Electronic Health Records: Data Security and Integrity of e-PHI

MLCHC Annual Clinical Conference
Worcester, MA
Wednesday, November 12, 2014
2:15pm – 3:30pm

Massachusetts League
of Community Health Centers

Agenda

Introduction
- Learning Objectives
- Overview of HIPAA

HIPAA: Privacy and Security

HIPAA: The Security Rule
- General Rules
- Protected Health Information (PHI) and Safeguarding PHI

Case Study
- Findings
- Resolution and Mitigation Plan

PHI Breach and Breach Reporting

Learning Objectives

- Identify key components and institutionalization of policies and procedures governing security of PHI.
- Identify tools and best practice workflows for EHR documentation to protect health information.
- Discuss options for resolving or mitigating common EHR documentation pitfalls and challenges.

Overview of HIPAA

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by Congress to establish a national framework for security standards and protection of confidentiality with regard to health care data and information. Before HIPAA there was no universally recognized security standard or basic mandates for Protected Health Information (PHI).
- The goal of HIPAA is to protect patients' confidentiality while enabling healthcare organizations to pursue initiatives that further innovation and patient care.

- The Office for Civil Rights (OCR) is responsible for administering and enforcing, the major provisions of HIPAA.
  - **The HIPAA Privacy Rule** protects the privacy of individually identifiable health information or PHI by establishing standards for the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used.
  - **The HIPAA Security Rule** establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).
  - The **HIPAA Breach Notification Rule** requires covered entities and business associates to provide notification following a breach of unsecured protected health information.
  - The confidentiality provisions of **the Patient Safety Rule** protect identifiable information being used to analyze patient safety events and improve patient safety.

- The scope of privacy and security protections under HIPAA was broadened in 2009 when the Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17, 2009. The HITECH Act:
  - Was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology.
  - Addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
- Under the HITECH Act of 2009, the EHR Incentive Program was established to provide incentive payments to Eligible Professionals, Eligible Hospitals and Critical Access Hospitals to adopt, implement, upgrade and demonstrate the meaningful use of certified electronic health record (EHR) technology.

HIPAA: Privacy and Security

The Privacy Rule

- Focuses on the right of an individual to understand and control the use of his or her personal information: PHI should not be divulged or used by others against an individual's wishes.
- Covers the confidentiality of PHI in all formats including electronic, paper and oral.
- Assures that PHI will be safeguarded from unauthorized disclosure while allowing the flow of health information to provide and promote high quality health care.

The Security Rule

- Focuses on administrative, technical and physical safeguards of e-PHI.
- Protects e-PHI that is created, received, used or maintained by a covered entity. This includes e-PHI that is external or internal, stored or in transit.
- Promotes the integrity and availability of e-PHI.
  - Integrity: e-PHI is not altered or destroyed in an unauthorized manner.
  - Availability: e-PHI is accessible and usable on demand by an authorized person.

HIPAA: The Security Rule

- The Security Rule establishes standards for protecting certain health information that is held or transferred in electronic form, such as an EHR.
- The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that "covered entities" must put in place to secure individuals' e-PHI.
  - "Covered entities" under the Security Rule include health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA.

- Covered entities must obtain assurances from "Business Associates" - persons or entities that perform functions or activities that may involve use or disclosure of PHI on behalf of the covered entities – that they, the business associates, will appropriately safeguard PHI.

- A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.
- The Security Rule is also designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

The HIPAA Security Rule: General Rules

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.
- Specifically, covered entities must:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce.

What is PHI or Protected Health Information?

