HIPAA Overview

HISTORY OF HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was submitted to Congress in 1992 as part of Public Law 104-191. The underlying purpose of HIPAA was to simplify and standardize the administrative process that the healthcare professional must manage through. By standardizing processes, the healthcare delivery system could then become more efficient. Through "Administrative Simplification", Congress called for steps to improve "the efficiency and effectiveness of the healthcare system by encouraging the development of a health information system through the establishment of standards and requirements for certain health information" (Health Insurance and Portability Act). As a result, the regulation's three major purposes were:

1. To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information.

2. To improve the quality of healthcare in the United States by restoring trust in the healthcare system among consumers, healthcare professionals, and organizations dedicated to the delivery of care; and

3. To improve the efficiency and effectiveness of healthcare delivery by creating a framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

HIPAA created three primary areas of regulations to ensure "administrative simplification" and efficient transmission of health information in a manner that protects all **individually identifiable health information**. The areas of regulations, that will be discussed later, are:

1. Transactions and Code Sets **–** The establishment of transmission and transaction standards for the electronic transfer of claims and healthcare information. This required providers to use uniform ("standard") coding to bill for their services.
2. Privacy Standards **–** Standards developed to ensure the protection of **protected healthcare information (PHI).**
3. Security Standards **–** Standards developed to protect **electronic protected health information (ePHI**).

Each of these standards had deadlines ranging from 2000 to 2006 and were to be enforced by the US Department of Health and Human Services (HHS) and its subdivision, the Office for Civil Rights (OCR). However, enforcement was mild and violations continued to occur.

On February 17th, 2009 President Obama signed the American Recovery and Reinvestment Act (ARRA) and the subdivision, Health Information Technology for Economic & Clinical Health Act (HITECH). The ARRA was created, "To promote accountability by coordinating and conducting oversight of Recovery funds to prevent fraud, waste, and abuse and to foster transparency on Recovery spending by providing

the public with accurate, user-friendly information" ("The Board"). The HITECH Act specifically targeted the health industry's carelessness with private health information. It invested $20 billion into the electronic exchange of health information and strengthened the privacy and security of health information. On February 18th, 2010, the HHS and OCR began enforcement of the ARRA and HITECH Acts.

As a part of the ARRA, the HITECH Act broadened the capacity of HIPAA in the following ways:

- The HHS and the Federal Trade Commission (FTC) are responsible for the implementation of HIPAA.
- Business associates are subject to and must comply with HIPAA's requirements, including security provisions, policies and procedures, and breach notifications.
- Expansion of methods of enforcement and penalties for violations made by covered entities, business associates, and individuals.
- Mandatory auditing and investigating.
- Electronic Health Records (EHRs) and Electronic Protected Health Information (ePHI) are now subject to HIPAA.

WHO IS AFFECTED?

Everyone is affected by HIPAA, but in different ways. Anyone's health information in the United States or Puerto Rico is protected by HIPAA. Patients have 6 rights, regarding their privacy, that are secured by HIPAA:

1. The right to restrict **disclosure** to others
2. The right to receive an account of PHI disclosures
3. The right to receive PHI by alternative means
4. The right to access and copy information
5. The right to request PHI amendments
6. The right to file a complaint

Covered entities (CEs), **business associates (BAs)** are required to comply with HIPAA and the HITECH Act. Even individuals must understand and comply with HIPAA and the HITECH Act as it relates and effects their work and performance.

A covered entity includes any entity that is covered or must comply with HIPAA. Originally HIPAA only applied to covered entities. According to the *Code of Federal Regulations*, a "Covered entity means:

(1) A **health plan**.
(2) A **healthcare clearinghouse**.
(3) A **healthcare provider** who transmits any health information in electronic form" (1 45CFR164.302).

Please note that healthcare providers who do not submit HIPAA transactions themselves but utilize other entities (such as a billing service or a hospital acting on behalf of the provider) must comply with HIPAA standards and regulations.

