Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Developed by:

Patricia Hyland, BS, RRT

Department Chair, ICVT,PAR & RES programs at Hudson Valley Community College, Troy, NY

HIPAA Origins

- On August 14, 2002, the United States Department of Health and Human Services (HSS) released the final rule on Standards for Privacy of Individually Identifiable Health Information, implementing the privacy requirements of the Administrative Simplification subtitle of HIPAA. (HHS Privacy Rule, 2002).

HIPAA Origins

- This comprehensive federal regulation gives individuals sweeping protections of privacy of their medical records
- The final privacy rule takes effect April 14, 2003.

HSS Secretary Tommy G. Thompson

"Patients now will have a strong foundation of federal protections for the personal medical information that they share with their doctors, physician's practices and others who provide their care and help pay for it, . . . The rule protects the confidentiality of Americans' medical records without creating new barriers to receiving quality health care. It strikes a common sense balance by providing consumers with personal privacy protections and access to high quality care."

HSS Secretary Tommy G. Thompson(HSS Press Office, 2002).

legislative goals of HIPAA

1. Guarantee health insurance coverage when workers change or lose their jobs
2. Reduce fraud and abuse in medical billing
3. Protect health information
4. Establish standards for administrative simplification

Definitions Important to HIPAA

- **Privacy**: addresses who may access information about an individual and the assurance that an individual's personal information will not be disclosed to others who are not involved in the individual's direct treatment or health care.

Definitions Important to HIPAA

- **Covered Entities**: Health care providers that conduct one or more of the eight electronic transactions stipulated in HIPAA, health plans and health care clearinghouses.

Definitions Important to HIPAA

- **Individually Identifiable Health Information (IIHI)**: Any subset of health information collected from an individual that
  - is created or received by a health care provider, health plan, employer, or health care clearinghouse
  - relates to the past, present or future physical or mental health condition; past, present and future provisions of care to an individual; or past present and future payment for the provision of health care to an individual and identifies the individual

Definitions Important to HIPPA:

Protected Health Information (PHI)

- All individually identifiable health information transmitted or maintained by a covered entity, regardless of form.
- transmitted by electronic media,
- maintained in any electronic media
- transmitted or maintained in any other form or medium, including paper records, oral communications and faxed documents. Note that electronic media includes Internet, Extranet, leased lines, dial up lines, private networks, and transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

Protected Health Information (PHI) Definition:

- PHI may exist in written, electronic, oral, or any other form
- Examples include:
  - Patient's name
  - Address
  - Phone number
  - the individual's social security number or any other information by which an individual could be identified

Definitions Important to HIPAA

- **Disclosure**: the release, transfer, and provision of access or divulgence of IIHI in any manner to anyone outside of the entity that maintains the IIHI.

Definitions Important to HIPAA

- **Use**: the employment, application, utilization, examination or analysis of IIHI within an entity that maintains IIHI.

Definitions Important to HIPAA

- **Designated Record Set**: a group of records maintained by or for a covered entity that are essential to the scope of the entity's operations and are used to make decisions about individuals. A record is defined as any item collection or grouping of information and is maintained, collected, used or disseminated.

Definitions Important to HIPAA

- **Minimum Necessary Information**: permitted routine disclosures must limit the PHI used or disclosed to the minimum necessary to achieve the purpose of that use or disclosure.

Definitions Important to HIPAA

- **De-identified Information**: health information is considered de-identified when it does not identify an individual and the covered entity has no reasonable basis to believe that the information can be used to identify the individual

Examples of Identifying Materials:

- Names
- All geographic subdivisions smaller than a state
- All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death, and all ages over 89

Examples of Identifying Materials:

- Telephone Numbers
- Fax Numbers
- Internet Protocol address number
- Biometric identifiers including fingerprint or voice recognition
- Electronic mail addresses
- Social security numbers
- Medical record numbers

Examples of Identifying Materials:

- Full face photographic images and any comparable images
- Any other unique identifying number characteristics or code
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers, including license plate numbers
- Device identifiers and serial numbers
- URLs

Identifiers

- The identifiers allowed in the limited data set are:
- Admission, discharge and service dates
- Birth date
- Date of death
- Age (any)
- Geographic subdivisions (all but street address

Definitions Important to HIPAA

- **Limited Data Set** in addition to de-identified health information, the Privacy Rule allows a limited data set to be used for research, public health or health care operations purposes. The covered entity is permitted to disclose PHI, with direct identifiers removed, subject to obtaining data a use agreement from the entity receiving the limited data set.

