HIPAA Security Rule

HIPAA Security Procedure - 01

About This Procedure

Effective: 02/01/2018
Last Updated: 12/13/2021

Responsible University Office:
Office of the Chief Privacy Officer

Responsible University Administrator:
Chief Privacy Officer
mawerlin@iu.edu

Procedure Contact:
HIPAA Privacy Officer
HIPAA Security Officer
hipaa@iu.edu

Scope

This procedure applies to all personnel, regardless of affiliation, who create, access or store Electronic Protected Health Information ("ePHI") under the auspices of Indiana University ("University"), and is designated for purposes of complying with the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule.

The University is a covered entity that has selected "hybrid status" under HIPAA, and as a hybrid covered entity, the University designates in writing its operations that perform covered entity functions (health provider, health plan) as healthcare components, which must comply with HIPAA. Additionally, certain units of the University perform business associate functions or other supporting functions, which must also comply with HIPAA. Please refer to the IU Covered Healthcare Components and IU HIPAA Affected Areas designations found on compliance.iu.edu, which are in scope for this procedure. And, for purposes herein, all areas that are in scope for this procedure will be referred to as Affected Areas.

Procedure Statement

As a hybrid entity, the HIPAA Security Rule requires Affected Areas within the University to:

- Put into place appropriate administrative, technical, and physical safeguards to ensure the integrity, confidentiality, and availability of all electronic Protected Health Information (ePHI) that is created, received, maintained or transmitted by the University.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required under 45 CFR part 164, subpart E.
- Ensure compliance with the HIPAA Security Rule by the University workforce.

SECURITY MEASURES

The following security measures address the standards and specifications of the HIPAA Security Rule and reference IU Policy where applicable. Each Affected Area must implement these measures and review and modify their security practices as needed to sustain the reasonable and appropriate protection of the confidentiality, integrity, and availability of ePHI.

Implementation of security measures to address HIPAA requirements should be reasonable and appropriate, taking into account:

- The size, complexity, and capabilities of the Affected Area;
- The Affected Area's technical infrastructure, hardware, and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risk to ePHI.

Documentation requirements

Documentation. To address HIPAA Section 164.316, all Affected Areas will maintain electronic documentation pertaining to any action, activity, assessment, policy, or procedure related to this the implementation of this procedure and the HIPAA Security Rule. This documentation must be available to workforce members responsible for implementing policies and procedures and retained in a secure location for 6 years from the date of creation or the date it was last in effect, whichever is later. Documentation should include proof that the policies are being followed and procedures performed, and those artifacts should be available for review in the event of an audit. Examples include but are not limited to:

- Policies & Procedures, including prior versions
- Risk Analyses (includes ePHI system inventory)
- Risk Management Plans
- Implementation results of Risk Management Plans
- Exceptions to Policies
- Rationale in choosing an Alternate Control
- Documentation related to access control
- Security Incident investigations

Administrative Safeguards

A. Security Management – Section 164.308(a)(1)

1. **Risk Assessment.** To address HIPAA Section 164.308(a)(1)(ii)(A), Risk Analysis, all Affected Areas will assign key workforce members to participate in and support a yearly risk analysis, which may include, but is not limited to their provision of an inventory of workflows, systems, people, processes, technologies, and safeguards related to ePHI. This Risk Analysis will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI managed by the Affected Area. This risk analysis will be managed by the University HIPAA Privacy and Security Compliance Office and will be presented to the area's management, who will provide support for the risk management plan set forth below. Additional risk analysis activities will be performed as needed to support major changes such as the introduction of new systems or new HIPAA Affected Areas.
2. **Risk Management Program**. To address HIPAA Section 164.308(a)(1)(ii)(B). Risk Management, the University HIPAA Privacy and Security Compliance Office will develop a Risk Management Plan in response to the threats and vulnerabilities identified during the risk analysis. Additionally, all Affected Areas will assign resources to support Risk Management Plan implementation activities to reduce ePHI related risks and vulnerabilities to an appropriate level, including:
    - 2.1 Implementation of security measures appropriate in response to threats and vulnerabilities identified during the risk analysis and on an on-going basis as identified.
    - 2.2 Creation of documented evidence to support that security measures implemented to address threats and vulnerabilities identified during risk analysis have sufficiently mitigated or remediated identified risks to an area management acceptable level and comply with general requirements under HIPAA Section 164.306(a).
3. **Sanction Policy**. To address HIPAA Section 164.308(a)(1)(ii)(C), Sanction Policy, all Affected Areas will adhere to the applicable University sanctions policy, refer to IU HIPAA-G01 Sanctions as a guidance.

