CCS CHOICE CYBERSECURITY

Healthcare Industry

Security & Compliance Resource Guide

Table of Contents

HIPAA/HITECH COMPLIANCE OVERVIEW

What is HIPAA?

A provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that sets standards for the privacy of health information that can identify an individual.

What is HITECH?

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) legislation was created in 2009 to stimulate the adoption of electronic health records (EHR) and supporting technology in the United States. It was also fundamental in driving the adoption of Meaningful Use.

Who oversees it?

The U.S. Department of Health and Human Services and the Office for Civil Rights.

Who does it apply to?

Healthcare Providers, Health Plans, Health Clearinghouses, and Business Associates.

Healthcare Providers	Health Plans	Health Clearinghouses	Business Associates
▪ Doctors ▪ Clinics ▪ Psychologists ▪ Dentists ▪ Chiropractors ▪ Nursing Homes ▪ Pharmacies ▪ Hospitals ▪ Surgeons ▪ Specialists ▪ Hospice Care	▪ Health Insurance Companies ▪ HMOs ▪ Company Health Plans ▪ Medicare ▪ Medicaid ▪ VA Healthcare Programs ▪ Flexible Spending Accounts	▪ Entities that process health information. ▪ Billing Services ▪ Community Health Management Information Systems	▪ Hosting Companies ▪ Managed Service Providers (MSPs) ▪ Software as a Service Providers ▪ CPA Firms and Accounting Services ▪ Claims Processing ▪ Medical Transcription Services ▪ Document Destruction Services ▪ Records Management ▪ Legal Services ▪ Consulting Services

How does it impact IT professionals?

Many Information Technology (IT) companies fall under the umbrella of the definition of a business associate. For the purposes of HIPAA, a business associate is any person or organization that is not a member of a covered entity's workforce that performs functions or activities on behalf of a covered entity ***who has access to or discloses*** Protected Health Information (PHI).

This means that if you provide remote administration or off-site backup of client equipment housing PHI data, your company needs to be covered by a business associate contract.

However, if you do not have access to the systems and services that house PHI, you are not required to be covered by a business associate contract. If you have any questions about whether or not you need to be covered by a business associate contract, you should consult your legal counsel.

What is Protected Health Information (PHI)?

Protected Health Information is a classification of data that includes all individually identifiable health information that is held or transmitted by a covered entity (doctor's office, health plan, billing office, etc.) or its business associate, in any form or media, whether electronic, paper, or oral.

Individually identifiable health information is any information, including demographic data, which relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

What is Meaningful Use?

Meaningful Use defines the minimum U.S. government standards for using electronic health records to exchange information between healthcare providers, insurers, and patients. It is used to determine if a healthcare provider can receive federal funds from EHR incentive programs.

- Stage 1, which began in 2010, focused on promoting adoption of EHR technology by healthcare providers.
- Stage 2, finalized in 2012, increased the thresholds of compliance criteria and provided for care-coordination requirements and patient engagement rules.
- Stage 3, which will likely be implemented in late 2015-2016, will focus on health information exchange and revised rules from the previous stages.
- The HITECH Act of 2009 provided economic incentives for healthcare professionals to achieve meaningful use. Though meaningful use is voluntary, those who fail to achieve the standard by 2015 will be penalized unless that provision of the act is overridden by Congress.

In order to claim adherence to meaningful use, healthcare providers must provide proof of a risk assessment and core security controls. This is where most MSPs will be an aid to their clients. By helping to establish a documented and deployed Information Security Policy, you can assist your clients in providing meaningful use.

What do your clients need to be HIPAA Compliant?

There are three major types of safeguards that must be adopted by your clients in order to be HIPAA compliant. These three categories are: administrative safeguards, physical safeguards, and technical safeguards.

SUMMARY OF HIPAA SECURITY RULE

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.1 To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish 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). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the healthcare industry. At the same time, new technologies were evolving, and the healthcare industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

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. Given that the healthcare marketplace is diverse, the Security Rule is 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.

This is a summary of key elements of the Security Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Privacy and Security Rules are obligated to comply with all of their applicable requirements and should not rely on this summary as a source of legal information or advice.

Statutory and Regulatory Background

The *Administrative Simplification* provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The Department received approximately 2,350 public comments. The final regulation, the Security Rule, was published February 20, 2003.2 The Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI.

The text of the final regulation can be found at 45 CFR Part 160 and Part 164, Subparts A and C.

What is the HIPAA Final Omnibus Rule?

On January 17th, 2013 HIPAA and HITECH regulations became subject to a 500 page overhaul of the rules and regulations known collectively as the Final Omnibus Rule. This Omnibus Rule went into effect for healthcare providers on March 26, 2013.

The Department of Health and Human Services summarizes the 500 pages of the Omnibus Rule as follows:

"This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the rules, which were issued as a proposed rule on July 14, 2010. These modifications:
    i. Make Business Associates of Covered Entities directly liable for compliance with certain HIPAA Privacy and Security Rules' requirements.
    ii. Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
    iii. Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
    iv. Require modifications to, and redistribution of, a Covered Entity's notice of privacy practices.
    v. Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
    vi. Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.
2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.
3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" threshold with a more objective standard and replaces an interim final rule published on August 24, 2009.
4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009."