Administrative Simplification

- Administrative Simplification is broken down into three categories that may be likened to the three legs of a stool. If any one leg is removed, the stool will topple and similarly if a Health Care organization fails to address any one component of Administrative Simplification, its HIPAA compliance efforts will fail .

Administrative Simplification Components: Standards for Privacy of the Individually Identifiable Health Information

- The Privacy component is based on the need to protect the privacy of every patient's personal health information. It applies to health information in written and oral electronic or any other form.

Administrative Simplification Components: Standards for Security and Electronic Signature

- The Security component is based on the need to ensure the integrity of and to control access to health information. It's designed to protect information from alteration, destruction, loss and accidental or intentional disclosure to unauthorized persons

Administrative Simplification Components: Standards for Electronic Transactions and Code Sets

- The electronic transaction component is based on the need for health care entities to be able to communicate efficiently with one another on such basic activities as:
  - claims processing
  - payment
  - establishing who is and isn't covered under a health plan
  - Determination of a patient's level of eligibility for services

Administrative Simplification Components: Standards for Electronic Transactions and Code Sets

- Medical practices and businesses subject to HIPAA regulations are referred to as covered entities. They include health care providers, health care plans and claims clearinghouses

Administrative Simplification Components: Standards for Electronic Transactions and Code Sets

- The purpose of this group of regulations is to provide:
  - a uniform selection of diagnosis and service codes
  - specific standard electronic transaction formats
  - Overall simplification and streamlining of electronic communications between covered entities.

"The Privacy Rule"

- The privacy rule was enacted to protect individuals from discriminatory or wrongful use of their personal health information such as:
  - Insurers using it to deny life or disability coverage
  - Employers using it as the basis for hiring or firing decision
  - Nosey neighbors, family member
  - Reporters using it for any number of unnecessary or exploitive purposes

In accordance with the privacy rule, health care providers must:

- obtain specific individual authorization before using or disclosing protected information in most non-routine circumstances such as releasing information to an employer
- provide patients with written notice of their privacy practices and the patients' privacy rights
- obtain specific individual authorization before sending marketing materials

HHS 2002

In accordance with the privacy rule, health care providers must:

- not circumvent the rule through the use of business associate agreements
- provide access by patients to their medical records, allow and process requests for changes to correct errors, and provide an accounting of non-routine uses and disclosures

HHS 2002

HIPPA Enforcement

- Responsibility of the Department of Health and Human Services (DHHS), Office for Civil Rights.
- There is no provision allowing patients to sue for violations of HIPAA but civil and criminal penalties do exist :
  - Fines up to $50,000 and/or imprisonment for up to 1 year for knowingly using Protected Health Information (PHI) inappropriately
  - Fines up to $100,000 and/or imprisonment for up to 5 years for inappropriately accessing PHI under false pretenses
  - Fines up to $250,000 and/or imprisonment for up to 10 years for any person or entity knowingly disclosing PHI for the purpose of malicious harm or for personal or commercial gain

HIPPA Compliance

- Compliance requires that covered entities establish policies, and procedures which include:
  - ✓ designation of a privacy office
  - ✓ privacy training for all employees
  - ✓ reasonable safeguards to prevent intentional or individual misuse of protected health information.
  - ✓ Sanctions for employee violation of any of the privacy requirements

HIPPA Compliance

- Covered entities must maintain documentation offering that every employee has completed Privacy training.
- Health care plans and providers are required to make a good faith effort to give a written notice to individuals covered under the plan or receiving health care called the “Notice of Privacy Practices”.

Notice of Privacy Practices

- Must explain the uses and disclosures of protected health information that may be made by the covered entity.
- Must explain the individual's rights and the covered entity's responsibilities with respect to PHI.
- Must be written in plain language so that the average reader can understand it.
- Only needs to be given once to the Individual unless the entity's privacy policy changes.
- Covered entities are legally required to follow the policies and procedures designated in their privacy notice.