- PHI is any individually identifiable health information or information that is a subset of health information, including demographic information, that is collected from an individual and is created or received by a covered entity and that relates to the individual's past, present, or future physical or mental health condition or any other information that can be reasonably used to identify the individual.
- The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

- Common examples of PHI:
  - Names
  - Addresses
  - Dates (birth, admission, discharge, death)
  - Telephone and fax numbers
  - E-mail addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Full face photographic images and any comparable images
  - Certificate/License and account numbers
- Individually identifiable health information excluded as PHI includes:
  - Employment records held by a covered entity in its role as employer
  - Education records covered by the Family Educational Rights and Privacy Act

Key Provisions for Safeguarding PHI

- As noted previously, the HIPAA Security Rule requires that covered entities provide safeguards for protecting e-PHI. To help covered entities assure the confidentiality, integrity, and availability of all e-PHI, series of administrative, technical and physical security procedures have been established. The key elements of the Security Rule include:
  - Risk Analysis and Management
  - Administrative, Physical and Technical Safeguards
  - Organizational Requirements
  - Policies and Procedures and Documentation Requirement

- Establishing policies and procedures to address the safeguards is key to ensuring that e-PHI is secure and mitigates risk for potential breach or unauthorized disclosure of e-PHI.
- On-going review and update of policies and procedures for compliance with the HIPAA Security Rule is required.
- Conducting a security risk analysis – a key element of the Security Rule – is a core measure for achieving meaningful use for the CMS EHR Incentive Programs. Failed audits for the EHR Incentive Programs have been primarily due to inadequate security risk analysis and documentation.

Risk Analysis and Management

- At minimum, a security risk analysis must be conducted annually.
- The analysis process must include:
  - Review of administrative, physical and technical safeguards in place to ensure e-PHI is secure.
  - Documentation of findings and an assessment of risk for unauthorized disclosure or use and/or breach of e-PHI.
  - A risk mitigation plan that documents the measures that will be taken to address the findings and the rationale for doing so.
  - Maintaining continuous, reasonable and appropriate security protections.

Sample Risk Scoring Tool

Effect	Value	Severity of Effect	Failure Probability	Detection of Effect	Priority		
None	1	No Risk to PHI as a result of the identified vulnerability	The identified vulnerability will never occur	The identified vulnerability will always be detected prior to compromise of PHI	**Low**	1	**RPN: 1-10**
Minor	2	Minor Risk that PHI will be compromised	The identified vulnerability is theoretically possible but is most unlikely to occur	The indentified vulnerability has a high likelihood of detection prior to compromise of PHI	**Medium Low**	2	**RPN: 11-25**
Moderate	3	Moderate Risk that PHI will be compromised	The identified vulnerability is likely to occur	The indentified vulnerability is likely to be detected prior to compromise of PHI	**Medium High**	3	**RPN: 26-49**
High	4	High Risk that PHI will be compromised	The identified vulnerability is extremely likely to occur	The indentified vulnerability is unlikely to be detected prior to compromise of PHI	**High**	4	**RPN: ≥50**
Catastrophic	5	PHI will be always be compromised as a result of the identified vulnerability	The identified vulnerability will always occur	The indentified vulnerability will never be detected prior to compromise of PHI			

Sample Security Risk Assessment

Vulnerabilities and Risks:
HIPAA Security Rule sections are color coded to identify the key areas of review:

Security Standards General Rule	Administrative Safeguards	Physical Safeguards	Technical Safeguards	Organizational Requirements

The table below includes risks identified through our risk assessment process. The specific area addressed is color coded as per above. The risks are listed in order of priority.

Area	HIPAA Security Rule	Identified Vulnerability	Associated Risk	Severity	Probability	Detection	Calculated RPN	Priority
Organizational	Business Associates Contracts & Other Arrangements	BACs are not tracked for accuracy or expiration. No written policy and procedure and no appropriate security language to ensure contractors, subcontractors and other covered entities safeguard PHI.	Inappropriate access to PHI granted.	4	4	4	64	4
Admin	Sanction Policy	Policies and procedures for worker sanctions due to PHI security violations are not current.	PHI security violations and improper sanctions.	4	3	4	48	3
Physical	Workstation Security	No policy addressing the risk of security breach posed by having document containing PHI visible and/or unattended on the organization's premises.	PHI security breach.	4	3	4	48	3
Technical	PHI Integrity	Procedures not documented for installing system patches and updates and anti-virus SW updates.	System and PHI vulnerable to inappropriate access, alteration and/or corruption.	4	3	3	36	3

