**University of Wisconsin-Madison**
**Policy and Procedure**

Policy Number: 8.3
Policy Title: HIPAA Security Auditing
Effective Date: June 9, 2015
Last Revision Date: February 12, 2015


## I. Policy

A. The University of Wisconsin-Madison, the units of the UW-Madison Health Care Component and each individual or unit within UW-Madison that is a Business Associate of a covered entity (hereafter collectively referred to as "units") shall audit access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.

B. The Security Rule requires covered entities to implement reasonable hardware, software, or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system or network auditing capabilities and resources. UW-Madison and each unit shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing which is consistent with available resources.

## II. Definitions

A. Audit: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a potential breach, patient complaint, or suspicion of employee wrongdoing. Audit activities shall also take into consideration information system risk assessment results.

B. Audit Controls: Technical mechanisms that track and record computer/system activities.

C. Audit Logs: Records of activity maintained by the system which provide:

1. The date and time of significant activity;
2. The origin of significant activity;
3. The identification of user performing significant activity;
4. A description of attempted or completed significant activity.

D. Audit Trail: Means to monitor information operations to determine if a security violation occurred by providing a chronological audit logs that

relate to an operating system, an application, or user activities. Audit trails help provide:

1. Individual accountability for activities such as an unauthorized access of ePHI;
2. Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information;
3. Problem analysis such as an investigation into a slowdown in a system's performance.

*An audit trail identifies who (login) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time).*

E. Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

F. Protected Health Information ("PHI"): Health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.

G. Trigger Event: Activities that may be indicative of a security breach that require further investigation.

H. Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

## III. Procedures

A. General

1. Responsibility for auditing information system access and activity is assigned at two levels.

a. The UW-Madison HIPAA Security Officer is responsible for:

   i. Auditing resources and facilities that are managed at the campus level. This includes, but is not limited to, the campus level security awareness and training program. See section III.F. below.

   ii. Security controls and backup for audit logs of resources and facilities the UW-Madison HIPAA Security Officer is responsible for auditing. See section III.E. below.

   iii. Arranging for or coordinating external audits and other external resources to assist in audits at all levels. See section III.G. below regarding external audits.

   iv. Advising the HIPAA Security Coordinator of each unit, and arranging for additional auditing support for the unit as warranted.

b. The HIPAA Security Coordinator of a unit is responsible for:

   i. Auditing resources and facilities that are managed by the HIPAA Security Coordinator's unit, including any unit-level security awareness and training.

   ii. Security controls and backup for audit logs of resources and facilities the HIPAA Security Coordinator is responsible for auditing. See section III.E. below.

   iii. Assisting the UW-Madison HIPAA Security Officer in campus level audits on matters related to the HIPAA Security Coordinator's unit.

   iv. Jointly auditing resources and facilities that are shared by multiple units and are jointly managed by the participants, with the HIPAA Security

Coordinator of one unit selected to lead the audit-related activities, and the HIPAA Security Coordinators of other participating units assisting the selected leader. The selected leader will also coordinate security controls and backup for audit logs of such resources and facilities. See section III.E. below.

2. The UW-Madison HIPAA Privacy Officer, UW-Madison Chief Information Officer (CIO) and other UW-Madison campus leaders provide leadership support for the UW-Madison HIPAA Security Officer so that resources can be identified and audits can be accomplished. The CIO or IT director of the unit or other unit leaders provide the corresponding leadership support for the HIPAA Security Coordinator of their unit.

3. The auditing procedures at both the campus level and the unit level are the same, with the exception of the general differences described in III.A.1-2 above, and any specific language included below.

4. The responsible individual, as defined in III.A.1. above, shall:

   a. Assign the task of generating reports for audit activities to the person responsible for the application, system, or network.

   b. Assign the task of reviewing the audit reports to the person responsible for the application, system, or network, or any other person determined to be appropriate for the task.

   c. Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.)

5. The auditing processes shall address access and activity at the following levels listed below.

a. User: User level audit trails generally monitor and log commands directly initiated by the user, identification and authentication attempts, and files and resources accessed.

b. Application: Application level audit trails generally monitor and log user activities, including data files opened and closed, specific actions, and printing reports.

c. System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.

d. Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

6. The responsible individual, as defined in section III.A.1. above, and their supporting leadership shall determine the systems or activities that will be tracked or audited by:

a. Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk assessment and ongoing risk management processes.

b. Maintaining confidentiality, integrity, and availability of ePHI applications and systems.

c. Assessing the appropriate scope of system audits based on the size of the resource or facility and the needs of the campus or unit by asking:

i. What information/ePHI is at risk?

ii. What systems, applications or processes are vulnerable to unauthorized or inappropriate access?

iii. What activities should be monitored (create, read, update, delete)?

iv. What information should be included in the audit record?

d. Assessing available organizational resources.