4. **Information Systems Activity Review**. To address HIPAA Section 164.308(a)(1)(ii)(D), Information System Activity Review, all Affected Areas will assign key workforce members to regularly review information system activity records—including audit logs, access reports, and security incident tracking reports—to ensure that implemented security controls are effective and that ePHI has not been potentially compromised. Measures that each Affected Area will address include:

   4.1 Developing a procedure to review event logging configurations on computer systems managing ePHI to ensure a configuration consistent with IU Policy IT-12 and the Audit Controls section of this procedure to address HIPAA Section 164.312(b).

   4.2 Developing a procedure to review and approve the capabilities of information system activity logs with area management.

   4.3 Developing a procedure for the regular and timely review of audit logs, access exception reports, and security incident reports.

B. Assign Security Responsibilities – Section 164.308(a)(2)

1. **Security Officials.** To address HIPAA Section 164.308(a)(2), Assigned Security Responsibility, the University has named a University HIPAA Security Officer. In addition, each Affected Area will name at least one HIPAA Security Liaison responsible for working with the University HIPAA Security Officer to implement this procedure and safeguards required to protect the confidentiality, integrity, and availability of ePHI. When appropriate, the HIPAA Security Liaison may also serve as the HIPAA Privacy Liaison.
2. **Document Security Responsibility.** To address HIPAA Section 164.308(a)(2), Documenting Security Responsibility, each Affected Area will document the name of the HIPAA Security Liaison, the date they were named a HIPAA Security Liaison, and the scope of their assigned duties.

C. Workforce Security – Section 164.308(a)(3)

1. **Workforce Security**. To address HIPAA Section 164.308(a)(3), Workforce Security, all Affected Areas will establish procedures that ensure workforce members have minimum necessary access to ePHI on the information systems used and supported by their workforce. In addition, all Affected Areas will implement procedures for terminating access to ePHI when the employment of a workforce member ends or the job responsibilities of the workforce member no longer warrants access to ePHI. Measures that each Affected Area will address include:

   1.1 Establishing a procedure that implements IU's Data Governance principle of assigning Data Managers to receive, evaluate, and authorize or deny requests for access to ePHI on information systems supported by an area.

   1.2 Performing appropriate background checks before any person is granted access to ePHI or information systems that store ePHI.

   1.3 Establishing a procedure for Data Managers to regularly review and revalidate workforce members access to ePHI to ensure that access to ePHI is appropriate.

   1.4 Establishing a procedure to remove/disable/modify access to ePHI, collect access control devices, and conduct exit interviews regarding privacy and security of ePHI when the employment of a workforce member ends or the job responsibilities no longer require access to ePHI.

D. Information Access Management – Section 164.308(a)(4)

1. **Information access Management**. To address HIPAA Section 164.308(a)(4), Information Access Management, all Affected Areas will establish procedures that ensure all access to ePHI is appropriately authorized. Measures that each Affected Area will address include:

   1.1 Establishing a procedure to make use of a searchable system to create and track requests and changes to access.

   1.2 Establishing a procedure to define and communicate appropriate workforce access consistent with the University's Minimum Necessary Policy HIPAA-P02 to the appropriate Data Manager and individuals assigned to implement access changes.

1.3 Establishing a procedure to regularly perform a technical evaluation of access controls on information systems storing ePHI to ensure the implementation of the appropriate access.

1.4 Establishing a procedure to isolate clearinghouse functions and to protect ePHI from unauthorized access.

E. Security Awareness and Training – Section 164.308(a)(5)

1. **Security Reminders.** To address HIPAA Section 164.308(a)(5)(ii)(A), Security Reminders, Affected Areas will ensure a procedure is in place to receive and disseminate periodic security updates. Affected Areas will acquire these periodic security updates from the HIPAA Privacy and Security Compliance Office and from sources required by IU Policy IT-12. In addition, Affected Areas will establish a procedure to ensure all members of their workforce complete HIPAA Privacy and Security training as described in IU Policy HIPAA-A02.
2. **Protection from Malicious Software.** To address HIPAA Section 164.308(a)(5)(ii)(B), Protection from Malicious Software, Affected Areas will ensure a procedure is in place to train workforce members of the risks associated malicious software, how malicious software is detected, and to report detections of malicious software as a computer security incident under IU Policy ISPP-26.
3. **Log-in Monitoring.** To address HIPAA Section 164.308(a)(5)(ii)(C), Log-in Monitoring, Affected Areas will ensure a procedure is in place to train their workforce on how to use IU provided monitoring solutions to review personal account activity and to receive log-in alerts. Workforce members must be trained to look for inappropriate login activity and how to respond to inappropriate or attempted log-in attempts.
4. **Password Management**. To address HIPAA Section 164.308(a)(5)(ii)(D), Password Management, Affected Areas will ensure a procedure is in place to train their workforce on how to periodically change their passphrase/password, protect their passphrase/password, and how to respond to compromised passphrase/passwords and other authentication devices.