With respect to a covered entity, a business associate is a person or organization who the covered entity discloses protected health information to so that the person or organization can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Examples include lawyers, auditors, consultants, third-party administrators, healthcare clearing houses, data processing firms, and billing firms. Originally, HIPAA did not include that business associates had to be compliant. At that time, a covered entity could only ensure that BA's maintained HIPAA compliancy through a business associate contract. Now the HITECH Act includes that BA's must also comply with HIPAA standards and regulations, including security provisions, policies and procedures, and breach notifications.

ENFORCEMENT & PENALTIES

Enforcement of the HIPAA & HITECH Act regulations and standards are the responsibility of the Office of Civil Rights (OCR), a division of the HHS. Enforcement activities include working with CEs and BAs to secure compliance through the use of technical assistance, answering questions and providing interpretations of the regulations. In addition, the OCR investigates complaints and violations (or breaches), conducts audits to establish compliance, and issues fines and penalties for violations. In fact, due to the HITECH Act, the Secretary of HHS is required to investigate every HIPAA complaint for willful neglect and impose a civil monetary penalty.

There are two types of violations that can occur and that the OCR investigates: civil and criminal violations. A civil violation is considered a less serious violation and covered entities and business associates are subject to civil penalties. A criminal violation is considered to be a serious violation and covered entities, business associates and individuals are subject to criminal penalties. An individual is criminally accountable for his or her own action, even when those actions are performed for the benefit of the employer. Criminal violations are usually turned over to the US Department of Justice (DoJ). The DoJ can then work with the Attorney General of the particular state in which the violation occurred if necessary. Due to the HITECH Act, the Attorney General of a state can bring civil suits in federal courts on behalf of their state's individual patients for HIPAA violations.

HITECH Act breaks civil penalties into four tiers:

Tier 1: Offender didn't know, and by reasonable diligence would not have known, that he/she violated the law.
- Minimum of $100 per violation – Annual maximum of $25,000 per violation for repeated violations
- Maximum of $50,000 per violation – Annual maximum of $1,500,000

Tier 2: Violation due to reasonable cause and not willful neglect.

- Minimum of $1,000 per violation – Annual maximum of $100,000 per violation for repeated violations
- Maximum of $50,000 per violation – Annual maximum of $1,500,000

Tier 3: Violation due to willful neglect but was corrected within 30 days.

- Minimum of $10,000 per violation – Annual maximum of $250,000 per violation for repeated violations
- Maximum of $50,000 per violation – Annual maximum of $1,500,000

Tier 4: Violation due to willful neglect and was not corrected within 30 days.

- Minimum of $50,000 per violation – Annual maximum of $1,500,000 per violation for repeated violations
- Maximum of $50,000 per violation – Annual maximum of $1,500,000

CEs and BAs are required to follow both federal (HIPAA & HITECH Act) laws and state laws. State laws can vary widely but if a state law is more stringent than that of HIPAA, the state law takes precedence in its area. Therefore, it is important to not only understand HIPAA and the changes of the HITECH Act but also state laws.

BREACH REQUIREMENTS

The HITECH Act defines a **breach** as, "The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." Breaches should be taken seriously, not only because those responsible for the breach are subject to civil or criminal penalties but also because patients could unwillingly become victim to fraud or other losses. Therefore it is important to not only do everything possible to secure PHI but CEs/BAs to have policies and procedures in place to accommodate any HIPAA or HITECH Act related questions, complaints, or reports of violations.

As part of the HITECH Act, the *Breach Notification Interim Final Rule* was created to encourage covered entities and business associates to quickly notify individuals affected by breaches. Covered entities and business associates must notify individuals whose protected health information has been, or is believed to have been, breached. Business associates that discover a potential or definite breach must also notify the related covered entity of those individuals who protected information has been or is believed by the business associate to have been breached. Breach notifications must me made "without reasonable delay" and no later than 60 calendar days after the CE or BA discover the breach.

