HIPAA and The Security Rule

Angie Cameron
Johnston Barton Proctor & Rose LLP
acc2@johnstonbarton.com

The Security Rule

- Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Part 160 and Part 164, Subparts A and C
  - Adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Compliance deadline was 2005, but there has been increased scrutiny over the past few years.

Overview of the Security Rule

- Administrative Simplification
  - Portion of HIPAA intended to protect the privacy and security of certain health information and promote efficiency in the health care industry.
  - Includes the following provisions of HIPAA
    - Privacy Rule
    - Electronic Transactions and Code Sets Rule
    - National identifier requirements (NPI)
    - Security Rule

Who must comply?

- Covered Entities
  - Covered Health Care Providers - any provider who transmits ***any health information in electronic form***.
  - Health Plans
  - Health Care Clearinghouses
  - Medicare Prescription Drug Card Sponsors

Definitions

- Important definitions to understand from HIPAA and the Security Rule
  - Covered Entity
  - Protected Health Information (“PHI”) -
  - Electronic Protected Health Information (“ePHI”) -

The Security Rule

- Applies to ePHI.
- Prior to HIPAA, no generally accepted set of security standards or general requirements.
- Use of computers to pay claims, answer eligibility questions, provide health information and other administrative and clinically based functions.
- Makes the medical workplace more mobile and efficient, but…
- Increases potential for security risks.

The Security Rule

- Three goals
  - Confidentiality - ePHI accessible only to authorized people and processes.
  - Integrity - ePHI is not altered or destroyed in an unauthorized manner.
  - Availability - ePHI can be accessed as needed by an authorized person.

Privacy Rule v. Security Rule

- Privacy Rule - sets standards for who may have access to PHI.
- Security Rule - sets standards for ensuring that only those who should have access to ePHI will actually have access.
- The Security Rule requirements should closely reflect those requirements found in the Privacy Rule.

Privacy Rule v. Security Rule

- Electronic v. oral/paper
  - Privacy applies to all types of PHI, including electronic.
  - Security applies only to PHI created, received, maintained or transmitted in electronic form. It does not apply to PHI transmitted or stored on paper or provided orally.
  - Examples: PHI transmitted over the internet, stored on a computer, a CD, or magnetic tape.

Privacy Rule v. Security Rule

- "Safeguard" requirement
  - 45 CFR 164.530(c) requires covered entities to adopt certain safeguards for PHI.
    - Administrative
    - Physical
    - Technical
  - Actions taken to comply with this safeguard requirement may address some of the Security requirements

Privacy Rule v. Security Rule

- Security Rule is more comprehensive than the Privacy Rule.
- Any state law contrary to the Privacy or Security Rule is preempted - the federal law prevails.

Implementation Specifications

- A detailed instruction for implementing a particular standard in the Privacy/Security Rules.
- The specification may be either "required" or "addressable."
- Required - CE must implement policies and procedures that meet the specification.
- Addressable - CE MUST assess whether reasonable and appropriate in the entity's environment to meet the specification.

Implementation Specifications

- Addressable
  - Analyze the likelihood of protecting the entity's ePHI from reasonably anticipated threats and hazards.
  - Implement if reasonable and appropriate - If not reasonable and appropriate:
    - Document rationale supporting the decision, and
    - Implement equivalent, alternate measure, OR
    - Not implement the specification, MUST document the reason.
    - CFR 164.306(d)(ii)(B)(2).

Implementation Specifications

- Addressable
  - In analyzing whether reasonable and appropriate, you may
    - Risk - what circumstances leave the entity open to unauthorized access and disclosure of ePHI?
      - Use of PDAs or computers
    - Security - what security measures are already in place or could reasonably be put into place?
      - Password protected
    - Financial - How much will implementation cost?
      - COST cannot be the only rationale for not implementing.

Approach to implementation

- CMS suggests a process by which to approach compliance with the Security Rule
  - Assess current security, risks and gaps
  - Develop an implementation plan
    - Read the Security Rule;
    - Review the addressable implementation specifications;
    - Determine security measures.
  - Implement solutions
  - Document decisions/choices
  - Reassess periodically

Implementation specifications

- CMS highlights that security is not a one-time project but rather an ongoing process that should be reviewed as the CE and technologies change.
- CMS does not recommend any specific technology.
- CMS recognizes that “there is no totally secure system”

Implementation Specifications

- In deciding which security measures to use, a covered entity should take into account its
  - Size
  - Capabilities
  - Costs and
  - Operational impact.
- Balance the risks of inappropriate use or disclosure of ePHI against the impact of various protective measures.