7. The responsible individual, as defined in section III.A.1. above, and their supporting leadership shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. At a minimum, trigger events will include:
   a. Patient complaint;
   b. Employee complaint;
   c. Suspected breach of patient confidentiality;
   d. High risk or problem prone event (e.g., VIP admission).
8. The responsible individual, as defined in section III.A.1. above, and their supporting leadership shall determine auditing frequency by reviewing past experience, current and projected future needs, and industry trends and events. The UW-Madison HIPAA Security Officer will provide advice on the suitable range of audit frequency by units. The unit will determine its ability to generate, review, and respond to audit reports using internal resources, and may request additional resources or assistance. The units and UW-Madison recognize that failure to address automatically generated audit logs, trails, and reports through a systematic review process may be more detrimental to the organization than not auditing at all (e.g., state/federal licensing and accrediting agencies).
9. The UW-Madison HIPAA Security Officer, UW-Madison IT Security staff, the HIPAA Security Coordinator of a unit, the unit's IT security staff, or their designees are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others without the explicit authorization of the UW-Madison HIPAA Security Officer. These tools may include, but are not limited to:
   a. Scanning tools and devices;
   b. War dialing software;
   c. Password cracking utilities;
   d. Network "sniffers";

e. Passive and active intrusion detection systems.

10. Audit documentation/reporting tools shall address, at a minimum, the following data elements:
    a. Application, system, network, department, or user audited;
    b. Audit type;
    c. Individual/department responsible for audit;
    d. Date(s) of audit;
    e. Reporting responsibility/structure for review audit results;
    f. Conclusions;
    g. Recommendations;
    h. Actions;
    i. Assignments;
    j. Follow-up.
11. The process for review of audit logs, trails, and reports shall include:
    a. A description of the activity as well as rationale for performing audit;
    b. Identification of which workforce members or department/unit will be responsible for review (workforce members shall not review audit logs which pertain to their own system activity);
    c. The frequency of the auditing process;
    d. Determination of significant events requiring further review and follow-up;
    e. Identification of appropriate reporting channels for audit results and required follow-up. The procedures in Policy # 8.8 “Notification and Reporting in the Case of Breach of Unsecured Protected Health Information” may be used to report a single event;

12. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), if publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

    a. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services – separation of duties).

    b. Testing shall be done on a routine basis (e.g., annually).

B. Audit Requests for Specific Cause

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Human Resources, Risk Management, the UW-Madison HIPAA Privacy Officer, the UW-Madison HIPAA Security Officer or a member of either the UW-Madison administration or the unit's administration.

2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by UW-Madison HIPAA Privacy Officer or UW-Madison HIPAA Security Officer.

3. A request for an audit as a result of a patient concern shall be initiated by UW-Madison HIPAA Privacy Officer or the UW-Madison HIPAA Security Officer. Under no circumstances shall detailed audit information be shared with the patient at any time. UW-Madison is not obligated to provide a detailed listing of those workforce members who use a patient's PHI for treatment, payment or health care operations.

    a. Should the audit disclose that a workforce member has accessed a patient's PHI inappropriately, the minimum necessary/least privileged information shall be shared with the HIPAA Privacy Coordinator of the unit, and the

workforce member's supervisor or Human Resources Department to determine appropriate sanction/ corrective disciplinary action.

b. Only de-identified information shall be shared with the patient regarding the results of the investigative audit process. This information will be communicated to the patient by UW-Madison HIPAA Privacy Officer or designee, after seeking appropriate risk management or legal counsel.

C. Evaluation and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner by the individual/department responsible for the activity/process (e.g., weekly, monthly, quarterly, etc.).

2. The reporting process shall allow for meaningful communication of the audit findings to those departments/units sponsoring the activity.

a. Significant findings shall be reported immediately in a written format. The procedures in Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information" may be used to report a single event.

b. Routine findings shall be reported to the sponsoring leadership structure in a written report format.

3. Reports of audit results shall be limited to internal use on a minimum necessary/ need-to-know basis. Audit results shall not be disclosed externally without the approval of legal counsel or the UW-Madison HIPAA Privacy Officer.

4. Generic security audit information may be included in organizational reports. Individually-identifiable patient PHI shall not be included in the reports.

5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be

documented and shared with the responsible and sponsoring departments/units.

D. Auditing Business Associate or Vendor Access and Activity

1. Periodic monitoring of business associate and vendor information system activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between UW-Madison and the external agency.

2. If it is determined that the business associate or vendor has exceeded the scope of access privileges, UW-Madison must reassess the business relationship. See Policy # 6.1 "Managing Arrangements with Business Associates of the University of Wisconsin-Madison".

3. If it is determined that a business associate has violated the terms of the HIPAA business associate agreement/addendum, UW-Madison must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

E. Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be available to evaluate a security incident. Generally, system administrators shall not have access to the audit trails or logs created on their systems.