For breaches involving less than 500 individuals:

- The individuals must be sent breach notifications by first class mail or, if stated as a preference by the individual, by email.

- If there is insufficient contact information for 10 or more affected individuals, a breach notice should be placed on the entity's website or in major media where affected individuals will likely be able to view the breach notification.
- The entity should keep a log of breaches and notifications and submit the log to the HHS Secretary annually.

For breaches involving over 500 individuals:

- The HHS Secretary must be notified immediately.
- The entity and the breach will be publicly posted on the HHS website.
- Prominent media outlets serving a State or jurisdiction must be notified of the breach.

All breach notifications must include:

- A description of the breach that happened, when it happened, and when the breach was discovered.
- A description of the protected health information that was involved in the breach and left unsecured.
- Steps individuals should take to protect themselves from potential fraud or other losses.
- A description of what the involved entity is doing/plans on doing to investigate the breach, diminish fraud or other losses, and to protect against further breaches.
- Contact procedures and information of the involved entity for affected individuals to contact for questions, concerns, and any additional information.

Please take note that all documentation associated with breaches and breach notifications must be retained by the entity for a period of 6 years, according to HIPAA regulations.

COST OF IMPLEMENTATION

Implementing HIPAA and the HITECH Act's regulations is costly. The major expenses include: using and disclosing only minimum necessary individually identifiable information, developing policies and coding privacy procedures, hiring privacy officials for each entity and the training of all personnel on the provisions of the policies.

In the past, the cost of implementing HIPAA and becoming compliant had been compared to the cost of preparing for Y2K. However, actually calculating the cost of implementing HIPAA can be difficult. There are many factors and therefore multiple results. To try and even get an idea of the costs, the American Hospital Association issued a "Report on the Impacts of the HIPAA Final Privacy Rule on Hospitals." According to the report, the initial projection of the total cost for hospitals over five years could have ranged from $4 to $22.5 billion. This estimation does not include other medical providers or facilities.

Through the ARRA and HITECH Act, the government is, “Investing $20 billion in health information technology infrastructure and Medicare and Medicaid incentives to encourage doctors and hospitals to use HIT [Health IT] to electronically exchange patients’ health information” (Health Information Technology). However, this will be, “Saving the government $10 billion, and generating additional savings throughout the health sector, through improvements in quality of care and care coordination, and reductions in medical errors and duplicative care” (Health Information Technology). This is just the beginning of what the costs are, providers and individuals will also be forced to invest money to continue to remain compliant.

Processing the scope of HIPAA and the HITECH Act can be difficult, especially with all of the requirements and costs. Please remember that these regulations are in place to improve health information privacy. Confidentiality is the key to ensuring that patients get adequate care.

REVIEW OF CONCEPTS

- **Individually Identifiable Health Information / Protected Health Information (PHI)** – Any information, including demographic information collected from an individual, that:
    - Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
    - Relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual; and
    - Identifies the individual, or there is a reasonable basis that the information can identify the individual.
- **Electronic Protected Health Information (ePHI)** – Any of the individually identifiable health information / protected health information (PHI) that is transmitted electronically or digitally.
- **Covered Entity (CE)** – There are three entities that must comply with HIPAA regulations:
    - A health plan;
    - A healthcare clearing house;
    - A healthcare provider who transmits any health information in electronic form.
- **Business Associate (BA)** – With respects to a covered entity, a person or organization whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. A BA was not responsible to comply with HIPAA until the HITECH Act.
- **Health Plan** – An individual or group plan that provides, or pays the cost of medical care. A health plan includes the following, and any combination thereof:
    - A group health plan if the plan has more than 50 participants or is administered by an entity other than the employer who established and maintains the plan
    - A health insurance issuer
    - A health maintenance organization
    - Part A or B of the Medicare program
    - The Medicaid program
    - A Medicare supplemental policy
    - A long term care policy
    - An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to two or more employees
    - The healthcare program for active military personnel
    - The Veterans healthcare program
    - The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
    - The Indian health service program
    - The Federal Employees Health Benefit Program
- **Healthcare Clearing House** – A public or private entity, including billing services, re-pricing companies, community health management information systems or community health

information systems, and “value-added” networks and switches that does either of the following:

  - Processes or facilitates the processing of health information received from another entity in a non-standard format or containing non-standard data content into standard data elements or a standard transaction.
  - Receives a standard transaction from another entity and processes or facilitates the processing of health information into non-standard format or non-standard data content for the receiving entity.