Security Standards

- The security standards are divided into three categories
  - Administrative - administrative functions that assist in meeting security standards, including assignment and delegation of security responsibility and training.
  - Physical - mechanisms required to protect electronic systems, equipment and data from threats, environmental hazards and unauthorized intrusion.
  - Technical - Automated processes used to protect data and control access to data, including authentication to access data, and encryption and decryption.

45 CFR 164.304

Administrative Safeguards

- 45 CFR 164.308
- Defined as “administrative actions and polices and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

Administrative Safeguards

- These standards comprise over half of the security requirements in the Security Rule.
- Begin with an evaluation of the security controls already in place and a risk analysis.

Administrative Safeguards

- Security Management Process - implement policies and procedures to prevent, detect, contain and correct security violations.
- Four implementation specifications
  - Risk analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review
- All four specifications are REQUIRED

Administrative Safeguards

- Security Management Process
  - Risk Analysis and Risk Management serve as tools to assist in the development of a CE's strategy to protect the confidentiality, integrity and availability of ePHI.

Security Management Process

- Risk Analysis - 164.308(a)(1)(ii)(A)
  - "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 covered entities."
  - Process of identifying potential security risks, and
  - Determining the probability of occurrence and magnitude of risks.

Security Management Process - Risk Analysis

- How does ePHI flow throughout the entity?
  - Do you email medical records to any other providers or contractors?
  - Do you email to corporate officers or consultants?
- Do you use portable devices?
  - iPads, Blackberry, iPhones.
  - If so, do employees have the ability to access ePHI from these devices?
- What external sources of ePHI?
  - Vendors, consultants create, receive, maintain or transmit?
- What human, natural or environmental threats exist to ePHI?

Security Management Process - Risk Management

- Risk management
  - 164.308(a)(1)(ii)(B)
  - "Implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a)."
  - Requires the CE to make decisions about how to address security risks and vulnerabilities.

Security Management Process - Risk Management

- What security measures are already in place to protect ePHI?
  - Passwords, automatic logoff, locked doors that contain ePHI, etc.
- Is leadership or management involved in risk management and mitigation decisions?
  - Reporting up the chain of command?
- Are security processes being communicated throughout the organization?
  - Training on policies and procedures?
- Does the CE need to engage other resources to assist in risk management?
  - Consultants, lawyers, risk management through insurance company

Security Management Process - Sanction Policy

- 164.208(a)(1)(ii)(C)
- "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."
- Workforce member is a defined term in HIPAA - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the CE, is under the direct control of such entity or business associate whether or not they are paid by the CE.

Security Management Process - Sanction Policy

- Does the CE have existing sanction policies and procedures that meet this specification? If not, can existing sanction policies be modified to include language relating to violations of these policies and procedures?
  - Do you have a policy that says “if you violate a rule or policy of the facility, you may be sanctioned up to and including termination”? (likely not sufficient but it’s a start)

Security Management Process - Sanction Policy

- Does the facility require employees to sign a statement of adherence to security policies and procedures as a prerequisite to employment?
  - Employee handbook?
  - Confidentiality statement?
- Does the statement of adherence state that workforce members acknowledge that violations of security policies and procedures may lead to disciplinary action - up to and including termination?

Security Management Process - Sanction Policy

- Does the sanction policy provide examples of potential violations?
- Does the sanction policy adjust the disciplinary action based on the severity of the violation?
  - More egregious the violation(s), the more severe the penalty.

Security Management Process

- Information System Activity Review 164.308(a)(1)(ii)(D)
- "Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."
- This should be used to determine if any ePHI is or has been used in an inappropriate manner.

Security Management Process

- Information System Review
  - What are the audit and activity review functions of the current information systems?
    - Is this done? Monitoring who is accessing what information?
  - Are the information systems adequately used and monitored to promote continual awareness of activity?
  - What logs or reports are generated by the systems?

Administrative Safeguards

- Assigned Security Responsibility
  - "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."
  - Unlike the implementation specifications in the Security Management Standard (the four outlined previously), this standard does not have a specific implementation specification.

Assigned Security Responsibility

- Assigned Security Responsibility
  - The purpose is fairly straightforward - identify the person who is operationally responsible for assuring that the facility complies with the Security Rule.
  - CE should be aware when assigning responsibility:
    - Comparable to Privacy Official
    - The Security Official and Privacy can be the same person but does not have to be.
    - Although one person should have overall responsibility, others may be assigned specific tasks.