Sample Risk Mitigation Plan

High Level Risk Mitigation Plan:

To address the above risks, we have identified the following mitigation plan. The plan includes the project lead and the expected completion date. Detailed project plan and budget will be developed upon approval of the proposed Risk Mitigation Plan:

Area	HIPAA Security Rule	Identified Vulnerability	Associated Risk	Mitigation	Lead	Completion Date
Organizational	Business Associates Contracts & Other Arrangements	BACs are not tracked for accuracy or expiration. No written policy and procedure and no appropriate security language to ensure contractors, subcontractors and other covered entities safeguard PHI.	Inappropriate access to PHI	Establish process to determine when a BAC is required, what must be included in the BAC, length of time BAC will be in effect. Conduct review of all current BACs to ensure compliance with HIPAA security regulations.	Jones	November 2013
Admin	Sanction Policy	Policies and procedures for worker sanctions due to PHI security violations are not current.	PHI security violations and improper sanctions.	Draft policies and procedures that clearly identify employee sanctions due to PHI breaches or potential breaches. Incorporate HIPAA security breach checklist to determine level of risk and appropriate sanctions.	Smith	December 2013
Physical	Workstation Security	No policy addressing the risk of security breach posed by having document containing PHI visible and/or unattended on the organization's premises.	PHI security breach.	Draft and incorporate a Clear Desk Policy detailing how sensitive information should be kept from view by the public into the policies and procedures manual and staff training program. Conduct spot checks to ensure adherence to the policy.	Jones	January 2014
Technical	PHI Integrity	Procedures not documented for installing system patches and updates and anti-virus SW updates.	System and PHI vulnerable to inappropriate access, alteration and/or corruption.	Incorporate procedures for installing system patches and updates and for managing Symantec Endpoint anti-virus management program into policies and procedures.	Smith	December 2013

Mitigation plans related to policy and procedure will be reflected by appropriate dated revisions in the organization's policy and procedures manuals.

Administrative Safeguards: Key Provisions

- Focus on establishing and maintaining a **Security Management Process.**
- Identify **Security Personnel** who is responsible for developing and maintaining the security policies and procedures.
- Establish policies and procedures for **Information Access Management** to:
  - Limit uses and disclosures of PHI to the "minimum necessary".
  - Ensure user or recipient is authorized and granted access to e-PHI based on role.
- Implement a **Workforce Training and Management** program to:
  - Ensure all staff are trained on security policies and procedures.
  - Ensure appropriate sanctions against staff who violate policies and procedures.
- Establish **Security Incident Procedures** for reporting and responding to an incident, including breach assessment and response.
- Establish a **Contingency Plan** for protecting and accessing e-PHI in emergencies.
- Conduct **periodic assessment** of effectiveness of security policies and procedures and how well they meet the current requirements of the Security Rule and revise as necessary.

- Example 1: Timely removal of access to EHR or e-PHI of terminated staff
- Example 2: Documentation of on-going training for staff, at minimum annually, and as needed whenever security requirements change. This includes update of policies and procedures as well as sanctions.
- Example 3: Contingency planning for securing e-PHI during emergency situations.

Physical Safeguards: Key Provisions

- Establish appropriate **Facility Access and Control** to limit physical access to areas where PHI can be accessed while ensuring that appropriately authorized access is allowed.
- Implement policies and procedures for Workstation and Device Security that:
  - Specifies proper use of and access to workstations and electronic media; and
  - Ensures protection of e-PHI when electronic media is transferred, removed, disposed of or re-used.

- Example 1: Removal and protection of e-PHI from equipment or media when disposing of, transferring, removing, or re-using.
- Example 2: Facility access procedures for personnel to control access to server rooms where e-PHI is stored.
- Example 3: Document maintenance records for security related repairs and modifications.

Technical Safeguards: Key Provisions

- Implement technical policies and procedures for **Access Control** that only allows authorized individuals to access e-PHI.
- Implement **Audit Controls** for hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- Implement policies and procedures for **Integrity Controls** to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- Ensure **Transmission Security** by implementing technical measures that guard against unauthorized access to electronically transmitted e-PHI.