2. Whenever possible, audit trail information shall be stored on a separate system to minimize the impact auditing may have on the audited system and to prevent access to audit trails by those with system administrator privileges. This is done to apply the security principle of "separation of duties" to protect audit trails from hackers. Audit trails maintained on a separate system would not be available to hackers who may break into the network and obtain system administrator privileges. A separate system would allow UW-Madison to detect hacking security incidents.

3. Audit logs maintained within an application shall be backed-up as part of the application's regular backup procedure.

4. UW-Madison shall audit internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required. Auditing of data back-up processes shall be carried out:

    a. On a periodic basis (recommend at least annually) for established practices and procedures.

    b. More often for newly developed practices and procedures (e.g., weekly, monthly, or until satisfactory assurance of reliability and integrity has been established).

F. Workforce Training, Education, Awareness and Responsibilities

1. Workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information. UW-Madison's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies.

2. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies. See Policy # 8.2 "HIPAA Security Oversight"; Policy # 9.1 "HIPAA Privacy and Security Training; Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA Privacy and Security Rules" and Policy # 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules".

G. External Audits of Information Access and Activity

Information system audit information and reports gathered from contracted external audit firms, business associates and vendors shall be evaluated and appropriate corrective action steps taken as indicated. Prior to contracting with an external audit firm, UW-Madison shall:

1. Outline the audit responsibility, authority, and accountability;
2. Choose an audit firm that is independent of other organizational operations;
3. Ensure technical competence of the audit firm staff;
4. Require the audit firm's adherence to applicable codes of professional ethics;
5. Obtain a signed HIPAA-compliant business associate agreement;
6. Assign organizational responsibility for supervision of the external audit firm.

## IV. Documentation Requirements

A. Audit logs and audit trail report information shall be maintained based on organizational needs. Retention of this information shall be based on:

1. Organizational history and experience;
2. Available storage space.

B. Reports summarizing audit activities shall be retained for a period of six years. See HIPAA Security Rule 45 CFR §164.105(c)(2) – Implementation Specification: Retention Period.

## V. Forms

None.

## VI. References

- 45 CFR § 164.308(a)(1)(ii)(D) (HIPAA Security Rule – Information System Activity Review)
- 45 CFR § 164.308(a)(5)(ii)(B) (HIPAA Security Rule – Protection from Malicious Software)
- 45 CFR § 164.308(a)(5)(ii)(C) (HIPAA Security Rule – Log-in Monitoring)
- 45 CFR § 164.308(a)(2) (HIPAA Security Rule – HIPAA Security Rule Periodic Evaluation)
- 45 CFR § 164.308(b) (HIPAA Security Rule – Business Associate Contracts and other Arrangements)

- 45 CFR § 164.312(b) (HIPAA Security Rule –Audit Controls
- 45 CFR § 164.312(c)(2) (HIPAA Security Rule – Mechanism to Authenticate ePHI)
- 45 CFR § 164.312(e)(2)(i) (HIPAA Security Rule – Integrity Controls)
- 45 CFR §164.316(a-b) (HIPAA Security Rule – Documentation)

**Resources**

- HIPAA Collaborative of Wisconsin "Auditing Information System Activity"
- UW-Madison IT Security "Departmental IT Security Baseline"

## VII. Related Policies

- Policy # 1.1 "Designation of UW-Madison Health Care Component"
- Policy # 6.1 "Managing Arrangements with Business Associates of the University of Wisconsin-Madison"
- Policy # 6.2 "Managing Business Associate Arrangements When the University of Wisconsin-Madison is the Business Associate"
- Policy # 6.3 "Use of and Safeguards for Protected Health Information by UW-Madison Internal Business Support Personnel"
- Policy # 8.1 "HIPAA Security Risk Management"
- Policy # 8.2 "HIPAA Security Oversight"
- Policy # 8.4 "HIPAA Security Contingency Planning"
- Policy # 8.7 "Destruction/Disposal of Protected Health Information"
- Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information"
- Policy # 8.9 "HIPAA Security System Access"
- Policy # 8.10 "HIPAA Security Remote Access"
- Policy # 8.11 "HIPAA Security Data Management and Backup"
- Policy # 8.12 "HIPAA Security Facilities Management"
- Policy # 9.1 "HIPAA Privacy and Security Training"
- Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA Privacy and Security Rules"
- Policy # 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules"
- UW-Madison "Computer Logging Statement"

- UW-Madison "Information Incident Reporting and Response"
- UW-Madison "Vulnerability Scanning"

The HIPAA policies listed above are located at: www.hipaa.wisc.edu. The UW-Madison policies are at: www.cio.wisc.edu/policies/.

## VIII. For Further Information

For further information concerning this policy, please contact the UW-Madison HIPAA Security Officer or the appropriate unit's HIPAA Security Coordinator. Contact information is available within the "Contact" tab at www.hipaa.wisc.edu.

## Reviewed By

UW-Madison HIPAA Privacy Officer
UW-Madison HIPAA Security Officer
UW-Madison Office of Legal Affairs

## Approved By

Interim HIPAA Privacy and Security Operations Committee