HIPAA Training
What is HIPAA?

- HIPAA— is an acronym which stands for Health Insurance Portability and Accountability Act of 1996.
- HIPAA was enacted on August 21, 1996.
- HHS is the primary federal agency responsible for administering HIPAA (HHS is the abbreviation for the U.S. Department of Health and Human Services.)
Who passed the HIPAA law?

Congress passed the landmark HIPAA law to:

- Provide consumers with greater access to health care insurance
- Protect the privacy and security of their health care data and to promote more efficiency
- Bring standardized into the health care industry (Accountability)
- Improve the efficiency of health care systems.
Health care was the main reason for HIPAA to be implemented. There was no standardization among insurance companies and Providers and several medical errors had been issued or billed incorrectly.

Congress agreed with concept of standardization, but concerns grew regarding confidentiality of a patient’s information; Privacy regulations for Protected Health Information (PHI) were developed.
Sue’s husband works at a hospital in the Emergency Department. Her husband has never divulged personal information such as names, dates of birth, treatment plans, or anything that would let her know who the person was. However, he has, on occasion, especially to gross her out, told her that for instance—he had to lance a wound a squeeze a bunch of pus out of it, or that he learned how to insert a Foley catheter into a woman, or that while inserting a thermometer into an infant's behind, that he was pooped all over.

* Is this a HIPAA violation?
No, he did not disclose the patients names. He only disclosed the procedures he performed. If he would have disclosed patients names then he would be in violation of HIPAA.
HIPAA law is not just for Health care.

- Insurance fraud and reform
- Pretax medical savings accounts
- HIPAA is a very complex federal law involving many regulations that affects the entire health care system— from “individuals” to employers, health plans, health care providers, health care clearing houses and other entities providing health information services.
Information that concerns an individual’s past, present or future physical or mental health, health care treatment, or payment for the provision of healthcare.

Information that identifies the individual or can reasonably be used to identify the individual (e.g. date of birth, SSN).

If common identifiers removed ("de-identified"), covered entity has no way of recovering that information, HIPAA does not apply.
No Double Standards!

“Ok, I know you’re still mad about that photo I took of your mother’s medical procedure and posted to my Facebook wall. But to Tweet your friends about my hemorrhoids is violating my privacy.”
HIPAA is just for health care professionals and if you are not employed for a health care company you can provide clients and patients information with no penalties.
No, if you provide confidential and private information on a client or patient you are violating the HIPAA violation.
HIPAA: 5 major provisions

- Title I: Health insurance Access, portability and renewability (AKA insurance reform)
- Title II: Preventing Fraud & Abuse; Administrative simplification; Medical Liability reform
- Title III: Tax related Health Provisions
- Title IV: Application & Enforcement of Group Health Plan Requirements
- Title V: Revenue Offsets
The primary Administrative Simplification objective:

- Improve effectiveness in health care delivery by creating standardized electronic data interchange formats.
- Implement controls to protect an individual’s health information
  - Mandated safeguards to protect access, use and disclosure of PHI and Electronic PHI
  - Penalties for non compliance.
Who must comply with HIPAA

- Everyone in health care or who are dealing with patient’s medical records.

- A covered unity includes:
  - Health plan
  - Health care clearinghouse
  - Health care provider
  - One that maintains protected health information: paper, electronic or oral
  - One that transmits PHI information
  - Business associates
Which of these health care professionals must comply with HIPAA?

A. Doctors
B. Doctor’s Assistants
C. Receptionists
D. Nurses
E. All of the above
F. None of the above
Answer

E. All of the above, because they all deal with PHI and electronic PHI.
Covered transactions

- Health claims or equivalent encounter information
- Health care payment & remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment & disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification & Authorization
What information does it apply to?

- HIPAA applies to:
  - Patient health information
  - Electronic patient health information
  - Covered transactions
HIPAA Penalties

- Penalties increased for failure to adopt & comply with the HIPAA privacy & Security rules.
- Penalties are based on a tiered structure according to the level of the violation:
  - If unaware of the violation, $100 for each incident up to a max of $25,000/ year, per violator.
  - If due to reasonable cause but not willful neglect, $1000 for each incident up to $100,000
  - If due to willful neglect but corrected, $10,000 for each violation up to $250,000
  - If due to willful neglect & uncorrected, $50,000 each up to $1.5 million.
  - Public exposure
  - Loss of accreditation
  - Imprisonment
Documentation Time Limits:
- Retain required HIPAA documentation for a minimum of 6 years from the date it was created or from the date it was last effected; whichever date is later. Includes:
  - Policies and procedures
  - Workforce training provided
  - Privacy notices
  - Privacy rule complaints and resolution
  - Business Associates contracts
  - Any other communication required by HIPAA to be in writing
State Laws

- HIPAA should not override stricter state laws.
  - For example...
    - In Texas the state requires that health care providers keep medical records for 7 years before discarding, but HIPAA requires only 6 years.
    - The health care provider in Texas should follow state law.
HIPAA privacy rule mandates privacy protection of **individually identifiable health information (IIHI)** when held by a covered entity, regardless of whether the information is used in an electronic format, except in limited circumstances.