Assigned Security Responsibility

- Would it serve the facility's needs to designate the same individual as Privacy and Security Official?
- Has the organization agreed upon, and clearly identified and documented, the responsibilities of the Security Official?
- How are the roles and responsibilities of the Security Official crafted to reflect size, complexity and technical capabilities of the facility?

Administrative Safeguards

- Workforce Security 164.308(a)(3)
  - "Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard], and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information."

Workforce Security

- Workforce members who need access to ePHI to carry out their duties must be identified.
- This can be done by job function, i.e. job description.
- For each job function, identify
  - Identify the ePHI needed;
  - When it is needed; and
  - Make reasonable efforts to control access to the ePHI.

Workforce Security

- Identify the computer systems and applications that provide access to ePHI.
- Minimum necessary rule applies in the Security Rule as well - When using or disclosing ePHI or when requesting PHI from another CE or business associate, a CE must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Workforce Security

- Implementation Specifications - all are addressable.
  - Authorization and/or Supervision
  - Workforce Clearance Procedure
  - Termination Procedure

Workforce Security - Implementation Specifications

- Authorization and/or Supervision 164.308(a)(3)(ii)(A)
- Where reasonable and appropriate:
  - "Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in location where it might be accessed."

Workforce Security - Implementation Specifications

- Determine whether a particular user or computer system has a right to carry out certain activities, like reading medical records.
- The goal should be to provide appropriate checks and balances to ensure that all members of the workforce have the appropriate access or some cases no access to ePHI.
- For instance, remember that volunteers are members of the workforce. What access should they have to ePHI?

Workforce Security - Implementation Specifications

- Are detailed job descriptions used to determine what level of access the person holding the position should have to ePHI?
- Who has the authority to determine who can have access to ePHI?
- Are there similar or existing procedures for paper records or files that can be used as guidance?

Workforce Security - Implementation Specifications

- Workforce Clearance Procedure 164.308(a)(3)(ii)(B)
  - "Implement procedures to determine that the access of the workforce member to ePHI is appropriate."
  - Are there existing procedures for determining that the appropriate workforce members have access to necessary information?
  - Are the procedures used consistently within the facility when determining access of related workforce job functions?

Workforce Security - Implementation Specifications

- Termination Procedures 164.308(a)(3)(ii)(C)
  - "Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made [in the Workforce Clearance Procedure]…"
  - Terminations procedures must be implemented to remove access privileges when an employee, contractor or other individual previously entitled to access no longer has these privileges - for instance when an employee leaves voluntarily or involuntarily.

Workforce Security - Implementation Specifications

- Termination Procedure
  - There should also be a process by which to change access when an employee leaves one position that has a different level of access.
  - Do the termination policies and procedures assign responsibility for removing information system and/or physical access?
  - Do the policies and procedures include timely communication of termination actions to insure that the termination procedures are followed?

Administrative Safeguards

- Information Access Management Standard 164.308(a)(4)
  - "Implement policies and procedures for authorizing access to ePHI that are consistent with the [Privacy Rule]."
  - The fourth standard under the Administrative Safeguards is a key to restricting access to persons and entities with a need to access the information.
  - Intent is to minimize the risk of inappropriate disclosure, alteration or destruction of ePHI.

Administrative Safeguards - Information Access

- Three Implementation Specifications
  - Isolating Health Care Clearinghouse Functions (Required)
  - Access Authorization (Addressable)
  - Access Establishment and Modification (Addressable)

Information Access

- Isolating Health Care Clearinghouse Functions
  - A health care clearinghouse is a public or private entity, including a billing service, repricing company, community health management information system or community health information system and value-added networks and switches that does either of the following functions:
    - Processes or facilitates the processing of health information received from another entity in a non standard format containing nonstandard data into standard data elements or a standard transaction.

Information Access

- Isolating Health Care Clearinghouse Functions
  - Receives a standard transaction from another entity and processes or facilitates the processing of health information into non-standard format or nonstandard data content for a receiving entity.

Information Access

- Access Authorization (Required)
  - “Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.”
  - Authorization is defined as the act of determining whether a particular user or computer system has the right, based on job function or responsibilities to carry out a certain activity.

Information Access - Access Authorization

- How is authorization documented?
- Are the policies and procedures for granting access consistent with the Privacy Rule?
- Have appropriate authorization and clearance procedures, as specified under workforce security, been performed prior to granting access?
- Do different workforce members require different levels of access based on job function?
- Is there a technical process in place, such as creating a unique user name and authentication process, when granting access to a workforce member?