Notice of Privacy Practices

- A covered health care provider having a direct treatment relationship with an individual must make a good faith effort to obtain the individual's written acknowledgement that he or she received the provider's notice of privacy practice.

Notice of Privacy Practices

- The NPP need not be given at every visit but with the exception of emergency situations must be given at the initial service regardless of whether the service is given personally or electronically.
- It must be posted in a clear and prominent location in the provider's service site.

Notice of Privacy Practices

- A Privacy notice must describe how PHI may be used by a covered entity for treatment, payment and many normal business operations.
- With only a few exceptions, covered entities may not use or disclose PHI for non-routine purposes unless proper authorization by the Individual is in place.

Notice of Privacy Practices Must :

- Indicate the intended specific uses and disclosures of the individual's PHI and must be signed and dated by the individual requesting disclosure..
- Be precise in its language and apply only to the specific activity identified in the form.
- Limited use and disclosure of PHI for non-routine purposes without authorization is permitted in circumstances where there is an overriding public interest.

Notice of Privacy Practices: Circumstances of Overriding Public Interest

- Notification of exposure to infectious disease to individuals effected and government agencies
- Reporting births and deaths
- Reporting child abuse or neglect
- Reporting adverse reactions to medications
- Notification of recalls for devices
- Disease prevention

Notice of Privacy Practices

- Individuals have the right to request restrictions on the use and disclosure of their PHI. Agreement to such a request is not required but if the restriction is agreed to by the covered entity it must abide by the restriction except in case of emergency. Any restriction agreed to must be documented and maintained for at least six years

PHI Disclosure Accounting

- Individuals have the right to receive an accounting of all non-routine disclosures of their PHI within a six-year period prior to their request. The clock starts ticking on the implementation date for the rule. Covered entities that did not track disclosure prior to that date will not be in violation of the rule if they make their best effort at collecting and providing the information to the individual requesting an accounting.

PHI Disclosure Accounting

An accounting of disclosures must include:

- The date of each disclosure
- The name of the entity or person who received the PHI
- If known, the address of such entity or person
- A brief description of the PHI disclosure
- A brief statement of the purposes of the disclosure that reasonably informs the individual of the basic for the disclosure.

Access

- The Privacy rule, with very few exceptions, gives individuals the right to access, inspect and copy PHI used to make decisions about them.
- Access must be granted within 30 days of a request if the information is maintained or accessible on-site.
- If maintained off-site access must be granted within 60 days of the request.

Exceptions to Access

- Before the health information is released to the individual however, any element that falls under one of the exceptions should be identified and removed. The exceptions to a patient's right to access his of her own PHI are:
  - psychotherapy notes
  - information compiled for use in a civil or criminal trial or administrative proceeding
  - certain health information maintained by a covered entity that falls under the CLIA of 1988 act.

PHI Amendments

- individuals have the right to request an amendment of their PHI. The request may be denied if the PHI is accurate and complete or was not compiled by the covered entity receiving the request.
- If a request for amendment is denied, the individual must be informed of options regarding future disclosures of the information in dispute.

Parental Control of a child's PHI

- Generally, parents have access to and control of the PHI about their **unemancipated** minor children under the Privacy rule.
- There are a limited number of exceptions to parental access and control of PHI, such as:
  - testing for HIV where State law permits an adolescent to be tested without the consent of a parent.
  - In certain cases, minors have the ability to obtain specified health care without parental consent under state or other applicable laws. In such cases it is the minor, not the parent, who is afforded the right to exercise the privacy rights afforded to individuals under the Privacy rule

Parental Control of a child's PHI

- Another exception under the Privacy rule exists when the provider is concerned about abuse or harm of a minor.
- A parent might not be recognized as a personal representative of the minor by the covered entity in these cases. The provider may exercise his or her professional judgment and refuse access to or disclosure of PHI about the minor.

Security Rule

- The focus of this rule is to safeguard PHI from destruction, loss, alteration or unauthorized disclosure. Although the proposed security rules specifically addresses only electronic PHI, it would be consistent with the spirit of the rule to secure all forms of PHI as well

Security Rule

- Covered entities must assess potential risk to the PHI in their possession and develop, implement and maintain appropriate security measures. These measures must be documented and kept current.

