

HIPAA: Security Safeguards: Electronic Records

□ POLICY

Rev: 11/01/2006

The University of Florida will implement appropriate safeguards to comply with the specifications of the federally mandated Security Rule, which require covered entities to protect the confidentiality and integrity, and to maintain the availability of all electronic protected health information created, received, maintained, or transmitted by the University and affiliated entities. These safeguards include:

- Protection against reasonably anticipated threats or hazards to the security or integrity of such information.
- Protection against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
- Mandatory compliance with the federal Security Rule and Florida State laws by all members of the workforce of medical components of the University of Florida and affiliated entities.

□ DEFINITIONS

Administrative safeguards: administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to guard protected health information and to manage the conduct of the workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability: making data or information accessible and useable upon demand by users.

Encryption: the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Information system: an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity: the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software: software, for example, a virus, designed to damage or disrupt a system.

Password: confidential authentication information composed of a string of characters.

Physical safeguards: physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

Security incident: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards: the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User: a person or entity with authorized access.

Workstation: an electronic computing device or any other device that performs similar functions, and electronic media stored in its immediate environment.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

HIPAA: Security Safeguards: Electronic Records (continued)

□ **PRIVACY REQUIREMENTS**

1. The University of Florida will use security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as specified in the Security Rule.
2. Administrative Safeguards to be implemented:
 - a. Policies and procedures to prevent, detect, contain, and correct security violations.
 - b. Appointment of a Security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.
 - c. Policies and procedures for authorizing access to electronic PHI, for ensuring that all members of the workforce have appropriate access to electronic PHI, and for preventing unauthorized workforce members from obtaining access to electronic PHI.
 - d. A security awareness and training program for all members of its workforce (including management).
 - e. Policies and procedures to investigate security incidents, and recommend appropriate disciplinary action, sanctions, and mitigation.
 - f. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI
 - g. A schedule of periodic technical and nontechnical evaluations that establish the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.
3. Physical Safeguards to be implemented:
 - a. Policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
 - b. Policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.
 - c. Physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.
 - d. Policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.
4. Technical Safeguards to be implemented:
 - a. Policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified above.
 - b. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.
 - c. Policies and procedures to protect electronic PHI from improper alteration or destruction.
 - d. Procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

HIPAA: Security Safeguards: Electronic Records (continued)

- e. Security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

□ PROCEDURES

1. Implementing Administrative Safeguards

- a. *Preventing, Detecting, Containing, and Correcting Security Violations*
 - 1) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity.
 - 2) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
 - 3) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
 - 4) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- b. *Authorizing Access to Electronic PHI*
 - 1) Authorization and/or supervision (Addressable). Authorize defined access and/or supervise workforce members who work with electronic PHI or in locations where it might be accessed.
 - 2) Workforce clearance procedure (Addressable). Determine that the access of a workforce member to electronic PHI is appropriate.
 - 3) Termination procedures (Addressable). Terminate access to electronic PHI when the employment of a workforce member ends or as otherwise required.
- c. *Security Awareness and Training Program*
 - 1) Security reminders (Addressable). Publish and otherwise communicate periodic security updates.
 - 2) Protection from malicious software (Addressable). Establish procedures for guarding against, detecting, and reporting malicious software.
 - 3) Log-in monitoring (Addressable). Monitor log-in attempts, and document and respond to discrepancies.
 - 4) Password management (Addressable). Establish and communicate procedures for creating, changing, and safeguarding passwords.
- d. *Responding to Security Incidents*
 - 1) Identify and respond to suspected or known security incidents;
 - 2) Mitigate, to the extent practicable, harmful effects of identified security incidents; and
 - 3) Document security incidents and their outcomes.
- e. *Contingency Plans for Emergencies*
 - 1) Data backup plan (Required). Create and maintain retrievable exact copies of electronic protected health information.
 - 2) Disaster recovery plan (Required). Restore any loss of data.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

HIPAA: Security Safeguards: Electronic Records (continued)

- 3) Emergency mode operation plan (Required). Enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
 - 4) Testing and revision procedures (Addressable). Periodically test and revise contingency plans.
 - 5) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.
- f. *Evaluation of Security Rule Compliance:* Perform periodic technical and nontechnical evaluations that establish the extent to which the University's security policies and procedures meet the requirements of the Security Rule.
2. Implementing Physical Safeguards
- a. *Limiting Physical Access to Electronic Information Systems*
 - 1) Contingency operations (Addressable). Define contingency routes for facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
 - 2) Facility security plan (Addressable). Establish and maintain safeguards for the facility and the equipment therein from unauthorized physical access, tampering, and theft.
 - 3) Access control and validation procedures (Addressable). Control and validate each person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
 - 4) Maintenance records (Addressable). Document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
 - b. *Workstations*
 - 1) Device and media controls. Monitor and control the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.
 - 2) Disposal of Electronic PHI (Required). Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.
 - 3) Media re-use (Required). Remove electronic PHI from electronic media before the media are made available for re-use.
 - 4) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
 - 5) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.
3. Implementing Technical Safeguards
- a. *Controlling Access*
 - 1) Unique user identification (Required). Assign a unique name and/ or number for identifying and tracking user identity.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

HIPAA: Security Safeguards: Electronic Records (continued)

- 2) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
 - 3) Automatic logoff (Addressable). Terminate an electronic session after a predetermined time of inactivity.
 - 4) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
- b. *Auditing Activity*
- 1) Hardware, software, and/or procedural mechanisms. Record and examine activity in information systems that contain or use electronic PHI.
 - 2) Integrity. Protect electronic PHI from improper alteration or destruction.
 - 3) Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.
- c. *Authentication:* Verify that a person or entity seeking access to electronic protected health information is the one claimed
- d. *Transmission Security*
- 1) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.
 - 2) Encryption (Addressable). Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

REFERENCE: HIPAA § 164.302 – 164.316 (Security Standards); Florida Statutes: 817.568 & 817.5681 (Criminal use of personal information)

EXHIBITS: None