Who is Covered by the Security Rule?

Covered Entities: The Security Rule, like all of the Administrative Simplification rules, applies to health plans, health care clearinghouses, and to 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 (the “covered entities”). For help in determining whether you are covered, use CMS's decision tool.

Business Associates

The HITECH Act of 2009 expanded the responsibilities of business associates under the Privacy and Security Rules. HHS is developing regulations to implement and clarify these changes.

General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

The Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner. “Availability” means that e-PHI is accessible and usable on demand by an authorized person.5

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity’s business, as well as the covered entity’s size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.
    - Its size, complexity, and capabilities,
    - Its technical, hardware, and software infrastructure,
    - The costs of security measures

- The likelihood and possible impact of potential risks to e-PHI.

RISK ANALYSIS & MANAGEMENT

The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately to determine which security measures are reasonable and appropriate for a particular covered entity. Risk analysis affects the implementation of all of the safeguards contained in the Security Rule. A risk analysis process includes, but is not limited to, the following activities:

- Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to ePHI and detect security incidents,12 periodically evaluates the effectiveness of security measures put in place,13 and regularly reevaluates potential risks to e-PHI.14
- Evaluate the likelihood and impact of potential risks to e-PHI;8
- Implement appropriate security measures to address the risks identified in the risk analysis;9
- Document the chosen security measures and, where required, the rationale for adopting those measures;10 and
- Maintain continuous, reasonable, and appropriate security protections.11

Administrative Safeguards

Security Management Process: Your client must be able to prove that they have a process in place for managing their security process, which includes identifying and analyzing potential risks to PHI and implementing security measures that limit risks and vulnerabilities to a reasonable level.

Security Personnel: Your client must designate a security official who is responsible for overseeing and maintaining the Security Management Process.

Information Access Management: The PHI rule states that disclosures of PHI be limited to the minimum access necessary to perform business functions. Users should only have access to the information required for their role in the organization.

Workforce Training and Management: Client employees with access to PHI must be trained and educated in security policies and procedures. A document must define appropriate sanctions against employees who violate the established policies and procedures.

Evaluation: Perform a periodic risk assessment that identifies how well the existing security policies and procedures meet the requirements of the HIPAA security rule.

Physical Safeguards

Facility Access and Control: Access to the client facility must be limited to those with authorized access.

Workstation and Device Security: Clients must implement a policy for use and access to workstations and electronic media. This includes a requirement to document a security policy regarding the transfer, removal, disposal, and reuse of electronic media.

Technical Safeguards

Access Control: Ensure that technical safeguards are in place to allow only authorized personnel to access PHI.

Audit Controls: Implement procedural mechanisms to record and examine access and other activity on systems that contain or use PHI.

Integrity Controls: Implement policies and procedures to ensure that PHI is not improperly altered or destroyed. Employ electronic measures to provide monitoring and alerts in the event that PHI is improperly altered or destroyed.

Transmission Controls: Implement technical security measures that guard against authorized access to PHI that is being transmitted over a data network.

Required and Addressable Implementation Specifications

Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and

appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.28

DATA BREACH NOTIFICATIONS

What Constitutes a Data Breach?

For the purposes of HIPAA/HITECH, a breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information. Any impermissible use or disclosure of PHI is considered a breach unless the covered entity or business associate can prove there is a low probability that the PHI has been compromised based on a risk assessment including:

1. The nature and extent of the PHI involved
2. Likelihood of re-identification
3. Who made use of or disclosed the PHI
4. Whether the PHI was actually accessed or viewed
5. The extent to which the risk of PHI has been mitigated

There are three exceptions to the definition of a breach:

1. Unintentional and good faith access or acquisition of PHI during the course of business by an authorized employee
2. Unintentional disclosure of PHI by an authorized person
3. Good faith belief that an unauthorized person to whom PHI was disclosed would be unable to retain the information.

Breach Notification Rules

HIPAA/HITECH includes specific provisions for data breach notification. These requirements are as follows:

Individual Notice: Covered entities must notify affected individuals following discovery of a breach of unsecured PHI. Individual notice must be provided by first-class mail, or email if the individual has accepted such notices electronically. If a covered entity has out-of-date or insufficient contact information for 10 or more individuals, public notice of the breach must be provided on the home page of their website for at least 90 days, or by providing the notice to major print and broadcast media where the individuals likely reside.

Media Notice: In the event that a breach affects more than 500 residents of a State or jurisdiction, in addition to individual notification, the covered entity must issue a

press release announcing the data breach to media outlets serving the affected area.

Notice to the Secretary: In addition to individual and media notification (where applicable) covered entities must notify the Secretary of the Department of Health and Human Services of breaches of unsecured PHI.

Enforcement and Penalties for Noncompliance

The Security Rule establishes a set of national standards for confidentiality, integrity and availability of e-PHI. The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

Learn more about enforcement and penalties in the Privacy Rule Summary and on OCR's Enforcement Rule page.

What are the dangers of not being HIPAA Compliant?

