



HIPAA Security Rule

A Detailed Review

Ann Geyer
Tunitas Group
209-754-9130
ageyer@tunitas.com
www.tunitas.com





Topics

- ✍ Background Information*
- ✍ Key Definitions and Concepts*
- ✍ Standards and Implementation Specification Details*
- ✍ Compliance Recommendations*



HIPAA Federal Law and Regs

✍ Statutory Requirement -- 1996

- General requirement for information security*
- Framework for security regulation*

✍ Privacy Rule -- 2003

- For **all PHI** (paper, electronic, spoken)*
- Emphasis on Patient Rights and Appropriate Use*

✍ Security Rule -- 2005

- For **electronic PHI***
- Emphasis on Confidentiality, Integrity, and Availability*

HIPAA Compliance Oversight



✍ **Dept of Health & Human Services (DHHS)**

- *Makes regulations*

✍ **Office of Civil Rights (OCR)**

- *Enforces privacy & security regulations; determines civil penalties*

✍ **Dept of Justice (DOJ)**

- *Files criminal indictments*

✍ **Office of Inspector General (OIG)**

- *Incorporates regulations into its sphere of control*

✍ **CMS/Medicare/Joint Commission**

- *Participation; Accreditation*

✍ **CA DHS**

- *Licensing; state level oversight*



Security Rule Summary

✎ Regulatory Purpose

- *Establish a minimum [regulatory] standard for the security of electronic health information used by covered entities*

✎ Compliance Date

- *April 21, 2005*

✎ Scope

- *3 Categories: Administrative, Physical, Technical*
- *18 Standards all required*
- *36 Implementation Specifications:
Required and Addressable (risk justified)*
- *Risk Management & Compliance Framework
Requirements*



HIPAA Security Expectations

✍ **Protect Confidentiality**

- *Directly related to patient privacy*

✍ **Ensure Integrity and Availability**

- *Important patient safety factors*
- *Many factors moving industry toward EMR systems which elevates these concerns*

✍ **Elevate Information Risk Management to the level of other compliance areas**

- *Infection control*
- *Ethical practices*
- *Billing fraud and abuse*

Information Subject to Security Rule

✍ Electronic Protected Health Information (EPHI)

- Which is PHI that is electronically collected, maintained or transmitted by a Covered Entity*
- PHI is any individually identifiable information about a patient that is created, received, processed, or stored by a health plan, clearinghouse, or healthcare provider*

✍ Not Included as EPHI

- Any PHI that is not stored electronically, and*
- Information that was not in electronic form prior to transmission (e.g. voice, paper faxes, film images)*





Changes from Draft to Final

- ✍* **Materially the same**
- ✍* **Many changes made to align Security with Privacy Rule**
 - *Definitions*
 - *Confidentiality and appropriate use safeguards*
 - *Business associate provisions*



Changes from Draft to Final

- ✍ Major re-organization to make Rule more understandable*
 - Consolidates categories and eliminates redundant requirements*
 - Expands the administrative safeguard category*
 - Limits the scope and eliminates esig standard*
 - Creates addressability concept to permit scalability and flexibility to support implementation choice*
 - Clarifies CE is not responsible for transmissions it receives, but is responsible for all EPHI upon receipt*
 - Eliminates distinction between internal and external movement*
 - Clarifies CE must emphasize EPHI availability when establishing security controls*



HIPAA Security Rule

✍ **General Rule** §164.306(a)

Covered Entities must:

1. **Ensure** the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the CE creates, receives, maintains, or transmits
2. **Protect** against any reasonably anticipated threats or hazards to the security or integrity of EPHI
3. **Protect** against any reasonably anticipated uses or disclosures of EPHI that are prohibited by the HIPAA Privacy Rule
4. **Ensure** compliance by the workforce



General Rule Significance

✍ ***Congress intends the Rule to set a high standard***

- *Ensure means to “Make Inevitable”*
- *Perspective adopted by many healthcare attorneys*

✍ ***But Rule also permits Flexibility*** §164.306(b)

- *CE may use any measures that implement the Rule requirements, and*
- *CE must take into account certain factors:*
 - *Size, complexity, and capabilities*
 - *Technical infrastructure, hardware and software security capabilities*
 - *Costs of security measures*
 - *Probability and criticality of potential risks*



Flexibility Provision Creates Conflicting Interpretations

✍ Examples

*CE can live within the limits of existing IS capabilities, or
Current limitations that permit undue risks must be
changed*

*The security measure costs too much, or
The CE didn't allocate sufficient budget to address
security requirements*

*CE can reject security measures that are too complex, or
CE must develop the skills and experience to apply best
available measures*