- **Healthcare Provider** – A provider of medical or health services or supplies and any other person or organization that furnishes, bills, or is paid for healthcare services or supplies in the normal course of business.
- **Breach** – As defined by the HITECH Act, “The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

WORKS CITED

"AMA - HIPAA Violations and Enforcement." *American Medical Association*. Web. 03 Mar. 2010. <http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.shtml>.

Code of Federal Regulations, 1 45 CFR 164.302 (2009). Print.

Hartley, Carolyn P., and Edward D. Jones III. *HIPAA Plain & Simple A Compliance Guide for Health Care Professionals*. [Chicago]: AMA, 2004. Print.

"Health Information Technology for Economic and Clinical Health Act or HITECH Act." *Waysandmeans.house.gov*. Committee on Ways and Means, 16 Jan. 2009. Web. 21 Jan. 2010. <http://waysandmeans.house.gov/media/pdf/110/hit2.pdf>.

Health Insurance Portability and Accountability Act of 1996, § 261 (1996). Print.

"Report on the Impacts of the HIPAA Final Privacy Rule on Hospitals." *Aha.org*. American Hospital Association, 29 Mar. 2001. Web. 22 Jan. 2010. <http://www.aha.org/aha/content/2001/pdf/FCGMarch2001.pdf>.

"The Board." *Recovery.gov*. Web. 19 Jan. 2010. <http://www.recovery.gov/About/board/Pages/TheBoard.aspx>.

QUESTIONS

1. HIPAA focuses on which of the following areas?
    a. Security
    b. Privacy
    c. Transactions & Code Sets
    d. All of the Above
2. HIPAA stands for:
    a. Health Information Protection and Accountability Act
    b. Health Insurance Portability and Accountability Act
    c. Health Insurance Protection and Assessment Act
    d. None of the Above
3. Which of the following is not considered a covered entity?
    a. A health plan
    b. A health insurance carrier
    c. A healthcare clearing house
    d. A healthcare provider
4. Business associates had to comply under HIPAA but not with the HITECH Act.
    a. True
    b. False
5. The HITECH Act expanded the capacity for HIPAA in the following ways except:
    a. The HHS and OFR are responsible for the implementation of HIPAA
    b. Business Associates must comply with HIPAA
    c. EHRs and ePHI are subject to HIPAA
    d. Mandatory auditing and investigating
6. Which of the following is not one of the six patient rights regarding their privacy?
    a. The right to request PHI amendments
    b. The right to receive an account of PHI disclosures
    c. The right to access other patient information
    d. The right to file a complaint
    e. The right to access and copy information
    f. The right to restrict disclosure to others
    g. The right to receive PHI by alternative means
7. Which of the following governmental regulatory agencies are responsible for enforcing the HIPAA & HITECH Act regulations?
    a. The Department of Health and Human Services (HHS)
    b. The Office of Inspector General (OIG)
    c. The Office of Civil Rights (OCR)
    d. None of the Above
8. The HITECH Act breaks violations into four tiers, the tier 1 penalty per violation is:
    a. $50
    b. $100

c. $150
d. $200

9. If California State Law regarding privacy protection is stricter than HIPAA, HIPAA will take precedence.
    a. True
    b. False
10. A breach notification must be sent within how many days?
    a. 30 Days
    b. 60 Days
    c. 6 Months
    d. 1 Year