ACTIONABLE IMPLICATIONS FOR COVERED ENTITIES

As with other provisions in the HIPAA legislation, the Final Security Rule has far-reaching implications for the healthcare industry with "real teeth" in terms of enforcement and sanctions. It was purposely written to apply to a range of covered entities – from small provider practices to large-scale practices, hospital systems, and health plans. Covered entities will meet the requirements by complying with the standards set forth in the rule as well as adopting all the required and any number of the addressable implementation specifications.

Given the high-level descriptive nature of the standards, there is a wide degree of flexibility for interpreting how to implement the standards. The "how-to" is driven by the required risk analysis process which should include a due diligence documentation trail supporting the decisions made pertaining to compliance with the standards (i.e., the "Evaluation" requirement.) This is a very important process for a covered entity to complete in order to demonstrate that "reasonable and appropriate" measures were taken to comply with the standards.

Given the compliance deadline of April 21, 2005 (except for small health plans which must comply by April 21, 2006), there are a number of steps that healthcare organizations can, and should, begin to initiate in order to get out in front of the compliance deadline. The following actions have been accorded high priority by numerous healthcare trade associations evaluating the Final Security Rule, including the American Hospital Association, the American Association of Health Plans, the American Association of Integrated Healthcare Organizations, and the Health Insurance Association of America:

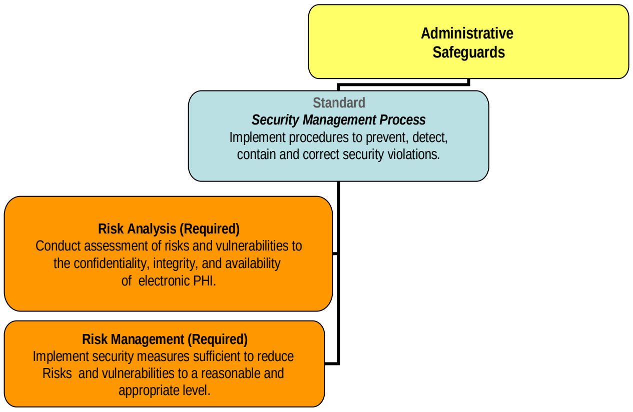
Identify All Electronic PHI Maintained or Transmitted by the Covered Entity

The Final Security Rule applies to all electronic protected health information (PHI). Therefore, covered entities should undertake a PHI mapping process to assess their use and transmission of electronic PHI in order to determine the information and data media that will fall under the requirements.

Perform a HIPAA Security Assessment to Identify Potential Risks and Vulnerabilities (Risk Analysis)

The Administrative Safeguards in the Final Security Rule require covered entities to conduct a Risk Analysis to determine shortfalls and vulnerabilities in security policy and procedures. A gap

Administrative Safeguards Standards and Implementations


Administrative Safeguards
Standard
Security Management Process
Implement procedures to prevent, detect, contain and correct security violations.
Risk Analysis (Required)
Conduct assessment of risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.
Risk Management (Required)
Implement security measures sufficient to reduce Risks and vulnerabilities to a reasonable and appropriate level.

analysis comparing the risk assessment against the Final Security Standards should be one of the first orders of business for covered entities. Ultimately, the determination of whether a covered entity has done enough to comply with the security rule will be based on the effectiveness of the risk analysis process that is employed.

Establish Information Access Control Policies and Procedures.

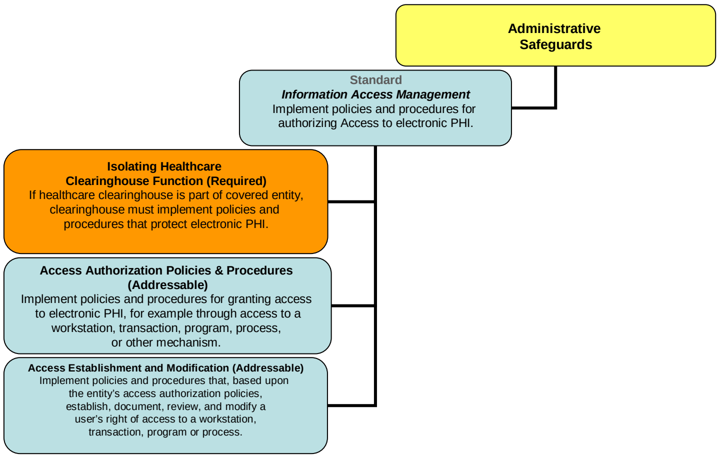
Covered entities should begin to review *access controls* and prepare written policies and procedures to ensure that electronic PHI access is restricted to privileged entities or individuals.