Resolution Process

✍ Patient Privacy Considerations

- Prudent judgment about undue risk to patients*
- Similar to research requirements*

✍ Regulator Clarifications

- Guidance Documents and FAQs*

✍ Industry Best Practices

- Security Industry or Healthcare Industry*

✍ OCR/DOJ Settlements

- Complaint driven*
- Common approach to other healthcare regulations*
- Led to corporate compliance programs*
- Usually resolved through negotiated settlements*

✍ Courts



What Legal Advisors Are Saying

✍ Responsibility & Liability Defense

- Security should be treated as a major risk management program*
- Security Officer should have (or support an executive with) corporate oversight authority*
- IT documentation should be upgraded to risk management standards*
- Security monitoring should be pro-active; identify risks and respond pre-emptively*
- Security risks and mitigation requirements should be incorporated into project approval decisions.*
- Security should be evaluated and results incorporated in corporate compliance reporting*



HIPAA Security Standards

✍ Simple Description

- The HIPAA Security Standards should be treated as Table of Contents for the Security Plan*
- Security Plan documents the organization's Risk Mitigation Decisions*
- Risk Mitigation is required; although organization has flexibility in choice of security measures*
- Organization is expected to address all likely risks; but may use the flexibility conditions to determine approach to risk mitigation*
- Organization must be prepared to defend its Plan if security breach leads to significant adverse impact on CIA (and patient privacy)*
- Mistakes count!*



Acceptable Risk

✍ Information Risk Management

- Manage the risks that impact the confidentiality, integrity, and availability of PHI*
- Reduce risk to an acceptable level*

✍ What's Acceptable

- Rule says acceptable risk is that which satisfies §164.306(a)*
- Strict Risk Analysis Perspective Too Limiting*
 - Because risk is reduced to a cost-benefit trade-off*
 - Which is organizationally focused; does not consider patient concerns*
 - Often under values the impact of confidentiality breaches*



HIPAA Security Rule

✍ **General Rule** §164.306(a)

Covered Entities must:

1. **Ensure** the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the CE creates, receives, maintains, or transmits
2. **Protect** against any reasonably anticipated threats or hazards to the security or integrity of EPHI
3. **Protect** against any reasonably anticipated uses or disclosures of EPHI that are prohibited by the HIPAA Privacy Rule
4. **Ensure** compliance by the workforce

Security Rule Standards

- ✍ Establish national expectations for healthcare security*
- ✍ Standardizes control categories rather than specific controls*
- ✍ All standards must be implemented*
 - Some of the standards have implementation specifications which may be **REQUIRED** or **ADDRESSABLE***
 - Entity may assess whether an **ADDRESSABLE** implementation specification is reasonable and appropriate safeguard*
 - Implement if reasonable*
 - If not reasonable*
 - Document why*
 - Implement an alternative measure*
 - Only after exhaustive assessment can no measure be implemented*



Compliance Determination

- ✍ ***Rule structures compliance on the basis of risk mitigation***
- ✍ ***CE must demonstrate sufficient understanding of the risks to EPHI***
 - *CE must conduct an “accurate and thorough assessment of the potential risks and vulnerabilities” §164.308 (a)(1)(ii)(A)*
- ✍ ***Non-compliant if***
 - ***Not thorough*** – *failure to consider all significant threats or consequences*
 - ***Not accurate*** -- *failure to adequately estimate the likelihood or impact of a threat or consequence*



Significance

✍ ***Not sufficient to implement a control for each HIPAA security standard***

- *Rule does not create a safe harbor*
- *Set of controls, collectively, must protect EPHI*
- *The Protection burden is high*

✍ ***Focus on policies, standards, procedures***

- *Should identify the risk mitigation expectations*
- *Should define audit programs to demonstrate security measure continues to work as expected*
- *Should establish compliance reporting to demonstrate CE management is “managing risk”*



Standards at a Glance

Category	Standards	Implementation Specifications	
		Required	Addressable
Administrative	9	10	11
Physical	4	2	6
Technical	5	2	5
Total	18	14	22

Administrative Safeguards

✍ Security Management Process

- Risk Analysis* *Required*
- Risk Management* *Required*
- Sanction Policy* *Required*
- Information System Activity Review* *Required*

✍ Assigned Security Responsibility

✍ Workforce Security

- Authorization and/or Supervision* *Addressable*
- Workforce Clearance Procedure* *Addressable*
- Termination Procedures* *Addressable*

✍ Information Access Management

- Isolating Clearinghouse Function* *Required*
- Access Authorization* *Addressable*
- Access Establishment and Modification* *Addressable*