- Example 1: Automatic log-off and session termination from EHR.
- Example 2: Timely signing off and locking of clinical notes.
- Example 3: Appropriate encryption of transmitted e-PHI and devices that store e-PHI.

Organizational Requirements: Key Provisions

- **Covered Entity Responsibilities**. If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.
- **Business Associate Contracts.** Effective 2013, HHS developed additional regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.
- **Policies and Procedures and Documentation Requirements.** Reasonable and appropriate policies and procedures must be implemented to comply with the provisions of the Security Rule.
  - Written security policies and procedures and written records of required actions, activities or assessments must be maintained, until six years after the later of the date of their creation or last effective date.
  - **Updates.** A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security e-PHI.

- Example 1: Maintain up-to-date, HIPAA compliant BACs.
- Example 2: Documentation and notification to staff of changes in procedures via change management policies and procedures.
- Example 3: Policies and procedures to ensure against breaches, cure the breach and/or end the violation.

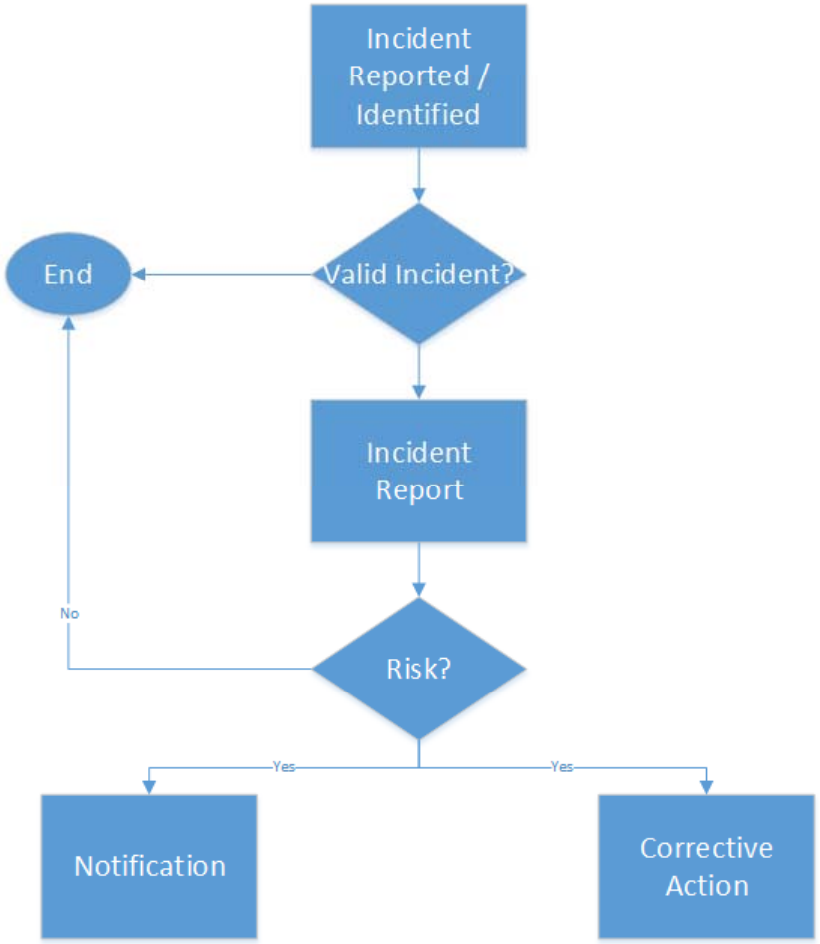
Case Study: Hucknall Community Health Center

- Break to review case study (15 minutes)
- Group Discussion (30 minutes)
  - Identify potential risks to e-PHI
  - Identify potential mitigation steps

PHI Breach: What Next?

