodians are responsible for implementing the technical procedures established by their Information System Owners for the purpose of recording and examining activity in the Information System.

3. Information System Owners are responsible for monitoring user access, and reporting anomalous activities in the Information Systems within their control to the respective CISO.

4. At a minimum, Information System Owners must ensure that Information Systems that store, process or transmit Protected Information have their logging audit records (e.g. firewall logs, system event logs, etc.) including user access audit records stored as directed by the respective Information Security Office. As general guidance, Information Systems supporting the clinical functions of the Organizations will store their audit logs as directed by the UCM Information Security Office; Information Systems supporting the research and academic functions of the Organizations will store their audit logs as directed by the BSD Information Security Office.

5. Information System Owners and IT Custodians should conform to the Data Classification and Data Handling Policy when sharing audit log information. For example, an audit log with Protected Information requires approval by the CISO of the Information System, in consultation with legal counsel, when sharing with a third party.

The Organizations will use the Risk Based Controls below to implement the procedures.

V. RISK BASED CONTROLS

Risk based controls are organized in three categories; Core (C), Low (L) and Moderate (M). Core controls are mandatory for all Information Systems. Information Systems designated as FISMA Low must comply with Low controls, in addition to the Core controls. Information Systems designated as FISMA Moderate must comply with Moderate controls, in addition to the Low and Core controls.

Auditable Events (AU-2 CM)

Core	• Information Systems that store, process or transmit Protected Information must employ automated logging mechanisms that generate audit records containing adequate detail to support after-the-fact investigations of security incidents. • Technical procedures for monitoring audit logs shall contain a list of the type of events considered to be being auditable. These technical procedures must provide rational for why the type of event is considered auditable. Events to consider include: o Failed authentication attempts o Successful authentication attempts o System startup or shutdown o Use of privileged accounts (system administrator accounts) o Change of user security privileges (addition of groups, password change, etc.)
Low	N/A
Moderate	The list of auditable events will be reviewed to determine its necessity and sufficiency on an annual basis and updated appropriately.

Content of Audit Records (AU-3 CM)

Core	• Audit records must contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome. Elements of the audit record to consider for capture include: o Date and Time of Activity o Identification of user or process performing activity o Origin of Activity (Source and/or Destination IP address, etc.) o Description of activity (create, read, access, update) o Success / Failure indications o Protected Information accessed, if applicable o File accessed, if applicable o Access control or flow rule invoked, if applicable
Low	N/A

Moderate	The Information System generates audit records containing additional information explicitly needed for specific audit requirements (examples: full text recording of privileged commands or the individual identities of group account users).

Audit Storage Capacity (AU-4 C)

Core	• Information Systems that store, access, or transmit Protected Information must have a sufficient amount of system storage allocated to store the audit records in accordance to requirement AU-11. • The amount of system storage can be reduced when central logging capabilities are implemented to maintain logs for the period defined in AU-11.
Low	N/A
Moderate	N/A

Response to Audit Processing Failures (AU-5 C)

Core	• Information Systems that store, process, or transmit Protected Information must be configured to alert the IT Custodian in the event the audit logging mechanism has failed. • In the event an Information System that stores, processes or transmits Protected Information reaches its configured capacity for audit log retention, the Information System must be configured to overwrite the oldest audit logs o If possible, and not detrimental to business functions, the system can be configured to halt its processing until the audit capturing functionality is restored.
Low	N/A
Moderate	N/A

Audit Monitoring, Analysis, and Reporting (AU-6 CM)

Core	• Suspicious, unusual or malicious activity must be reported to the applicable Information Security Office of the Organizations.
Low	• Reviews of audit records must occur at least on a routine basis for Information Systems that store, process, or transmit Protected Information.
Moderate	• Audit logs will be reviewed, analyzed and reported in an automated manner leveraging either the UCM or the BSD centralized log management system.

Audit Reduction and Report Generation (AU-7 CM)

Core	• The central log management system, operating by the respective Information Security Offices, shall provide a means to generate reports for audit review, analysis, and after-the-fact investigations of security incidents. • The reduction of audit content (i.e. audit information provided in a summary format) will not alter the original audit content or time ordering of audit

	records.
Low	N/A
Moderate	The central log management system, operated by the respective Information Security Offices, will automatically process audit records and generate reports for events of interest based on, at a minimum, identity of the individual or process, logical or physical networks location a specific Information System component

Time Stamps (AU-8 C)

Core	• Information System audit logs must employ time stamps. Time stamps of audit records must be generated using internal system clocks that are synchronized system-wide either to the UCM time management server, the BSD time management server, or the University time management server. • Time stamps will record the based on the Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). o If capable, the time stamp will also record the local time offset from UTC (-6 hours)
Low	N/A
Moderate	N/A

Protection of Audit Information (AU-9 CM)

Core	The Information System will be configured to protect audit information with the minimum necessary access, to prevent unauthorized access, modification and deletion.
Low	N/A
Moderate	Only IT Custodians of the Information System, or the respective Information Security Offices of the Organizations may access the audit functionality of the Information System.

Audit Record Retention (AU-11 C)

Core	Information Systems that store, process or transmit Protected Information must maintain user access audit logs for a period of three (3) months; except for the following Information Systems, the period for maintaining user access logs shall be six (6) months: • The official Electronic Medical Record / Electronic Health Record • The official Imaging system (PACS) • The official Healthcare billing systems • The official HR systems, or Enterprise Resource Program (ERP)
Low	N/A
Moderate	N/A

Audit Generation (AU-12 LM)

Core	• Information Systems that store, process or transmit Protected Information must: o Provide audit record generation capabilities that meets AU-2 Information Systems must either a) send audit log data to the applicable Information Security Office's central logging environment in real time, or b) produce audit log content within 1 hour of the request to the applicable Information Security Office of the Organizations
Low	N/A
Moderate	N/A

VI. Cross References

POL-AC Access Control Policy

VII. Policy References

HIPAA Security Rules: 42 C.F.R. § 164.308(a)(1)(ii)(D)
HIPAA Security Rules: 42 C.F.R. § 164.312(b)

VIII. INTERPRETATION, IMPLEMENTATION AND REVISION

Each CISO is responsible for the interpretation and implementation of this policy, and responsible for recommending revisions of this policy to the Cyber Security Executive Committee.

Kenneth Polonsky
Dean, Biological Sciences Division

Sharon O'Keefe
President, The University of Chicago Medical Center

IX. Approval and Ownership

Owner	Title	Date
Privacy & Security Steering Committee	Policy Development Group	12/11/15
Approved By	**Title**	**Date**
Kenneth Polonsky, MD	Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs	12/17/15
Sharon O'Keefe, RN	President, University of Chicago Medical Center	12/17/15

X. Revision History

Version	Description	Review Date
1.0	Initial Version	12/17/15