✍ Security Awareness and Training

- Security Reminders* *Addressable*
- Protection from Malicious Software* *Addressable*
- Login Monitoring* *Addressable*
- Password Management* *Addressable*



Administrative Safeguards (cont'd)

✍ Security Incident Procedures

- Response and Reporting* *Required*

✍ Contingency Plan

- Data Backup Plan* *Required*
- Disaster Recovery Plan* *Required*
- Emergency Mode Operation Plan* *Required*
- Testing and Revision Procedure* *Addressable*
- Applications and Data Criticality Analysis* *Addressable*

✍ Evaluation (Audit)

✍ Business Associate Contracts

- Written Contracts or Other Arrangements* *Required*



Physical Safeguards

✍ Facility Access Controls

- Contingency Operations*
- Facility Security Plan*
- Access Control & Validation Procedures*
- Maintenance Records*

Addressable
Addressable
Addressable
Addressable

✍ Workstation Use

✍ Workstation Security

✍ Device and Media Controls

- Disposal*
- Media Re-use*
- Accountability*
- Data Backup and Storage*

Required
Required
Addressable
Addressable



Technical Safeguards

✍ Access Control

- Unique User ID*
- Emergency Access Procedure*
- Automatic Logoff*
- Encryption and Decryption*

Required
Required
Addressable
Addressable

✍ Audit Controls

✍ Integrity

- Mechanism to Authenticate EPHI*

Addressable

✍ Person or Entity Authentication

✍ Transmission Security

- Integrity Controls*
- Encryption*

Addressable
Addressable



Detailed Discussion of the Standards and Implementation Specifications



Administrative Safeguards

✍ **Standard: Security Management Process** §164.308(a)(1)(i)

- *“Implement policies and procedures to prevent, detect, contain and correct security violations.”*

Comments

- *Calls for establishing a security management process that covers the creation, administration, and oversight of policies to address the complete security spectrum and provide for the prevention, detection, containment, and correction of security violations.*
- *Specifications now ordered with respect to priority order (per regulatory perspective)*
- *All implementation specifications considered important enough to be required*



Implementation Specifications

✍ Risk Analysis (required)

- *“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.”*

Comments

- *Depth and scope consistent with type and size of your organization*

Recommendations

- *Systems maintaining PHI*
- *Security processes (security administration, security monitoring, incident response, forensic procedures, and malicious code)*
- *Physical access to facilities containing PHI (data center and other critical operations areas)*
- *Contingency planning*
- *Operating system and platform configurations*
- *Network configurations (wired and wireless)*
- *Data repositories (databases and warehouses)*
- *Portal and web architecture*



Implementation Specifications

✍ Risk Management (Required)

- “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”*

Comments

- Risk Management is the fundamental process required to comply with the Security Rule*
- Includes actions necessary to document and mitigate the risks identified in the risk analysis. Risks must be mitigated to a reasonable and acceptable level.*
- Acceptable level will differ with each covered entity and will be dependent on a number of factors: flexibility factors, the estimated risk, the cost to mitigate, etc.*

Recommendations: *A comprehensive Information Risk Management program should include*

- Incorporating risk identification and mitigation requirements into all new projects*
- Documenting of security implementation decisions*
- Documenting the threats and vulnerabilities to information resources*
- Evaluating the consequences and impacts of EPHI threats*
- Performing periodic security assessments*
- Reporting to management*



Implementation Specifications

✍ Sanction Policy (Required)

- *“Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.”*

Comments

- *Type and severity of sanctions are determined by the CE*
- *Existing policy may be sufficient for this purpose*
- *Important to apply sanctions fairly and uniformly across the workforce*



Implementation Specifications

✍ 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.”*

Comments

- Regulator intent that information system activity be subject to periodic review*
- At a minimum the review should cover system audit logs, access reports, and security incidents reports*
- Flexibility provision leaves the degree and scope up to the CE*
- Also dependent on what implementation and enforcement choices your organization*
- Should balance proactive controls (e.g. privilege assignment and access control) with reactive controls (e.g. audit trails and activity reviews)*



Implementation Specifications

Recommendations

- *Structure a process for exception report review (Who reviews, how often, what information is reviewed, what reporting is required)*
- *Determine what information is needed to create useful exception reports (What audit data, what monitoring, how often, what level of detail)*
- *Procedures for monitoring systems which have no internal auditing or monitoring capabilities*
- *Procedures for monitoring administrators and superusers for policy and procedure compliance*
- *Use monitoring tools where appropriate*
- *Establish monitoring data retention periods*
- *Establish a compliance evaluation program for security policies and procedures (can be a combination of self-audit, internal and external audit)*



Administrative Safeguards

✍ **Standard: Assigned Security Responsibility** §164.308(a)(2)

- “Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [Security Rule] for the entity.”

