HIPAA'S SECURITY RULE: THE BEGINNER'S GUIDE

Before [HIPAA](), there were no general requirements or security standards for protecting patient health information in the healthcare industry. Without regulations set in place, healthcare providers could

not confidently state that their patients' sensitive data was properly protected. Once the Health Insurance Portability and Accountability Act was passed by the federal government, businesses now had explicit standards and mandates to follow to ensure that medical histories and patient information were properly stored, transferred, and transmitted.

As technology continues to expand and evolve, however, a majority of organizations in the industry have moved away from the manual paper documentation of patient encounters, and have migrated all of their Protected Health Information (PHI) to the cloud. While the transition to digital systems has greatly increased efficiencies, improved workflows, and reduced costs, the need for higher security standards has never been greater. This is where the Security Rule comes into play.

The Security Rule is one of the biggest regulations under HIPAA, and it carries the most significance for those in the software and IT fields. Essentially, the Security Rule aims to protect the privacy of patients' digital health information while at the same time allowing companies the flexibility to adopt new technologies that may improve the efficiency and quality of patient care. While the Security Rule is extremely beneficial for organizations, it is also very long and in-depth, giving even the most proficient worker a run for their money.

The following is a summary of the HIPAA Security Rule and its purpose is to help inform your employees of the content of this regulation while guiding your company to compliance. This in no way is a comprehensive reference to the guidelines, and should only be used as a bridge between the entire legal document and your organization.

Who Does the Security Rule Apply To?

The HIPAA Security Rule applies to covered entities and their business associates (BA). Covered entities include health plans, healthcare clearinghouses, and any healthcare provider that has access to PHI and confidential patient data.

- Healthcare providers include doctors, clinics, dentists, chiropractors, psychologists, nursing homes, and pharmacies, to name a few
- Health plans can include HMOs, health insurance companies, company health plans, military or veteran healthcare programs, and government programs like Medicare and Medicaid
- Healthcare clearinghouses include any organizations that process PHI, such as community health management systems, billing services, or repricing companies

What Information is Protected?

While HIPAA in its entirety protects anything that is considered protected health information, the Security Rule in itself only applies to individually identifiable health information that is received, transmitted, or stored in electronic form (known as ePHI). The Security Rule does not apply to PHI transmitted orally or in writing.

Some information that may be considered ePHI includes:

- Past or present physical or mental health condition
- Type of healthcare provided to the patient
- Past or present payment or billing history for the healthcare provided
- Any personal information that may identify the patient, such as name, address, birthdate, and Social Security Number

Safeguards

In order to ensure the confidentiality and security of ePHI, the Security Rule has safeguards set in place for covered entities, including Administrative Safeguards, Physical Safeguards, and Technical Safeguards. All three safeguards include specific implementation guidelines, with some being "required" and others being "addressable". While addressable implementation specifications are not mandatory, it is usually considered best practice to follow them.

Administrative Safeguards

The Administrative Safeguards are a collection of procedures, policies, and actions that manage the conduct of the covered entity's workforce and their role in maintaining the security of ePHI. The Administrative Safeguards comprise over half of the regulations under the Security Rule, and are vital when trying to implement a HIPAA compliance program.

There are 9 standards under the Administrative Safeguards section:

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Underneath those 9 standards, there are 18 total actions you must implement to achieve compliance:

1. Security Management Process
    a. Risk Analysis (required): Perform and document a risk analysis to see where ePHI is being used and stored in order to determine all the ways that HIPAA could be violated
    b. Risk Management (required): Implement measures to reduce these risks
    c. Sanction Policy (required): Implement sanction policies for any employees who fail to comply
    d. Information Systems Activity Reviews (required): Regularly review system activity, logs, audit trails, etc. for compliance
2. Assigned Security Responsibility
    a. Officers (required): Designate HIPAA Security and Privacy Officers
3. Workforce Security
    a. Employee Oversight (addressable): Implement procedures to authorize and supervise employees who work with ePHI, and to grant and remove ePHI access to employees. Ensure that an employee's access to ePHI ends when they leave the organization
4. Information Access Management
    a. Multiple Organizations (required): Ensure that ePHI is not accessed by parent or partner organizations or subcontractors that are not authorized
    b. ePHI Access (addressable): Implement procedures for granting access to ePHI
5. Security Awareness and Training