Information Access

- Access Establishment and Modification
  - After determining who should have access, then determine how access should access be established and modified.
  - "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."

Access Establishment and Modification

- Implement and manage access privileges to workstations, transactions, programs and processes.
- This may be assigned to a specific person or more than one person.
- Termination of access privileges is also part of this process, who can be the same as the person who implements access.

Access Establishment and Modification

- Are policies and procedures in place for establishing access and modifying access?
- Are system access policies and procedures documented and updated as necessary?
- Do members of management or other workforce members periodically review the list of persons with access to ePHI to ensure they are valid and consistent with those authorized?

Administrative Safeguards

- Security Awareness and Training standard
  - The fifth standard for Administrative Safeguards - "Implement a security awareness and training program for all members of its workforce (including management."
  - Training for all new and existing members of the workforce - don't forget volunteers.
  - Periodic training with changes in environment or operational changes that may affect ePHI.

Security Awareness and Training

- Four implementation specifications:
  - Security Reminders (Addressable)
  - Protection from Malicious Software (Addressable)
  - Log-in Monitoring (Addressable)
  - Password Management (Addressable)

Security Awareness and Training

- Security Reminders
  - Notices in printed or electronic form
  - Discussion at monthly meetings
  - Reminders posted in specific areas
  - Formal retraining on security policies and procedures.
- Could be incorporated into current training or ways to remind staff of policies and procedures.

Security Awareness and Training

- Protection from Malicious Software
  - The facility should have procedures for guarding against, detecting and reporting malicious software.
  - Any program that harms information systems such as viruses, Trojan horses or worms.
  - Email attachments and programs downloaded from the internet often the culprit.
  - Consider policies regarding staff's access to internet on facility computers and use of company email for personal use.

Security Awareness and Training

- Log-in Monitoring
  - Address how users log onto systems and how they manage passwords.
  - Many systems can be set to identify when multiple unsuccessful attempts have been made to log-in. Other systems may record attempts in a log or audit trail.
  - May need to contact system vendor to determine what capabilities their systems may have in monitoring.

Security Awareness and Training

- Password Management
  - "Procedures for creating, changing, and safeguarding passwords."
  - Train your staff on the use of passwords and establish guidelines for creating passwords and changing them during periodic change cycles.
  - Are there policies in place that prevent workforce members form sharing passwords?
  - Is the workforce advised to commit their passwords to memory?
  - Are common sense precautions taken, such as not writing down passwords and leaving them in visible areas?

Administrative Safeguards

- Security Incident Procedures Standard
  - "Implement policies and procedures to address security incidents."
  - Purpose of this standard is to require covered entities to address security incidents within their environment.
  - Meant to reduce the type and amount of security incidents.

Security Incident Procedures

- Security incident is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system."
- Implementation Specification - Response and Reporting
  - 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 incidents and their outcomes.

Security Incident Procedures

- Security incident procedures must describe how workforce members are to respond to an incident, which may include:
  - Preserving evidence
  - Mitigating the situation that caused the incident
  - Documenting the incident and outcome, and
  - Evaluating security incidents as part of ongoing risk management.

Security Incident Procedures

- Possible incidents:
  - Stolen or otherwise inappropriately obtained passwords that are used to access ePHI.
  - Corrupted backup tapes that do not allow restoration of ePHI.
  - Virus attacks that interfere with the operations of information systems with ePHI.
  - Physical break-ins leading to the theft of media with ePHI.
  - Failure to terminate the account of the former employee that then is used by an unauthorized user to access information systems with ePHI.
  - Providing media with ePHI to another user not authorized to access it.

Security Incident Procedures

- Are policies and procedures developed and implemented to address security incidents?
- Do the security incident policies and procedures list possible types of security incidents and response to each?
- Do the security policies and procedures identify to whom incidents must be reported?

Administrative Safeguards

- Contingency Plan Standard
  - “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 ePHI.”
  - Purpose is to establish strategies for recovering access to ePHI if the facility experiences an emergency or other occurrence.
  - Goal is to have access to ePHI when needed.

Contingency Plan

- Five implementation specifications
  - Data Backup Plan (Required)
  - Disaster Recovery Plan (Required)
  - Emergency Mode Operation Plan (Required)
  - Testing and Revision Procedures (Addressable)
  - Applications and Data Criticality Analysis (Addressable)

Contingency Plan

- Data Backup Plan
  - "Establish and implement procedures to create and maintain retrievable exact copies of ePHI."
  - May already exist as current business practice
  - Ask:
    - What ePHI must be backed up?
    - Does the plan include all important sources of data such as patient accounting systems, electronic medical records, electronic test results, digital recordings of diagnostic images, etc.?