Comments

- Requirement analogous to the Privacy Officer
- Final Rule requires a **single person** be responsible for development and implementation of the policies and procedures required by the Rule
- Responsibilities include management and supervision for
 - developing and implementing policies and procedures to protect the confidentiality, integrity and availability of EHI
 - the execution and use of security measures to protect data
 - the conduct of personnel
 - monitoring, analyzing and providing a resolution for security violations
- Delegation of responsibilities by the Security Officer is permitted

Administrative Safeguards

Recommendations

- *Level of authority commensurate with responsibility*
- *Things to consider*
 - *How security officer will report compliance to senior management (general compliance requirement)*
 - *Document assignment of responsibilities and identify coordination and compliance reporting relationships*





Administrative Safeguards

✍ **Standard: Workforce Security** §164.308(a)(3)(i)

- *“Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, and to prevent those workforce members who are not authorized to have access under the Information Access Management standard from obtaining access to electronic health information.”*

Comments

- *Requirement to determine what is appropriate access for each workforce category and/or member*
- *Must be consistent with privacy considerations, job responsibilities, minimum necessary privileges*



Implementation Specifications

✍ Authorization and/or Supervision (Addressable)

- *“Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.”*

Comments

- *Preamble explains intent is to manage the activities of operating and maintenance personnel*
- *Recognizes not always possible to have a “knowledgeable person” available to manage*
- *So can set authority levels for such persons and then hold them accountable (similar to finance authority management) or provide general supervision*

Recommendations

- *Determine what functions or work locations require supervision (i.e. workers cannot be left unattended)*
- *Clearly define authority levels for operational and maintenance personnel.*
- *Include personnel who may not touch EPHI, but work in locations where EPHI is accessible*
- *Also personnel who are substituting, training, or otherwise performing operations and maintenance functions outside of their normal responsibilities*



Implementation Specifications

✍ Workforce Clearance Procedure (Addressable)

- “Implement procedures to determine that the access of a workforce member to EPHI is appropriate*

Comments

- Does not mean background checks*
- Intent is motivate a process to review requests for access*

Recommendations

- Use least privilege principle consistent with minimum necessary requirements of the privacy rule*
- Other restrictions derived from privacy policies, job responsibilities, level of risk, supervision and other situational factors*



Implementation Specifications

✍ Termination Procedures (Addressable)

- *“Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by access authorization policies.”*

Comments

- *Covers any personnel to whom you have authorized access; access may be physical or electronic*

Recommendations

- *Set policy for the obvious*
 - *Return or replace locks and combinations*
 - *Remove from access lists*
 - *Terminate access accounts*
 - *Return computers and media*
 - *Delete personal files*
- *Estimate definite timeframes based on criticality*
- *Assign termination responsibilities*



Administrative Safeguards

✍ **Standard: Information Access Management** §164.308(a)(4)(i)

- *“Implement policies and procedures for authorizing access to EPHI.”*

Comments

- *Intent is to ensure there are formal rules for authorizing and assigning access to EPHI and for restricting access*



Implementation Specifications

✍ Isolating Healthcare Clearinghouse Functions (Required)

- “If a CE operates a healthcare clearinghouse, it must implement policies and procedures to protect the EPHI maintained by the clearinghouse from unauthorized access by the larger organization.”*

Recommendations

- Clearinghouse is acting as business associate of its clients*
- Needs Client approval to use or disclose PHI for purposes not directly related to clearinghouse functions*
- Client may need patient authorization if the use or disclosure is not for Treatment, Payment, or Healthcare Operations (TPO)*



Implementation Specifications

✍ Access Authorization (Addressable)

- “Implement policies and procedures for granting access to EPHI, for example through access to a workstation, transaction, program, process, or other mechanism.”*

✍ Access Establishment and Modification (Addressable)

- “Implement policies and procedures that, based on the entity’s access authorization policies, establish, document, review and modify a user’s right of access to a workstation, transaction, program or process.”*

Comments

- Evaluate all ways that a person or entity could access EPHI and make sure that there is a process for controlling access*
- References to user, role, and context access control were removed from the final rule*

Recommendations

- Adopt standardized access control methods across systems and applications wherever feasible*



Administrative Safeguards

✍ **Standard: Security Awareness and Training** §164.308(a)(5)(i)

- *“Implement a security awareness and training program for all members of the workforce including management.”*

Comments

- *HHS has stated that this standard is critical to compliance*
- *The rule allows each CE to determine how to manage awareness and training*
- *All Implementations Specifications are addressable*