F. Security Incident Procedures – Section 164.308(a)(6)

1. **Security Incident Procedures.** To address HIPAA Section 164.308(a)(6), Identifying, reporting, and responding to security incidents, Affected Areas will ensure a procedure is in place to train workforce members on IU Policy ISPP-26 Information and Information System Incident Reporting, Management, and Breach Notification and IU Policy IT-12.

G. Contingency Plan – Section 164.308(a)(7)

1. **Contigency Plan.** To address HIPAA Section 164.308(a)(7), a Contingency Plan, all Affected Areas will have procedures in place that include for responding to an emergency or other occurrences that affect the availability of information systems that store, maintain, or transmit ePHI. Measures that each Affected Area should address include:

    1.1 Establishing a procedure for identifying systems used to store, maintain or transmit ePHI.

    1.2 Establishing a procedure for maintaining formal contingency plans, ensuring workforce members understand their role in contingency processes, and regularly testing contingency plans.

    1.3 Establishing a procedure for evaluating the relative criticality of specific information systems and other assets in support of Affected Area business functions or health care processes in order to prioritize systems for data backup, disaster recovery planning, and emergency operation plans.

    1.4 Establishing a and maintaining step-by step to restore exact copies of ePHI using secure backup solutions.

    1.5 Establishing a procedure for regularly reviewing or assessing data backups for reliability and data integrity.

    1.6 Establishing a procedure to identify the events that would require data restoration, step-by-step processes to determine what data will be restored, and how systems will be tested if a full recovery is required.

    1.7 Establishing a procedure for maintaining an emergency mode operation plan that includes the continuity of critical processes related to the security of ePHI while operating in emergency mode.

1.8 Establishing a procedure to update contingency plans based on test results and major changes in information systems.

H. Evaluation – Section 164.308(a)(8)

1. **Evaluation**. To address HIPAA Section 164.308(a)(8), Evaluation, Affected Areas will perform an annual technical and non-technical review, and as necessary in response to major technology or operational changes or newly recognized risks to ePHI, to demonstrate its compliance with this Procedure and the HIPAA Security Rule. Results of the review are to be presented to the Affected Area's management, which will provide a documented response, including remediation steps, for any identified gaps in compliance with this procedure or newly recognized risks to ePHI.

I. Business Associate Contracts and Other Arrangements – Sections 164.308(b) and 164.314(a)

1. **Business Associate Agreements**. To address HIPAA Section 164.308(b) and 164.314(a), Business Associate Agreements, Affected Areas must have a procedure to ensure their workforce are trained to follow IU HIPAA policies, IU Policy DM-02 and IU Guidance HIPAA-G06.

Physical Safeguards

A. Facility Access Controls – Section 164.310(a)

1. **Facility Access Control Analysis**. To address HIPAA Section 164.310(a)(1), Facility Access Controls, Affected Areas will conduct an analysis of existing physical security vulnerabilities of information systems which store, maintain, or transmit ePHI. The analysis will take into account the amount and value of ePHI accessible at each location. The analysis includes an inventory of all system, devices, and media that contain or access ePHI. A physical security plan shall be developed for each location or location type (e.g. research office, outpatient clinic, administrative office, server room or facility), with minimum physical controls to ensure appropriate and timely access to ePHI. The physical security plan, and any policies and procedures needed to execute the plan, will take into account the following:

   1.1 Types of physical access based on role (e.g. workforce member, patient, vendor)

   1.2 Management of physical access (provisioning, auditing, and terminating physical access)

   1.3 Environmental controls commensurate to the criticality of the physical location

   1.4 Physical safeguards appropriate to the facility type, location, and data accessible at each facility or facility type

   1.5 Contingency operations plan for facility access during a disaster or emergency, including accessing data at the alternate processing, storage, and work site

2. **Facility Access Controls**. To address HIPAA Section 164.310(a)(2), Facility Access Controls, Affected Areas will ensure that systems which manage ePHI are kept in areas with physical security controls that restrict access. Each Affected Area will create procedures and provision physical safeguards as appropriate to safeguard ePHI from unauthorized physical access, tampering, and theft. This will include:

   1.1 Controls that prevent unauthorized access to these systems. These controls can include entry doors that require a key, combination locks, biometric authentication, or card readers.