Contingency Plan

- Data Backup
  - Ask:
    - Has the facility considered the various methods of backups - tape, disk or CD?
    - Does the backup plan include storage of backups in a safe and secure place?
    - Is the organization's frequency of backups appropriate for its environment?

Contingency Plan

- Disaster Recovery Plan (Required)
  - "Establish (and implement as needed) procedures to restore any loss of data."
  - General disaster plan may meet this requirement.
  - Be sure to make sure the general plan covers recovery of ePHI.

Contingency Plan - Disaster Recovery

- For consideration:
  - Does the disaster recovery plan address issues specific to the covered entity's operating environment?
  - Does the plan address what data is be restored?
  - Is a copy of the disaster recovery plan readily accessible at more than one location?

Contingency Plan

- Emergency Mode Operation Plan - Required
  - "Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode."
  - When operating in emergency mode, facilities should have security policies to protect ePHI.

Emergency Mode Operation

- Things to consider:
  - Does the organization's plan balance the need to protect the data with the organization's need to access the data?
  - Will alternative security measures be used to protect the ePHI?
  - Does the emergency mode operation plan include possible manual procedures for security protection?
  - Does the emergency plan include telephone numbers and contact names for all persons that must be notified in the event of a disaster, as well as the roles and responsibilities of those people involved in the restoration process?

Contingency Plan

- Testing and Revision Procedures - Addressable
  - "Implement procedures for periodic testing and revision of emergency plans."
  - Applies to the other specifications under the Contingency Plan.
  - Scenario based walk thrus or complete live tests are examples.
  - Testing and revision will vary in frequency and comprehensiveness.

Testing and Revision

- Things to consider:
  - Are the processes for restoring data documented?
  - Do those responsible for performing contingency tasks understand their responsibilities?
  - Have those responsible actually performed a test of the procedure?
  - Have the results of each test been documented and any problems with the test reviewed and corrected?

Contingency Plan

- Application and Data Criticality (Addressable)
  - The last implementation specification under the Contingency Plan standard states
    - "Assess the relative criticality of specific applications and data in support of other contingency plan components."
  - Prioritize systems for data backup, disaster recovery and emergency operations plans.

Administrative Safeguards

- Evaluation standard
  - "Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental and operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule]."

Evaluation

- Purpose is to establish a process for CE's to review and maintain reasonable and appropriate security measures.
- On-going evaluations should be conducted on a scheduled basis - such as annually or every two years.

Evaluation

- Things to consider:
  - How often should an evaluation be done? For example, are additional evaluations performed if security incidents are identified, changes are made in the organization, or new technology is implemented?
  - Is an internal or external evaluation, or a combination of both, most appropriate for the CE?
  - Are periodic evaluation reports and the supporting material considered in the analysis, recommendations, and subsequent changes fully documented?

Administrative Safeguards

- Business Associate Contracts and Other Arrangements standard
  - "A covered entity 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 that the business associate will appropriately safeguard the information."

Business Associates

- Business associate is defined by HIPAA as a person who:
  - On behalf of a covered entity, creates, receives, maintains, or transmits protected health information, or
  - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, involving the disclosure of PHI.

Business Associates

- Similar to the Business Associate standards contained in the Privacy Rule, but is specific to business associates who create, receive, maintain or transmit ePHI.
- Satisfactory assurances from the BA that it will appropriately safeguard ePHI.

Business Associates

- Standard does not apply to the transmission by a CE of ePHI to a health care provider concerning the treatment of an individual.
- A CE who provides satisfactory assurances as a BA of another CE will be in noncompliance with the Security Rules.

Business Associates

- One Implementation Specification: Written Contract or other Arrangement
  - "Document the satisfactory assurances required by paragraph (b)(1) through a written contract or other arrangement with the business associate that meets the requirements of [the Organizational Requirements]."

Business Associates

- Things to consider:
  - Have all Bas been identified?
  - Have existing BA contracts created and implemented for compliance with the Privacy Rule, which involve ePHI, been reviewed to determine if Security Rule requirements are addressed?
  - To minimize additional work efforts, can existing BA contracts, which involve ePHI, be modified to include Security Rule requirements?

- Matrix attached as Exhibit.

Other Safeguards

- Physical
- Technical

QUESTIONS?

THANK YOU

ANGIE CAMERON
acc2@johnstonbarton.com