Recommendations

- *Establish a system of periodic security reminders and updates*
- *Synch activities to key threats and consequences*
- *Identify when security policies and procedures require training*
- *Use training as part of enforcement efforts*
- *Involve management in the awareness and training promotion*



Implementation Specifications

✍ **Security Reminders** (Addressable)

- “Periodic Security Reminders”

✍ **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”



Administrative Safeguards

✍ **Standard: Security Incident Procedures** §164.308(a)(6)(i)

- *“Implement policies and procedures to address security incidents.”*

Comments

- *HHS removed reference to breach and now uses incident*
- *Security incident is defined as “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system”*
- *Intent is to require a CE to proactively monitor activities that would indicate a problem, investigate and confirm and respond.*
- *Where an authorized use or disclosure is determined, must also address privacy rule requirement for mitigation.*



Implementation Specifications

✍ Response and Reporting (Required)

- *“Identify and respond to suspected or know security incidents; mitigate to the extent practicable harmful effects of the security incidents that are known to the CE; and document security incidents and their outcomes.”*

Comments

- *CE must be able to follow defined policy and procedures for reporting and responding to a confirmed incident.*

Recommendations

- *Procedures should include*
 - *Assignment of responsibilities*
 - *Escalation procedures*
 - *Forensic procedures to capture evidence*
 - *Media plan*
 - *Patient mitigation (privacy requirement)*
 - *Risk Management reporting*



Administrative Safeguards

✍ **Standard: Contingency Plan** §164.308(a)(7)(i)

- *“Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI.”*

Comments

- *Common sense requirement*
- *Requires CE to have a plan for ensuring the CIA of EPHI in an emergency.*
- *Important that plans addresses each of the CIA components*



Implementation Specifications

✍ Data Backup Plan (Required)

- “Establish and implement procedures to create and maintain retrievable exact copies of EPHI.”*

Comments

- Priority on critical systems and on Designated Record Set components*
- Frequency determined by CE on the basis of risk (consequences)*
- Backup media must be treated as EPHI*



Implementation Specifications

✍ Disaster Recovery Plan (Required)

- “Establish (and implement as needed) procedures to restore any loss of data.”*

Comments

- Be able to restore data that is lost as a consequence of a disaster(e.g. fire, vandalism, system failure, power outage, natural disaster)*
- EPHI Backups will exist because of the backup requirement*
- Intent is to have a plan to recover configuration and system data so that operations can be restored.*
- Attention on servers, communications, and infrastructure items*
- Plan should address: appropriate scope, recent system updates, crisis management teams and assignment of responsibilities, and latest testing results.*



Implementation Specifications

✍ Emergency Mode Operation Plan (Required)

- “Establish (and implement as needed) procedures to enable continuation of critical business processes to assure access to EPHI and to provide for adequate protection of EPHI while operating in emergency mode.*

Comments

- Ensure that EPHI is protected even during a disaster, crisis, or emergency*
- Crisis team should be identified to activate contingency and recover plans*
- Team is expected to be knowledgeable in HIPAA requirements and to ensure appropriate actions are taken*
- Should identify and address those operations that cannot safely proceed without EPHI availability*
- Strategy for business operations recovery*



Implementation Specifications

✍ Testing and Revision Procedures (Addressable)

- “Implement procedures for periodic testing and revision of contingency plans*

Comments

- Must assess the need to have contingency and recovery plans tested periodically or when significant changes have been made*
- Is plan sufficient*
- Do personnel understand their responsibilities*
- Was execution of the plan timely*



Implementation Specifications

✍ Applications and Data Criticality (Addressable)

- “Assess the relative criticality of specific applications and data in support of other contingency plan components”*

Comments

- Must assess the need to classify information systems, applications and data*
- For example, whether system stores EPHI or provide access to EPHI*
- Classifications should be useful for managing security in an emergency situation*



Administrative Safeguards

✍ **Standard: Evaluation** §164.308(a)(8)(i)

- *“Perform a periodic technical and non-technical evaluation, based initially upon the security rule standards, and subsequently in response to environmental or operational changes affecting the security of EPHI that establish the extent to which a CE security policies and procedures meet the requirements.”*

Comments

- *Evaluation is an audit function; can be internal or external*
 - *CE is expected to review its overall security system, not just the technical components*
 - *Intent is to evaluate the overall effectiveness of policies, standards, procedures as well as products and controls.*
- *Should cover at a minimum the following items:*
 - *Risk analysis, including threat assessment*
 - *Operating system and network security configurations*
 - *Workforce security compliance*
 - *Access controls and PHI authorization procedures*
 - *Security awareness and training, sufficiency and effectiveness*
 - *Security incidence procedures, including response and reporting*
 - *Physical and transmission security procedures*
 - *Security model (data classification/ownership/)*
 - *Security organizational procedures (assignment of responsibilities/coordination)*
 - *Security architecture and design*