Security Rule

- The HIPAA security rule covers four main subject areas: 1) administrative procedures, 2) physical safeguards, 3) technical security services and 4) technical security mechanisms. The security rule also requires covered entities to designate a Security Officer to oversee security implementation.

Security Rule Safeguard Examples:

1. Computer hardware and software
2. storage and disposal of data and back-up of data
3. Controlling who has access to data
4. Maintenance of facilities and visitor access to facilities and the testing and revising of electronic programs

Physical Safeguards

- Physical safeguards should be provided for medical records on paper and as reasonably possible for oral communications of HPI as well.
- Example of safeguarding oral communication is to make sure the door is closed in examining rooms during conversations with patients.

Reference Websites

- *HIPPA privacy: Joint information center* http://www.bicker.com/attserv/practice/hcare/hipaa/164.530b.asp
- HHS Privacy Rule, 45 C.F.R. § 160, 164http://www.hhs.gov/ocr/hipaa/privrulepd.pdf
- *HSS issues first major protections for patient privacy*. http://www.hs.gov/news/press/2002pres/20020809a.htm

Practice Scenario for Privacy Rule: Would looking at this patient's chart be a violation of HIPAA?

- *Medical Receptionist*: Hi Nancy, I'm trying to find out about a friend of mine who's a patient of Dr. Higin. Her name is Rachel Smith.
- *Nurse*: Rachel Smith? - She's a patient here?
- *Medical Receptionist*: Yes, she's a patient but she's also my Goddaughter, she's 7 years old and she's been sick a lot lately. I checked her in yesterday to see Dr. Higin.
- *Nurse*: Oh wow, I remember her I think. I hope it's nothing serious. Let's look at her chart.

Patient Rights Scenario

Caller: Hi, I am calling to find out about a patient of yours, Betty Boop. This is her husband Bob Boop. I wanted to find out about her test results. The Doctor said he'd have them today

Medical Receptionist: I'm afraid I can't give you that information.

Caller: Why not? I told you that I'm her husband. Can I give you her social security number or something to verify who I am?.

Receptionist: No, that won't be necessary but if your wife would give us a call, we would be happy to give her the results.

Caller: My wife's at work and she asked me to call

Receptionist: Well I'm afraid she didn't tell us about that.

Patient Rights Scenario

Caller: This is ridiculous! Let me speak to the Doctor.

Medical Receptionist: I'm sorry Mr. Boop but the doctor is with a patient now and it wouldn't matter anyway. When it comes to a patient's protected health information we are bound by very strict federal privacy rules

Question: Did the receptionist respond appropriately according to the HIPAA Privacy rule?

Practice Scenario for Security Rule

A Nurse Manager sees a post it note on the Medical Transcriptionist's computer screen that looks like a password and asks her what it is.

Medical Transcriptionist: Sorry, I can't keep all of my passwords straight.

RN: Please put them in a notebook and keep it locked in your desk. You'll have to remove this.

Medical Transcriptionist: Ok, but what's the big deal?

Nurse Manager: The big deal is that anyone can use your passwords to gain access to a lot of sensitive information.

Practice Scenario for Security Rule:Do you think that the Nurse Manager is right according to the HIPAA Security Rule?

Medical Transcriptionist: Why would anyone want to do that?

Nurse Manager: Don't you read the papers? Information theft is a big deal these days. But besides that, consider Dr. Higin's son instead. Dr. Higin sometimes brings him in on Sundays when he comes in to dictate his notes. The kid's a real computer genius. He wouldn't need a reason, he might do it just to see if he could. If he did and the information ever got out and into the wrong hands, we'd be liable for all kinds of finds and penalties and you'd be out of a job. Maybe it's not likely to happen, but is it really worth the risk just to save all the time and effort of unlocking and opening your desk drawer?

Additional Thought Questions

- Does my job performance ensure the privacy and security of PHI?
- Is my computer terminal or workstation in an area where unauthorized people can gain access to PHI?
- What precautions can I take to protect a patient's right to privacy when I have to discuss the patient's condition within earshot of others?
- If I discover a break in security, do I know the process for me to report it?

HIPAA Training Test

Please click here to open and print the test.