Among the procedures to be considered are implementation of unique log-in names, password protection of electronic files and means of tracking security incidents. In addition, covered entities should draft sanctions procedures for employees who violate the entity's security policies, as well as personnel termination procedures to eliminate access to electronic PHI by former employees.

Develop Mechanisms To Protect Electronic PHI From Improper Use Or Destruction.

Covered entities should begin implementing security mechanisms to verify that electronic PHI has not been altered or destroyed while being transmitted to or from the covered entity. Such measures should include provisions for guarding against unauthorized access to electronic PHI transmitted by the covered entity

Administrative Safeguards
Standards and Implementations



Administrative Safeguards

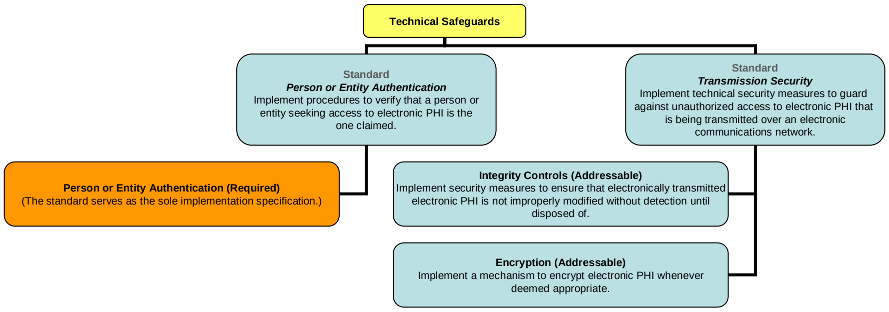
Standard
Information Access Management
Implement policies and procedures for authorizing Access to electronic PHI.

Isolating Healthcare Clearinghouse Function (Required)
If healthcare clearinghouse is part of covered entity, clearinghouse must implement policies and procedures that protect electronic PHI.

Access Authorization Policies & Procedures (Addressable)
Implement policies and procedures for granting access to electronic PHI, for example through access to a workstation, transaction, program, process, or other mechanism.

Access Establishment and Modification (Addressable)
Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process.

Technical Safeguards
Standards and Implementations



Technical Safeguards

Standard
Person or Entity Authentication
Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

Standard
Transmission Security
Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

Person or Entity Authentication (Required)
(The standard serves as the sole implementation specification.)

Integrity Controls (Addressable)
Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

Encryption (Addressable)
Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

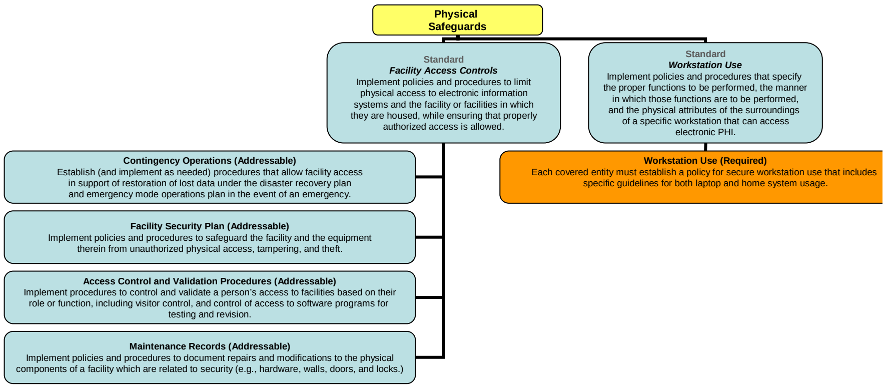
over an electronic communications network such as the Internet.

Conduct Risk Assessment of Physical Safeguards Related To Electronic PHI.

Assess the risks associated with physical safeguards of electronic PHI and implement policies and procedures to limit physical access to electronic information systems and the facility (or facilities) that house this information.

Workstations should also be assessed and policies/procedures formulated for proper safeguarding of electronic PHI (including laptops and home system usage).

Physical Safeguards
Standards and Implementations



Physical Safeguards

Standard
Facility Access Controls
Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Standard
Workstation Use
Implement 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 that can access electronic PHI.

Contingency Operations (Addressable)
Establish (and implement as needed) procedures that allow 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.

Facility Security Plan (Addressable)
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Access Control and Validation Procedures (Addressable)
Implement procedures to control and validate a 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.

Maintenance Records (Addressable)
Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks.)