Administrative Safeguards

✍ **Standard: Business Contracts** §164.308(b)(i)

- *“A CE may permit a business associate to create, receive, maintain, or transmit EPHI on its behalf only if the CE obtains satisfactory assurances that the BA will appropriately safeguard the information.”*

Comments

- *Does not cover all parties to whom you may disclose EPHI, just those who are acting on your behalf*
- *BA Agreement must include the terms and conditions required by both the privacy and security rules*
- *New BA agreements must be in place by March 21 2005*

Recommendations

- *Not necessary to spell out specific security measure; but may be a good idea for certain situations*
- *Guard against over specifying or you may end up with the liability*
- *Establish requirements for due diligence of BA security measures*
- *CE is ultimately responsible for selecting BA who adequately protect both the privacy and the security of PHI*



Physical Safeguards



Physical Safeguards

✍ Facility Access Controls

- Contingency Operations*
- Facility Security Plan*
- Access Control & Validation Procedures*
- Maintenance Records*

Addressable
Addressable
Addressable
Addressable

✍ Workstation Use

✍ Workstation Security

✍ Device and Media Controls

- Disposal*
- Media Re-use*
- Accountability*
- Data Backup and Storage*

Required
Required
Addressable
Addressable



Physical Safeguards

✍ **Standard: Facility Access Controls** §164.310(a)(1)

- *“Implement policies and procedures to limit physical access to EPHI systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.”*

Comments

- *Facility is defined as the physical premises and the interior and exterior of a building*
- *All Implementation Specifications are addressable*
- *CE is expected to determine what are reasonable and appropriate controls for securing the physical access to EPHI*
- *What’s reasonable and appropriate needs to be documented using the risk analysis approach (i.e. threats, consequences, vulnerabilities, likelihood, costs to reduce risk to acceptable levels)*
- *Physical security requirements applied to locations that house EPHI are the responsibility of the HIPAA Security Officer, although may be delegated.*

Recommendations

- *Focus on building access and authorization with emphasis on data storage locations*
- *Physical security during emergency operations or at remote facilities*
- *Selection of controls depends on risk analysis*



Implementation Specifications

✍ 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.”*

Comments

- *Reference back to contingency and recovery plans*
- *Even in emergencies, physical controls should be present, although their operations may be different (risk justified)*

✍ Facility Security Plan (Addressable)

- *“Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.”*

Comments

- *Common sense approach*
- *What is needed to make your facility a safe place*
- *What is needed to prevent unauthorized access to EPHI or the locations that contain EPHI*
- *Risk justified decisions*



Implementation Specifications

✍ 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.”*

Comments

- Bit of a catch-all category to cover a requirement for physical access controls*

Recommendations

- Cover workforce members and vendors, contractors, and visitors*
- Establish when escort or identify inspection is required*
- Address operations personnel who may require non-standard access (i.e. after-hours, emergency conditions, trainees, vacation schedule, etc)*
- Evaluate user access to locations and whether restricted areas are warranted*
- Procedures to restrict access to systems and software for testing purposes (separation of duties)*
- Consider how physical security incidents will be handled and reported*



Implementation Specifications

✍ Maintenance Records (Addressable)

- *“Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.”*

Comments

- *Intent is to ensure that changes to physical or hardware environment do not introduce new risks.*
- *May not be reasonable for leased facilities (document)*
- *Consider what physical security controls are required for facilities, whether owned or leased*
- *Also consider remote locations, telecommuters, etc.*
- *Document analysis and requirements*



Physical Safeguards

✍ **Standard: Workstation Use** §164.308(b)

- *“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 or class of workstation than can access EPHI.”*

Comments

- *Controls over workstations that contain or have access to EPHI*
- *Covers all types: desktops, administrators, testing, laptops, wireless devices, pagers, even newer cell phones, and display devices*
- *Don't forget biometric, Rx dispensers, and specialized application terminals*

Recommendations: *Things to consider*

- *Appropriate uses for specific types of workstations and/or certain locations*
- *Trade off of physical access controls with data access controls*
- *Usage guidelines for Affiliate vs personal equipment*
- *Approved software restrictions and licensing requirements*



Physical Safeguards

✍ **Standard: Workstation Security** §164.308(c)