    a. Security Reminders (addressable): Periodically send updates and reminders about security and privacy policies to employees
    b. Protection Against Malware (addressable): Have procedures for guarding against, detecting, and reporting malicious software
    c. Login Monitoring (addressable): Implement a system to monitor logins and report discrepancies
    d. Password Management (addressable): Ensure that there are procedures for creating, changing, and protecting passwords
6. Security Incident Procedures
    a. Response and Reporting (required): Identify, document, and respond to security incidents
7. Contingency Plan
    a. Contingency Plans (required): Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data
    b. Contingency Plans Updates and Analysis (addressable): Periodically test and revise contingency plans
    c. Emergency Mode (required): Establish procedures for protection of the security of ePHI while operating in emergency mode
8. Evaluations (required)
    a. Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures
9. Business Associate Agreements (required)
    a. Have special contracts with business partners who will have access to your ePHI in order to ensure that they will be compliant and have proper security set in place

Physical Safeguards

Physical Safeguards are a set of rules and guidelines that focus on the physical access to ePHI. Physical access can include anywhere outside of the office walls that employees may look at ePHI, such as on their personal computers or in their homes.

There are 4 standards under the Physical Safeguards section:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Underneath those 4 standards, there are 10 total actions you must implement to achieve compliance:

1. Facility Access Controls
    a. Contingency Operations (addressable): Establish procedures that allow facility access in the event of an emergency
    b. Facility Security Plan (addressable): Implement procedures to safeguard the facility and equipment from unauthorized physical access, tampering, or theft
    c. Access Control and Validation Procedures (addressable): Implement procedures to control and validate a person's access to facilities based on their role or function
    d. Maintenance Records (addressable): Implement policies to document repairs and modifications to the physical components of a facility which are related to security (e.g.

hardware, walls, doors, and locks)
2. Workstation Use (required)
    a. Implement procedures that specify the proper workstation that can access ePHI
3. Workstation Security (required)
    a. Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users
4. Device and Media Controls
    a. 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
    b. Media Re-Use (required): Implement procedures for removal of ePHI from electronic media before they are available for re-use
    c. Accountability (addressable): Maintain a record of the movements of hardware and electronic media and any person responsible of them
    d. Data Backup and Storage (addressable): Create a retrievable, exact copy of ePHI before moving any equipment

Technical Safeguards

The Technical Safeguards focus on the technology that protects ePHI and controls access to it. While the Security Rule does not require you to use specific technologies, it still outlines that the technology you do decide to use needs to follow all guidelines for compliance.

There are 5 standards listed under the Technical Safeguards section.

- Access Control
- Audit Controls
- Integrity
- Authentication
- Transmission Security

Underneath those 5 standards, there are 9 total actions you must implement to achieve compliance:

1. Access Control
    a. Unique User Identification (required): Assign a unique name and/or number for identifying and tracking user identity
    b. Emergency Access Procedure (required): Establish procedures for obtaining necessary ePHI during an emergency
    c. Automatic Logoff (addressable): Implement electronic procedures that end a session after a predetermined time of inactivity
    d. Encryption and Decryption (addressable): Implement software to encrypt and decrypt ePHI
2. Audit Controls (required)
    a. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
3. Integrity
    a. Mechanism to Authenticate ePHI (addressable): Implement electronic systems that confirm ePHI has not been altered or destroyed in an unauthorized manner
4. Authentication (required)
    a. Implement procedures to verify that a person or entity seeking access to ePHI is the one

claimed

5. Transmission Security
    a. Integrity Controls (addressable): Implement security measures to ensure that electronically transmitted ePHI is not modified without detection until disposed of
    b. Encryption (addressable): Implement systems to encrypt ePHI whenever deemed appropriate

Conclusion

While the Security Rule may seem extremely intensive (it is), we hope that this guide has helped to summarize all that it entails while further educating you on its content and how to reach compliance. For anyone in the software or IT fields, ensuring all regulations under the HIPAA Security Rule are being followed and implemented is no easy matter, but it is vital nonetheless.

Resources from BMC

For more information about achieving HIPAA compliance, check out BMC's guide an Introduction to HIPAA Compliance: Everything you need to know about HIPAA Compliance.