- The privacy standards/administrative requirements grants patients a **RIGHT** to see, control, & receive a copy of their health information.
- The privacy rule allows for health information disclosure expectations (e.g. research, law enforcement, and incidental use)
Incidental Use & Disclosure

- An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the rule.
- It is not expected that a CE’S safeguards will guarantee their privacy of PHI from all potential risks.
- Incidental disclosures include the following occurrences:
  - Sign in sheets
  - Patient charts at hospital bedside
  - Doctors talking with patients in semi-private rooms
The standards mandate that a CE must safeguard individual’s health information that is created, held or transferred in electronic form (ePHI).

The rule does not apply to personal health information transmitted orally or in writing, paper to paper faxes, or voice mail.
Security Rule Applies to...

- Person/organization (a covered entity) who in the normal courses of business, transmits health information electronically.
  - Health plan – both individual and group plans
  - Health care clearinghouse – both public and private
  - Health care provider
Covered Entities

- Business Associates
- 3rd party Vendors
- Anyone who performs data transmission services on behalf of different CEs.
Electronic files should be backed up.
Security Standards – I

Administrative safeguards for ePHI

- Addressing various security issues regarding the CE’s daily operations.
- Managing the conduct of employees regarding ePHI
- Directing the selection, development, and use of “security controls”

- Required documented policies & procedures must be made available to people who are responsible for implementing the procedures.
Administrative Safeguards for ePHI

- Security Management Process
- Assigned Security Personnel
- Workforce Security
- Information Access Management
- Security Awareness & Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts & Other Arrangements
Physical Safeguards refer to controlling physical access to ePHI stored on computers and/or electronic devices by authorized individuals.

Physical Safeguards for ePHI
1. Facility Success Controls
2. Workstations Use
3. Workstation Security
4. Device & Medical controls.
Technical Safeguards detail how various technologies should be used to protect & control ePHI, but do not specify requirements for types of technology to use.

- The minimum standards or least that a CE must do to protect ePHI is defined but a CE may choose to do more.
- Such a decision should be made from the required individual Risk Analysis & Vulnerability Assessment. The rule requires a CE to document the process.
- While general threats to ePHI are known each CE own vulnerability results will determine the risk specific to that entity.
Security Standards III continued

- Technical Safeguards for ePHI
  - Access Controls
  - Audit Controls
  - Data Integrity
  - Person or Entity Authentication
  - Transmission Security

- Examples of Technical safeguards:
  - User IDs and Passwords
  - Encryption
Standards vs. Specifications

- Standards explain what a CE *must do*..
- Specifications explain *how to do it*
  - The 36 Implementation Specifications are further classified as either “REQUIRED” or “ADDRESSABLE”

- 14 Specifications are Required (R) = The CE must comply with the implementation
- 22 Specifications are Addressable (A) = “Addressable does not mean optional”
The security management process standards include the following *Required Specifications*:

- Risks Analysis
- Risk Management
- Sanction Policy
- Information System Activity Review
Information Access Management

- Isolation of Clearing house function – Health care clearinghouse is part of another organization because it had ePHI.
- Access Authorization
- Access Establishment & Modification – requires written policies and procedures.
- Examples:
  - Employee access and removal of access
The Covered Entity (CE) must:

1. Develop procedures & policies to identify security incidents & respond based on established protocols
2. Decreased the harmful effects of different security incidents which are already known to the health provided
3. Document all the security incidents and various outcomes.
Security Contingency Plans

- The covered Entity must provide:
  - Develop a Data Back up plan & Data recovery plan—establish & implement procedures for making exact copies of ePHI for restoration of data loss due to catastrophe
  - Test and revise procedures for the continuation of critical business process while protecting the security of ePHI when operating in emergency mode.
CE is required to maintain all documentation on its policies, procedures & decision for 6 years.

CE must on a regular schedule review all its documentation related to security and revise or update it as needed to ensure ePHI confidentiality, integrity, & availability.

CE might incur no Security Rule penalties for some implementation decisions later found not compliant as long as documentation is proper and available.
Examples of Non-Compliance Risks

- Financial penalties
- Litigation
- Increased cost of coverage
- Imprisonment
- Higher Capital costs which are associated with forced compliance
- Ransom audits.
HITECH – Health Information Technology for Economic and Clinical health Act

This act became a law as part of the American Recovery and Reinvestment Act of 2009 (ARRA)
Subtitle D– Privacy

- A significant part of the HITECH act
- Directly pertains to the HIPAA privacy & Security concerns associated with electronic transmission of Protected Health Information.

- The intent of Subtitle D– Privacy is to bring clarification to HIPAA Privacy & Security Rules, with the new requirements & changes that impacts Covered Entities and the Business Associates of Covered Entities.