- *“Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.”*

Comments

- *Common sense approach*

Recommendations: Things to consider

- *Asset tags and locks (theft controls)*
- *Physical access controls or encryption of EPHI*
- *Physical location restrictions on use*



Physical Safeguards

✍ **Standard: Device and Media Controls** §164.308(d)(1)

- *“Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within a facility.”*

Comments

- *CE expected to control the movement and removal of EPHI on these types of devices*

Recommendations: Things to consider

- *Guidelines on when EPHI can be removed from Affiliate resources*
- *Authorization procedures to use certain types of media*
- *Inventory control of Affiliate owned media*
- *Guidelines on use of personally owned media*



Implementation Specifications

✍ Disposal (Required)

- *“Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.”*

✍ Media Re-use (Required)

- *“Implement procedures for removal of EPHI from electronic media prior to re-use.”*

Comments

- *CE is expected to establish policies and procedures for safe destruction*
- *Need to address all media used by workforce members*

Recommendations

- *Standard methods for erasing or overwriting media prior to re-use or disposal*
- *Standards for how to destroy media*
- *Make part of security awareness and training*



Implementation Specifications

✍ Accountability (Addressable)

- “Maintain a record of the movement of hardware and software and any person responsible for movement.”*

Comments

- Assess need to know where hardware and software is and who is responsible for it*
- Procedures should address inventory control requirements, equipment tracking, requirements for portable equipment*
- Don't forget the biometric and clinical device equipment*



Implementation Specifications

✍ Data Backup and Storage (Addressable)

- “Create a retrievable, exact copy of EPHI, when needed, prior to moving equipment.”*

Comments

- As part of the Data Backup Plan Administrative Requirement, already backing up EPHI on a routine basis*
- Here intention is to determine when backup is required prior to moving equipment*



Technical Safeguards



Technical Safeguards

✍ Access Control

- Unique User ID*
- Emergency Access Procedure*
- Automatic Logoff*
- Encryption and Decryption*

Required
Required
Addressable
Addressable

✍ Audit Controls

✍ Integrity

- Mechanism to Authenticate EPHI*

Addressable

✍ Person or Entity Authentication

✍ Transmission Security

- Integrity Controls*
- Encryption*

Addressable
Addressable



Technical Safeguards

✍ **Standard: Access Control** §164.312(a)(1)

- *“Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those person or software programs that have been granted access rights as specified.”*

Comments

- *Intent is clearly to require access controls*
- *Final rule provides more flexibility, by eliminating reference to any type of technical access control*



Implementation Specifications

✍ Unique User Identification (Required)

- “Assign a unique name and/or number for identifying and tracking user identity.”*

Comments

- Required to ensure that all users are uniquely identified*

Recommendations

- Consider user profiles to implement separation of duties*
- Be consistent with privacy policies, especially minimum use restrictions*
- Consider needs of monitoring, audit trails, and security incidence investigations*



Implementation Specifications

✍ Emergency Access Procedure (Required)

- “Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency*

Comments

- Access control procedures must address access during emergency situations*

Recommendations

- Guidelines for granting emergency access*
- Logging activity during an emergency*
- Revoking emergency access at end of emergency*
- Review of activities during the emergency*
- Establishing and separating emergency access accounts*



Implementation Specifications

✍ Automatic Logoff (Addressable)

- *“Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.”*

Recommendations

- *Evaluate when automatic log-off is reasonable and appropriate*
- *Establish standard procedures*

✍ Encryption and Decryption (Addressable)

- *“Implement a mechanism to encrypt and decrypt EPHI.”*

Comments

- *Decision to encryption or not must be risk justified*
- *If require encryption, should provide policies and procedures for users and technical support*
- *Standardize acceptable encryption methods*



Technical Safeguards

✍ **Standard: Audit Controls** §164.312(b)

- *“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.”*

Comments

- *Audit Controls are required*
- *Must implement auditing, logging, and monitoring controls to provide sufficient information to enable security incident identification and investigation*
- *Reasonable and appropriate controls are risk justified*
- *Requires documentation of decisions*
- *Controls enable CE to meet Administrative Safeguard requirements*

Recommendations: *Examples of monitoring events*

- *Switching user id during a session*
- *Password failures*
- *Attempts to use unauthorized privileges*
- *Modifications to production applications*
- *Modifications to system software, especially configurations*
- *Changes to user privileges*
- *Changes to logging subsystems*



Technical Safeguards

✍ **Standard: Integrity** §164.312(c)(1)

- *“Implement policies and procedures to protect EPHI from improper alteration or destruction.”*

✍ **Implementation Specification: Authentication EPHI (Addressable)**

- *“Implement electronic mechanisms to corroborate the EPHI has not been altered or destroyed in an unauthorized manner.”*