- Definition of Breach
  - A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- Reporting of Breaches
  - **Individual.** Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information within 60 days.
  - **Notice to the Secretary.** In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and completing the Breach Notification form. (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)
  - **500 or more records:** Reported within 60 days after the breach.
  - **Less than 500 records:** Reported annually and no later than 60 days after the end of the calendar year.

Breach Reporting



- Compromise the security and privacy of the PHI" means that the breach poses a significant risk of financial, reputational or other harm to the individual.
- The four factor risk assessment includes:
  - The nature and extent of PHI involved;
  - To whom the disclosure was made;
  - Whether the PHI was actually viewed or acquired; and
  - The extent to which the risk to the PHI has been mitigated.

Closing: Questions?

Adrian Bishop
abishop@ahpnet.com

Nancy Tabarangao
nancy.tabarangao@verizon.net

Good health. Right around the corner.

40 Court Street, 10th Floor
Boston, MA 02108
ph 617-426-2225
www.massleague.org

Massachusetts League
of Community Health Centers

Resources

Summaries of the rules discussed here, as well as links to the full text and training materials, can be found on the US Department of Health and Human Services website by using this link: http:www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

- NACHC Information Bulletin, August 2013, *Four-Factor Risk Assessment for Determining Whether PHI Has Been Compromised*
- AHIMA. "Integrity of the Healthcare Record: Best Practices for EHR Documentation." *Journal of AHIMA* 84, no.8 (August 2013): 58-62. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050286.hcsp?dDocName=bok1_050286

ATTACHMENT: HIPAA SECURITY RULE - SUMMARY

HIPAA Security Requirements						
Eligible Professional Meaningful Use Core Measure - Protect Electronic Health Information						
Objective		**Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.**				
Measure		**Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.**				
Item	**HIPAA Citation**	**HIPAA Security Rule Standard Implementation Specification**	**Requirement Summary**	**Implementation Required or Addressable**	**Check if Pertinent to Organization**	**Requirement**
SECURITY STANDARDS: GENERAL RULES						
1	**164.306(a)**	**Ensure Confidentiality, Integrity and Availability**	**P&P to manage security violations**		X	(a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.
2	164.306(b)	Flexibility of Approach	Conduct vulnerability assessment		X	(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The covered entity's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.
3	164.306(c)	Standards	Implement security measures to reduce risk of security breaches		X	A covered entity must comply with the standards as provided in this section and in §164.308, §164.310, §164.312, §164.314, and §164.316 with respect to all electronic protected health information.
4	164.306(d)	Implementation Specifications	Worker sanction for P&P violations		X	In this subpart: (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification. (2) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (3) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity must— (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity— (A) Implement the implementation specification if reasonable and appropriate; or (B) If implementing the implementation specification is not reasonable and appropriate— (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and, (2) Implement an equivalent alternative measure if reasonable and appropriate.
5	164.306(e)	Maintenance	Procedures to review system activity		X	Security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at §164.316.

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
ADMINISTRATIVE SAFEGUARDS						
1	**164.308(a)(1)(i)**	**Security Management Process**	**P&P to manage security violations**	**Required**	X	Implement policies and procedures to prevent, detect, contain and correct security violations
2	164.308(a)(1)(ii)(A)	Risk Analysis	Conduct vulnerability assessment	**Required**	X	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
3	164.308(a)(1)(ii)(B)	Risk Management	Implement security measures to reduce risk of security breaches	**Required**	X	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.206(a).
4	164.308(a)(1)(ii)(C)	Sanction Policy	Worker sanction for P&P violations	**Required**	X	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
5	164.308(a)(1)(ii)(D)	Information System Activity Review	Procedures to review system activity	**Required**	X	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
6	**164.308(a)(2)**	**Assigned Security Responsibility**	**Identify security official responsible for P&P**	**Required**	X	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
7	**164.308(a)(3)(i)**	**Workforce Security**	**Implement P&P to ensure appropriate PHI access**	**Required**	X	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a))(4) of this section from obtaining access to electronic protected health information.
8	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Authorization/supervision for PHI access	Addressable	X	Implement procedures for authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
9	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Procedures to ensure appropriate PHI access	Addressable	X	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
10	164.308(a)(3)(ii)(C)	Termination Procedures	Procedures to terminate PHI access	Addressable	X	Implement procedures for termination access to electronic protected health information when the employment of a workforce member ends or as required by determination made as specified in paragraph (a)(3)(ii)(B) of this section.
11	**164.308(a)(4)(i)**	**Information Access Management**	**P&P to authorize access to PHI**	**Required**	X	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
12	164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	P&P to separate PHI from other operations	**Required**	X	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement polices and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
13	164.308(a)(4)(ii)(B)	Access Authorization	P&P to authorize access to PHI	Addressable	X	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process or other mechanism.
14	164.308(a)(4)(ii)(C)	Access Establishment and Modification	P&P to grant access to PHI	Addressable	X	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.