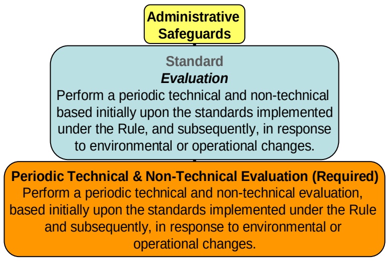
Workstation Use (Required)
Each covered entity must establish a policy for secure workstation use that includes specific guidelines for both laptop and home system usage.

Conduct Thorough Evaluation of Security Measures.

The final rule calls for an evaluation of the security around an entity's electronic PHI, both technical (e.g., architecture) and non-technical (e.g., policies and procedures) elements as defined in the rule.

This evaluation is consistent with the initial proposed rule's concept of "certification" as the "technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements." Each covered entity may elect to perform the evaluation on its own or through an external agency or some combination of both.

Administrative Safeguards
Standards and Implementations



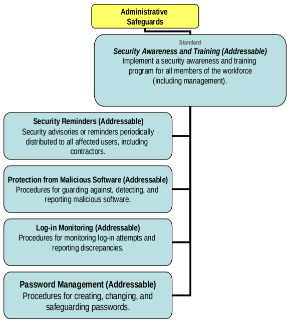
Administrative Safeguards

Standard
Evaluation
Perform a periodic technical and non-technical based initially upon the standards implemented under the Rule, and subsequently, in response to environmental or operational changes.

Periodic Technical & Non-Technical Evaluation (Required)
Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Rule and subsequently, in response to environmental or operational changes.

Develop and Implement Security Awareness Training.

Administrative Safeguards
Standards and Implementations



Administrative Safeguards

Standard
Security Awareness and Training (Addressable)
Implement a security awareness and training program for all members of the workforce (including management).

Security Reminders (Addressable)
Security advisories or reminders periodically distributed to all affected users, including contractors.

Protection from Malicious Software (Addressable)
Procedures for guarding against, detecting, and reporting malicious software.

Log-in Monitoring (Addressable)
Procedures for monitoring log-in attempts and reporting discrepancies.

Password Management (Addressable)
Procedures for creating, changing, and safeguarding passwords.

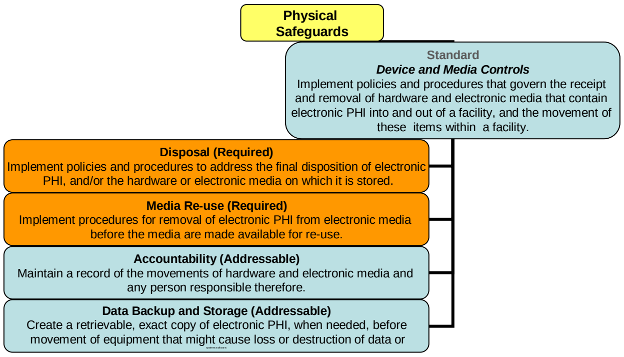
The Final Security Rule requires that covered entities address the “reasonableness and appropriateness” of measures to “implement a security awareness and training program for all members of its workforce (including management). The following items fall into the category of “Security awareness and training:”

- Periodic security reminders and updates
- Procedures for guarding against, detecting, and reporting malicious software
- Procedures for monitoring log-in attempts and reporting discrepancies
- Procedures for creating, changing, and safeguarding passwords

Media Control Policies and Procedures

Develop written policies and procedures for handling and disposal of devices and media that store electronic PHI, to limit inadvertent loss or disclosure of secure information.

Physical Safeguards
Standards and Implementations



Standard
Device and Media Controls
Implement 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 a facility.

Disposal (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.

Media Re-use (Required)
Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

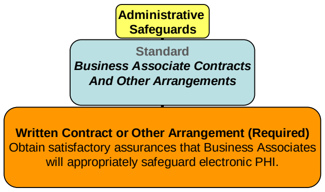
Accountability (Addressable)
Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Data Backup and Storage (Addressable)
Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment that might cause loss or destruction of data or systems software.

Evaluate Business Associate Contracts

Covered entities will need to evaluate, and modify where appropriate, existing Business Associate contracts to ensure that the contract language has stated provisions for appropriately safeguarding all electronic PHI that is received, maintained, and transmitted by the Business Associate, on behalf of the covered entity.

Administrative Safeguards
Standards and Implementations


Administrative Safeguards
Standard
Business Associate Contracts And Other Arrangements
Written Contract or Other Arrangement (Required)
Obtain satisfactory assurances that Business Associates will appropriately safeguard electronic PHI.