Comments

- *Addresses the need to have integrity controls for stored data*
- *Selection of method must be risk justified*
- *Attention not just to the EPHI, but also to operations that could modify data (e.g. file maintenance, restoral procedures, system updates, etc)*



Technical Safeguards

✍ **Standard: Person or Entity Authentication** §164.312(d)

- *“Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.”*

Comments

- *Authentication is defined as a process utilized by a system to confirm the identify of a user by means of account validation and/or password verification schemes.*
- *No specific implementation is required*
- *Can use any method deemed appropriate (risk justified)*



Technical Safeguards

✍ **Standard: Transmission Security** §164.312(e)(1)

- *“Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.”*

Comments

- *Applies to all types of networks, no exceptions*
- *Two addressable implementation specifications*



Implementation Specifications

✍ Integrity Controls (Addressable)

- “Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.*

Comments

- Controls to ensure integrity*
- Often included in transmission protocol*
- May be basis for requiring BA to use certain protocols*



Implementation Specifications

✍ Encryption (Addressable)

- “Implement a mechanism to encrypt EPHI whenever deemed appropriate.”*

Comments

- OCR expects larger organizations to begin using encryption*
- Files or messages that contain lots of data or more sensitive EPHI are targets*
- Can avoid encryption, but only if risk justified*
- Encryption is safe harbor*
- Only need encryption PHI Identifiers*
- Preamble calls for special attention to email encryption by providers*
- Preamble seems to permit exception if encryption would interfere with provider (physician) communications because of interoperability issues*



Organizational Requirements

✍ **Standard: Business Associate Contracts** §164.314(a)(1)

- *“The contract between the CE and its BA must meet the [following] requirements, as applicable:*
- *A CE is not in compliance if it knew of a pattern of activity or practice of the BA that constituted a material breach or violation of the BA’s obligation under the contract, unless the CE took reasonable steps to cure the breach or end the violation, and if such steps were unsuccessful to*
 - (A) terminate the contract, if feasible; or*
 - (B) report the problem to the Secretary of HHS, if not.*

Comments

- *Same requirements as for Privacy Rule*
- *No obligation to actively monitor BA operations*
- *Must take action, if a problem becomes known*
- *Security Rule requires the BA to report security incidences (see implementation specifications)*



Implementation Specifications

✍ Business Associate Contracts (Required)

- “The contract between a CE and BA must provide for the following:
 - (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the CIA of EPHI that it creates, receives, maintains, or transmits on behalf of the CE, as is required by the Security Rule*
 - (B) Ensure that any agent, including subcontractors, to whom the BA provides such information agrees to implement reasonable and appropriate safeguards;*
 - (C) Report to the CE any security incident of which it becomes aware; and*
 - (D) Authorize termination of the contract, if the CE determine that the BA has violated a material term of the contract.**

Comments

- Require the BA to be knowledgeable about HIPAA regulations*
- If possible, obligate the BA to comply with the Security Rule safeguards (risk justified decisions)*
- Provide guidelines on what security incidents are meaningful*
- Establish a compliance reporting mechanism*



Policies and Procedures

✍ **Standard: Policies and Procedures** §164.316(a)

- *“Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements.”.*

Comments

- *Policies and procedures may be changed at any time, but changes need to be documented*
- *Policy versions need to be retained for 6 years after their last effective date (documentation requirement)*
- *HHS expects that many policies and procedures already exist or which could be modify as necessary to comply with the security rule*



Documentation

✍ **Standard: Documentation** §164.316(b)(1)

- *“Maintain the policies and procedures required by the security rule in writing which may be electronic; and*
- *If an action, activity, or assessment is required to be documented, maintain a written record which may be electronic.”*

Comments

- *Covers all policies and procedures, plans, responses, and the risk analyses that justify security decisions*
- *Documentation must be retained for 6 years after its last effective date (same as privacy)*
- *Consensus that requirement applies to includes system and network configuration documentation as well as training materials*
- *Documentation must be available to those within the organization that need to know and comply (publication and access requirement)*
- *Must be reviewed periodically and updated as needed in response to environment and operational changes (e.g. security incident, new vulnerability, system changes, personnel changes, etc)*



Implementation Specifications

✍ Time Limit (Required)

- *“Retain the documentation required by the Security Rule for 6 years from the date of its creation or the date when it was last in effect, whichever is later.”*

✍ Availability (Required)

- *“Make documentation available to those person responsible for implementing the procedures to which the documentation pertains.”*

✍ Updates (Required)

- *“Review documentation periodically, and update as needed, in response to environmental and operational changes affecting the security of the EPHI.”*