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
ADMINISTRATIVE SAFEGUARDS						
15	**164.308(a)(5)(i)**	**Security Awareness Training**	**Training program for workers and managers**	**Required**	X	Implement a security awareness and training program for all members of its workforce (including management).
16	164.308(a)(5)(ii)(A)	Security Reminders	Distribute periodic security updates	Addressable	X	Periodic security updates.
17	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Procedures to guard against malicious software	Addressable	X	Procedures for guarding against, detecting, and reporting malicious software.
18	164.308(a)(5)(ii)(C)	Log-in Monitoring	Procedures and monitoring of log-in attempts	Addressable	X	Procedures for monitoring log-in attempts and reporting discrepancies.
19	164.308(a)(5)(ii)(D)	Password Management	Procedures for password management	Addressable	X	Procedures for creating, changing, and safeguarding passwords.
20	**164.308(a)(6)(i)**	**Security Incident Procedures**	**P&P to manage security incidents**	**Required**	X	Implement policies and procedures to address security incidents.
21	164.308(a)(6)(ii)	Response and Reporting	Mitigate and document security incidents	**Required**	X	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
22	**164.308(a)(7)(i)**	**Contingency Plan**	**Emergency response P&P**	**Required**	X	Establish (and implement as needed) 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 protected health information.
23	164.308(a)(7)(ii)(A)	Data Backup Plan	Data backup planning & procedures	**Required**	X	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
24	164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Data recovery planning & procedures	**Required**	X	Establish (and implement as needed) procedures to restore loss of data.
25	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Business continuity procedures	**Required**	X	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operation in emergency mode.
26	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Contingency planning periodic testing procedures	Addressable	X	Implement procedures for periodic testing and revision of contingency plans.
27	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Prioritize data and system criticality for contingency planning	Addressable	X	Assess the relative criticality of specific applications and data in support of other contingency plan components.