   1.2 Documenting those persons who are permitted authorized access to a facility or location based on role or function.

   1.3 Requiring visitors and non-workforce members to be escorted and monitored by an authorized person when entering and remaining in a facility or location.

   1.4 Providing a log of access to the location as appropriate, which can be either a written log or an electronic record from an ID card reader.

   1.5 As appropriate, environmental controls to sustain optimal operating conditions for computer systems. In the case of a server room or data center, documented temperature, power, and network service levels needed to maintain business operations.

1.6 Ensuring that records of repairs, maintenance, and modifications to physical security related components of a facility managing ePHI are kept, documenting who performed the activity, who authorized the activity, and details of the activity, including dates and times.

1.7 Documentation of decisions regarding room or facility decisions when the physical location cannot be protected to the minimum for the facility or facility type (i.e. leased or shared space).

B. Workstation Use – Section 164.310(b)

1. **Workstation Use.** To address HIPAA Section 164.310(b), Workstation Use, Affected Areas will ensure that only designated workstations compliant with IU Policy IT-12 will be used to access and manage ePHI while in an environment that would prevent or preclude unauthorized access to an unattended workstation, and limit the ability of unauthorized individuals to view ePHI.

C. Workstation Security – Section 164.310(c)

1. **Workstation Security.** To address HIPAA Section 164.310(c), Workstation Security, Affected Areas will ensure that physical safeguards are in place to protect workstations that access and manage ePHI, including as appropriate: cable locks, screens that are turned away from unauthorized users, and access authorization mechanisms that require a user ID and passphrase/password to access the workstation. The workstation should also be configured with a passphrase/password protection feature that is evoked after 15 minutes of inactivity. Additional safeguards should be considered for laptops and remote or public locations where physical security is decreased.

D. Device and Media Controls – Section 164.310(d)

1. **Device and Media Controls**. To address HIPAA Section 164.310(d)(1), Device and Media Controls, Affected Areas will ensure that procedures are in place to govern the receipt and removal of hardware and electronic media that contains ePHI into and out of a facility, and the movement of these items within the facility. Media can include hard disks, tapes, flash drives, CD ROMs, DVDs, optical disks, and other means of storing computer data. Measures that each Affected Area will address include:

    1.1 Establishing procedure to address the disposal ePHI and hardware or electronic media on which ePHI it is stored.

    1.2 Establishing a procedure to proper remove ePHI from electronic media before the media are made available for internal or external re-use.

    1.3 Maintain a record of the location and movements of electronic media and hardware, including the person responsible.

    1.4 Create a retrievable, exact copy (backup) of ePHI as needed, before movement of equipment.

Technical Safeguards

A. Access Control – Section 164.312(a)

1. **Access Control**. To address HIPAA Section 164.312(a), Access Control, Affected Areas will ensure that access controls are in place to protect the integrity and confidentiality of ePHI residing on information systems, including applications, databases, workstations, servers, and network equipment. Measures that each Affected Area will address include:

    1.1 Determine the access granularity, provisioning, auditing, and authentication capabilities of the system.

    1.2 Determine if the system will require remote access, and provide controls as appropriate to safeguard remote access.

    1.3 Assign a unique user ID to track user identity on systems managing ePHI.

    1.4 Establish procedures for obtaining necessary ePHI during an emergency, in which normally unauthorized personnel require access to ePHI or the systems that manage ePHI.

    1.5 Configure systems to terminate a logon session after a predetermine time or period of inactivity. Mechanisms to accomplish logon session terminations include passphrase/password-

protected screen-savers, automatic logoff of the application or network session, and the ability to manually lock out access when leaving a workstation.

1.6 Encrypt devices and media that contain or access ePHI. Documentation of devices and media should include a minimum standard for each approved encryption method, including allowed protocols and key lengths, key management, and any exceptions to the standard.