Included in Part I are provisions that:

- Expand the HIPAA Privacy and Security Rules
- Initiate various changes that will have a direct impact on protected heath care information and the use & management of HER.
- Affect all Health Care Providers, Hospitals & 3rd party service providers, either maintain or required access to an individual’s medical information.
What does HITECH ACT apply to?

- New regulations that apply to 3rd party vendors or organizations
- New regulations that apply to Business Associates in the same manner that they apply to a Covered entity.
- Changes to the status or treatment of Business Associates
- New breach Notification requirements
- New rules for the accounting of disclosure of PHI
Effective January 1, 2011 and January 1, 2014
Must agree to patients PHI disclosure restriction requests
Must be aware there are expectations that exist regarding health plans and payments.
Business Associates

- Described as but not limited to:
  - Person or organization other than a member of the covered entity's workforce who . . .
  - Performs certain functions or activities on the behalf of covered Entities or . . .
  - Provides certain services to a Covered Entity that . . .
  - Involve the use or disclosure of individual identifiable health information (IIHI)
Subject to same HIPAA regulations as covered entities in the following areas.

- Must comply with HIPAA administrative Technical & Physical safeguards.
- Must established & Maintain appropriate HIPAA policies & Procedures
- Must document all Security Rule Compliance activates
- Will be responsible for same civil and criminal penalties
Business Associates –

- Must report breaches
- Contracts to include all new requirements
- Restricted from PHI uses and disclosures not in compliance with Business Associates contract

- Additions to Business Associates Category:
  - Personal Health Record Vendors
  - Health Information Exchange
Vendors or Organizations that exchange or provide PHI to CE & Business Associates are:
- Required to enter into a written contract with the CE
- Will be regarded as Business Associates
Covered Entities and Business Associates

- Prohibited of receiving payment for PHI unless authorized by the patient
- Must notify each patient who is affected by a breach when their private health information is accessed, acquired, or disclosed because of the breach
- Adhere to patients restriction on disclosures to health plans of their health information related to privately paid services.
Personal Health Records & Electronic Health Records

- **PHR** is a electronic record of an patients health information by which the patient:
  - controls access to the information
  - has the ability to manage, track, and participate in his or her own health care

- **EHR** is an electronic health record of a patients heath information that once existed in the patients paper medical record.
EHRs– Accounting of Disclosures

- Effective: January 1, 2011 & January 1, 2014
- (U.S. Department of Health and Human Services must adopt and publish standards within 6 months from enactment)

Accounting of Disclosures for EHRs:
- Disclosures of treatment, payment & operations
- Accounting must be made if requested & must include 3 years of medical record history
- Patient can be charged a “reasonable” fee for accounting cost, however, not greater than the direct labor cost.
Who must notify patients of any breach?

- Covered Entities
- Business Associates
- Personal Health Record Vendors
When Unsecured PHI was accessed, acquired or disclosure in a breach notifications to patient must be sent “without” reasonable delay” – no later than 60 days after breach.

- To be sent 1st class mail– unless specifically started by patient that information can be emailed.
- If 10 or more victims can’t be located, notice on website or in the media must be posted
- Breaches involving >500 victims: Mandatory & immediate reporting to HHS
- Breaching involving < 500 victims: CE keeps log, provide to HHS annually
- If more the 500 victims, HHS will publicly post on internet.

*Unsecured PHI is essentially any unencrypted data.
HIPAA Regulations

"WARNING. You have violated HIPAA! An email notification has been sent to a federal agency, your supervisor, and your mother."
Selling of Personal Health information

- NO SELLING OF PHI:
  - Change to HIPAA privacy rule – previously allowed for some uses.
  - No payment for PHI will be received by a covered entity, even if disclosure is permitted without an authorization from patient that includes permission to sell.
  - Expectations exist for: research, public health activities, sale or transfer of practice.
Definitions:

- **HIPAA** – Health Insurance Portability and Accountability Act of 1996
- **ARRA** – federal economic stimulus bill “American recovery and Reinvestment Act of 2009
- **HITECH** – Health information Technology for Economic and Clinical Health Act
- **HHS** – Department of Health and Human Services
- **EHR** – Electronic Health Record – electronic versions of patients history, maintained by the health provider in the course of care.
- **PHI** – Protected Health Information
- **ePHI** – The electronic version of Protected Health Information
Definitions continued:

- **Covered Entities**: Health plan, Health care clearinghouse, health care provider who transmits any information in electronic form in connection with transactions covered by HITECH.
- **Business Associates**: On behalf of CE, a person who performs, assist or provides, legal actuarial accounting, consulting, data aggregation management, administrative accreditation or financial services.
- **Security safeguards**: For the storage access and transmissions of an individual's protected health information.
- **Privacy**: Limits the use or disclosure of PHI.
References

US Department of Health & Human Services
http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

HIPAA Cartoons are copyrighted by R.J. Romero, www.hipaacartoons.com
Now go to the quiz! You will need an 80% to pass.