- Up to $50,000 fine per incident
- Up to a 1.5 million dollar civil penalty based on the extent and negligence of the violation
- Criminal penalties of up to $250,000 and imprisonment for up to ten years
- The HITECH Act permits State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules

MERIT-BASED INCENTIVE PAYMENT SYSTEM (MIPS)

What is it?

- MIPS is a Quality Payment Program (QPP) used by The Medicare Access CHIP Reauthorization Act of 2015 (MACRA) after the Medicare Part B Sustainable Growth Rate (SGR) was repealed.
- A patient scoring system for the evaluation of patient care and satisfaction
    - Quality, weighted as 50-60% of your score
    - Advancing Care Information, weighted as 25%
    - Clinical Improvement Activities, weighted as 15%
    - Resource Use, which will grow in weighted value over the years.

Who Does it Apply To?

- Initially it applied to Doctors, Dentists, Physician Assistants, Nurse Practitioners, Clinical Nurse Specialists and Certified Registered Nurse Anesthetists in 2017-2018
- Beginning in 2019, it will also apply to physical and occupational therapists, speech/ language pathologists, audiologists, clinical psychologists and dieticians and nutritionists

Why Care?

- Its mandatory
- If nothing is done, reimbursements will not stay the same, they will decrease
- Deductions are not static, but cumulative. Therefore, the increase and decrease will compound

What are the Goals of MIPS?

- To improve patient care and access to information
- To gather information and use it to prevent things like re-admissions and recurrent conditions

What Actions Can You Take?

- Gather information about patient perceptions of the quality of care
- Evaluate the patient interactions
- Use that information not only in reporting to CMS, but in creating plans for improvement.
- If done properly, in all likelihood, your clients will gain as much reimbursement increase as possible, including bonus points, and even decrease the costs associated with their patients' use of the system.

Medical Industry Security & Compliance Needs Analysis

Needs Analysis Below are 4 areas to discuss with healthcare clients when analyzing specific security needs. Utilize these questions and answers to create the Risk Assessment proposal.

HIPAA/HITECH Compliance

1. Do you have any compliance requirements?
2. Have you ever been audited? Were you ready?
3. Are you familiar with state PII laws?
4. Do you take credit cards? If so, are you PCI compliant?
5. How many credit cards do you process per year?
6. What is the credit card process?
7. Who in the company is responsible for compliance?
8. Have you ever had an audit or fine?
9. Do you know anyone who has had a breach?
10. Do you take medical insurance?
11. Do you accept Medicare or Medicaid? Is it at least 33% of your business?
12. Do you have a best practices or compliance structured framework in place? If so, what controls do you follow?
13. Has your staff had any specific compliance training?
14. How do you handle compliance management?
15. Do you capture and review logs?

General Business

1. Do you store sensitive data?
2. How important is your data?
3. How much is your data worth?
4. Do you know how much sensitive data you store?
5. Who is the asset owner and responsible for your data?
6. How many states do you operate in?
7. How are backups done? Onsite? Offsite?
8. Do you have an incident response plan?
9. Have you ever had a risk assessment?
10. Have you ever had a vulnerability scan or penetration test?
11. Do you have a structured password policy? Where are passwords stored?
12. Do your users have remote access? How do they connect?
13. Do you require any of your clients to have security in place?
14. Do any of your clients require you to have any security or compliances in place?
15. Do you have Cybersecurity Insurance? Ever had a claim?
16. How many servers, workstations and laptops are in place?

17. How do you handle mobile devices?
18. Do you have an employee handbook with security policies?
19. Has your staff had security awareness training?
20. Do you know your potential collateral damage in the event of a breach?

Security

1. Who is responsible for security?
2. Have you ever had a virus or infected system?
3. Have you ever lost any files?
4. Have you ever had a breach?
5. Has a machine ever been lost or stolen?
6. Have you ever had a server crash?
7. What is the longest period of downtime you have experienced?
8. Are you concerned about a breach?
9. Any vendors asking you for security requirements?
10. What would be the impact to your business of a security breach?
11. Do you have email or file encryption?

Workflow

Data in Motion

1. Do you send sensitive data via email?
2. Do you transfer large files?
3. Do you receive sensitive data from outside sources? If so, do you save it locally?
4. Do you send wire transfers?
5. Do you upload and download files from any cloud systems?

Data at Rest

1. Where is sensitive data stored?
2. What is your retention policy for files?
3. What is your retention policy for email?

Vendors

1. How many vendors do you work with? How many cloud vendors?
2. Do you store sensitive data in the cloud?
3. Do any vendors have access to your systems?
4. Do you send sensitive data to your vendors?
5. Do your vendors have any of your sensitive client data?
6. Do your vendors send you sensitive data?
7. Do any of your vendors require you to have any security or compliances in place?

ADDITIONAL HIPAA/HITECH Resources

- Read more about covered entities in the Summary of the HIPAA Privacy Rule
- Additional guidance on Business Associates
- MIPS
    - MIPS Overview
    - Quality Payment Program
    - What You Need To Know About MIPS
- Learn more about enforcement and penalties in the Privacy Rule Summary and on OCR's Enforcement Rule page
- HITECH Act of 2009