B. Audit Controls – Section 164.312(b)

1. **Audit Controls**. To address HIPAA Section 164.312(b), Audit Controls, Affected Areas should have audit controls implemented that allow an independent reviewer to review system activity. The following types of audit log events must be logged or a subset of these events may be used based on risk and technical capabilities:

1.1 Log on and logout (Success and Failure)

1.2 Passphrase/Password changes

1.3 All system administration actions

1.4 Switching accounts or running privileged actions from another account (i.e. Linux/UNIX SU or Windows RUNAS)

1.5 Creation or modification of super-user groups

1.6 Clearing the audit log file(s)

1.7 Failures in auditing

1.8 Startup and shutdown of audit functions

1.9 System shutdown and reboot

1.10 System errors

1.11 Application shutdown, restart, and errors

1.12 Security setting modifications

1.13 Change to a file or its user permissions or privileges

1.14 Changes to database settings, records, or ownership

1.15 Account creation, modification, or deletion

1.16 Accessing, creating, modifying, deleting, or printing of ePHI

2. **Content of Audit Logs:**

2.1 Affected areas must ensure that the actions of individual system users can be uniquely traced to those users so they can be associated with their actions. Where technically feasible, logs should contain what type of event occurred, when the event occurred based on an authoritative source, where the event occurred, the source of the event, and the outcome of the event

3. Log Storage and Disposal:

3.1 If technically feasible, security related audit logs will be transferred within 5 minutes to central log management infrastructure which enables processing, reviewing, and alerting on these logs when needed.

3.2 Security related audit logs must be retained for ninety (90) days for immediate recall and an archive of the audit records for one (1) year for after-the-fact investigations of security incidents.

3.3 Logs older than a year should be retained in keeping with the retention policy for the data type, and should be producible within five business days of request.

3.4 The confidentiality, integrity, and availability of security related audit logs and access events related to ePHI considered to be a Legal Health Record must be protected through appropriate technical controls.

C. Integrity – Section 164.312(c)

1. **Integrity.** To address HIPAA Section 164.312(c)(1), Integrity, Affected Areas will implement integrity controls to protect ePHI. Integrity controls should be specified and documented for each information system that stores, processes, or transmits ePHI. Measures that Affected Areas will address include:

   1.1 Establishing processes to protect ePHI from improper alteration or destruction.

   1.2 Establishing processes to detect and respond to improper alteration or destruction of ePHI.

   1.3 For file and record level protection, the Audit Controls specified in Section 164.312(b) should record any changes to a file or data field, sufficient to determine the extent of any unauthorized activity and return the record to its previous state if the record is determined to be altered or destroyed in an unauthorized manner.

D. Person or Entity Authentication – Section 164.312(d)

1. **Authentication.** To address HIPAA Section 164.312(d), Person or Entity Authentication, Affected Areas will have mechanisms in place that verify that a person seeking access to ePHI is the one claimed. Authentication processes for access to ePHI must follow IU Standard DM-01s and use where technically feasible a University provided central authentication service.

E. Transmission Security – Section 164.312(e)

1. **Transmission Security.** To address HIPAA Section 164.312(e)(1), Transmission Security, Affected Areas will have controls in place that guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Measures that each Affected Area will address include:

   1.1 Implement security measures to ensure that the integrity of ePHI is maintained in transit.

   1.2 Implement security measures to encrypt ePHI in transit using algorithms considered to be strong.

   1.3 For each communication channel, the Affected Area will document the encryption method used.

   1.4 Prior to deployment, and periodically thereafter, the transmission will be analyzed to confirm that it is encrypted by utilizing protocol analysis software.

Reason for the Procedure

This procedure sets forth the framework for the University's compliance with the HIPAA Security Rule. It is applicable to those units of the University that have been designated as Affected Areas or any area that may create, access or store ePHI as defined under HIPAA. This procedure is limited to the HIPAA Security Rule. Other aspects of law, including rules governing privacy and human subject research, are addressed in other University policies. See the University's IRB website for policies governing human subject research, and the University's Policies, Procedures and Handbooks web site for policies concerning privacy and computer security.

ePHI includes any electronic data relating to the past, present or future physical or mental health, health care, treatment, or payment for health care. ePHI includes information that can identify an individual, such as name, social security number, address, date of birth, medical history or medical record number, and includes such information transmitted or maintained in electronic format, but excluding certain employment and student records.

History

02/01/2018 New procedure
12/13/2021 Updated procedure contacts

Related Information

HIPAA Privacy and Security Compliance Plan