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
ADMINISTRATIVE SAFEGUARDS						
28	**164.308(a)(8)**	**Evaluation**	**Periodic security evaluation**	**Required**	X	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart.
29	**164.308(b)(1)**	**Business Associate Contracts and Other Arrangements**	**EP implement BACs to ensure safeguards**	**Required**	**X**	A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. (3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).
30	164.308(b)(4)	Written Contract	Implement compliant BACs	Required	X	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
PHYSICAL SAFEGUARDS						
31	**164.310(a)(1)**	**Facility Access Controls**	**P&P to limit access to systems and facilities**	**Required**	X	Implement 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.
32	164.310(a)(2)(i)	Contingency Operations	Procedures to support emergency operations and recovery	Addressable	X	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.
33	164.310(a)(2)(ii)	Facility Security Plan	P&P to safeguard equipment and facilities	Addressable	X	Implement policies and procedures to safeguard the facility and the equipment there in from unauthorized physical access, tampering, and theft.
34	164.310(a)(2)(iii)	Access Control Validation Procedures	Facility access procedures for personnel	Addressable	X	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.
35	164.310(a)(2)(iv)	Maintenance Records	P&P to document security-related repairs and modifications	Addressable	X	Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
36	**164.310(b)**	**Workstation Use**	**P&P to specify workstation environment & use**	**Required**	X	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 that can access electronic protected health information.
37	**164.310(c)**	**Workstation Security**	**Physical safeguards for workstation access**	**Required**	X	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
38	**164.310(d)(1)**	**Device and Media Controls**	**P&P to govern receipt and removal of hardware and media**	**Required**	X	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
39	164.310(d)(2)(i)	Disposal	P&P to manage media and equipment disposal	Required	X	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
40	164.310(d)(2)(ii)	Media Re-use	P&P to remove PHI from media and equipment	Required	X	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
41	164.310(d)(2)(iii)	Accountability	Document hardware and media movement	Addressable	X	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
42	164.310(d)(2)(iv)	Data Backup and Storage	Backup PHI before moving equipment	Addressable	X	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
TECHNICAL SAFEGUARDS						
43	**164.312(a)(1)**	**Access Control**	**Technical (administrative) P&P to manage PHI access**	**Required**	X	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
44	164.312(a)(2)(i)	Unique User Identification	Assign unique IDs to support tracking	**Required**	X	Assign a unique name and/or number for identifying and tracking user identity.
45	164.312(a)(2)(ii)	Emergency Access Procedure	Procedures to support emergency access	**Required**	X	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
46	164.312(a)(2)(iii)	Automatic Logoff	Session termination mechanisms	Addressable	X	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
47	164.312(a)(2)(iv)	Encryption and Decryption	Mechanism for encryption of stored PHI	Addressable	X	Implement a mechanism to encrypt and decrypt electronic protected health information.
48	**164.312(b)**	**Audit Controls**	**Procedures and mechanisms for monitoring system activity**	**Required**	**X**	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
49	**164.312(c)(1)**	**Integrity**	**P&P to safeguard PHI unauthorized alteration**	**Required**	**X**	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
50	164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Mechanisms to corroborate PHI not altered	Addressable	X	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
51	**164.312(d)**	**Person or Entity Authentication**	**Procedures to verify identities**	**Required**	**X**	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
52	**164.312(e)(1)**	**Transmission Security**	**Measures to guard against unauthorized access to transmitted PHI**	**Required**	**X**	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
53	164.312(e)(2)(i)	Integrity Controls	Measures to ensure integrity of PHI on transmission	Addressable	X	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
54	164.312(e)(2)(ii)	Encryption	Mechanism for encryption of transmitted PHI	Addressable	X	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

HIPAA Security Requirements

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Requirement Summary	Implementation Required or Addressable	Check if Pertinent to Organization	Requirement
ORGANIZATIONAL REQUIREMENTS						
55	**164.314(a)(1)**	**Business Associate Contracts or Other Arrangements**	**EP must ensure BA safeguards PHI**	**Required**	X	(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful. (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
56	164.314(a)(2)	Business Associate Contracts	BACs must contain security language	**Required**	X	(i) Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will-- (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.
57	**164.314(b)(1)**	**Requirements for Group Health Plans**			X	Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii). or as authorized under §164.508. a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
58	164.314(b)(2)(i)	Implement Safeguards		**Required**	N/A	Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan
59	164.314(b)(2)(ii)	Ensure Adequate Separation		**Required**	N/A	Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures
60	164.314(b)(2)(iii)	Ensure Agents Safeguard		**Required**	N/A	Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information
61	164.314(b)(2)(iv)	Report Security Incidents		**Required**	N/A	Report to the group health plan any security incident of which it becomes aware.
62	**164.316(a)**	**Policies and Procedures**	**P&P to ensure safeguards to PHI**	**Required**	X	A covered entity must, in accordance with § 164.306: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
63	164.316(b)(1)	Documentation	Document P&P and actions & activities	**Required**	X	Documentation. (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
64	164.316(b)(2)(i)	Time Limit	Retain documentation for 6 years	**Required**	X	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
65	164.316(b)(2)(ii)	Availability	Documentation available to system administrators	**Required**	X	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
66	164.316(b)(2)(iii)	Updates	Periodic review and updates to changing needs	**Required**	X	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.