TODAY'S SESSION

- A Little Background....
- HIPAA Basics
- The Privacy Rule
- HITECH’s Breach Notification Regulations
- The Security Rule
- Resources

HOUSEKEEPING NOTES:

- This presentation reflects HIPAA as it stands today
  - Omnibus Rule's effective date of 3/26/2013
  - HITECH updates are included
    - However, I will not call them out separately or tell you how it used to be!
  - We will take a 15 minute break at approximately 10:20am; please feel free to get up as needed. This is a LONG session.
A LITTLE BACKGROUND

The modern version of the Hippocratic Oath:

“I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.”

- Late 5th Century B.C.

PRIVACY DEFINED

● In the United States:
  + 1890 U.S. Supreme Court justices Samuel Warren and Louis Brandeis publish “The Right to Privacy” in Harvard Law Review
  + Defined as “the right to be left alone”
  + Constitution does not specifically provide Right to Privacy
### Privacy Protections in the United States

Framework of Sectoral Laws and Self-Regulatory Model

- Fair information Practices Approach
  - Process-oriented
  - Two major concepts are Notice and Choice
    - Example: Gramm-Leach-Bliley Act (GLBA)
- “Permissible Purpose” Approach
  - Limits data use to purposes permitted under law
    - Example: Fair Credit Reporting Act (FCRA)
- Newer Approach:
  - Combine the above to have elements of each
    - Example: HIPAA

### Code of Fair Information Principles

- Developed in 1970s
- By U.S. Dept of Health, Education and Welfare Advisory Committee on Automated Data Systems (now HHS)

Core Elements:
- Individual Participation
- Disclosure
- Secondary Usage
- Record Correction
- Security

### Other U.S. Laws Dealing with Health Care Privacy

**Federal**
- Genetic Information Non-Discrimination Act (GINA)
- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Privacy Act of 1974 (regulates federal gov’t)
- Family Educational Rights & Privacy Act (FERPA)

**State**
- Security Breach Notification Laws
- Minors’ Rights
- Sensitive health conditions
  - Mental health
  - AIDS/HIV status
  - Psychiatric treatment
- Sector-specific
  - Regulates licensed providers
  - Insurance-specific regulations (DOI)

### Federal State

- Federal law resource: The Center for Democracy & Technology
**IMPORTANT DEFINITIONS**

Contrary - it would be impossible to comply with both laws; other law stands as obstacle to purposes of HIPAA

More stringent = prohibits or restricts a use or disclosure, permits greater rights of access or amendment, provides greater amount of information, provides greater scope or duration, increases privacy protections or reduces coercive effect of the circumstances surrounding the express legal permission, provides for retention or reporting of more detailed information or for a longer duration, provides greater privacy protection for the individual

**State laws contrary to HIPAA are preempted (trumped) unless:**
1. State law is more stringent
2. Law provides for reporting of disease, injury, child abuse, birth, death; for public health surveillance, investigation, or intervention
3. Minor exceptions for health plan reporting & if Secretary of DHHS deems otherwise

1. If not contrary, must comply with both

**42 USC § 290dd-2 & 42 CFR Part 2**

Purpose - to encourage patients to seek treatment without fear of having privacy compromised

Disclosure requires AUTHORIZATION

Exceptions are very limited

Issue: REDISCLOSURE NOT ALLOWED without another Authorization (not like HIPAA)

**BE CAREFUL!!**

**OTHER FEDERAL LAW - EXAMPLE**

× **42 USC § 290dd-2 & 42 CFR Part 2 (Part 2)**
× Federal law that regulates substance abuse treatment records (alcohol, drugs)

**BE CAREFUL!!**

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (“HIPAA”),**

× First federal law addressing all types of healthcare information
TWO OBJECTIVES OF HIPAA

- Portability
  + Ensure that individuals would be able to maintain their health insurance between jobs

- Accountability
  + Combat fraud & abuse
  + Designed to ensure the security and confidentiality of individuals’ information/data
  + Mandates uniform standards for electronic data transmission of administrative and financial data relating to patient health information

HIPAA ENFORCEMENT

- Civil Actions
  + By:
    - Office for Civil Rights of Dept. of Health and Human Services
    - State Attorney’s General Office
  + Types:
    - Civil Money Penalties
    - Settlements

- Criminal Actions
  + By U.S. Department Of Justice (DOJ)
  + Investigated by FBI
  + Against organizations subject to HIPAA
  + Against individuals

Source: http://www.hhs.gov/about/regionmap.html
### CIVIL MONEY PENALTY STRUCTURE

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each violation</th>
<th>For each violation of identical provision in Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1000 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Willful Neglect – Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1.5M</td>
</tr>
</tbody>
</table>

### CIVIL ENFORCEMENT OF HIPAA

- HHS announces first HIPAA breach settlement involving less than 500 patients – December 31, 2012
- Massachusetts Provider Settles HIPAA Case for $1.5 Million – September 17, 2012
- Alaska DHSS Settles HIPAA Security Case for $1.7 Million – June 26, 2012
- HHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards – April 13, 2012
- HHS settles HIPAA case with BCBST for $1.5 million – March 13, 2012
- Resolution Agreement with the University of California at Los Angeles Health System – July 6, 2011
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc. – February 14, 2011
- CEV Money penalty issued to Capital Health of Prince George’s County, MD – February 4, 2011
- Resolution Agreement with Management Services Organization Washington, Inc. – December 13, 2010
- Resolution Agreement with Rite Aid Corporation – July 27, 2010
- Resolution Agreement with CVS Pharmacy, Inc. – January 16, 2009
- Resolution Agreement with Providence Health & Services – July 16, 2008


### CRIMINAL ENFORCEMENT OF INDIVIDUALS

- "Knowingly" obtain or disclose PHI
  - up to $50K fine
  - imprisonment up to 1 year

- Offenses committed with "intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm"
  - Up to $250K fine
  - Imprisonment up to 10 years

- Commit offense under false pretense
  - up to $100K fine
  - Imprisonment up to 5 years
ENFORCEMENT EXAMPLES (CRIMINAL)

- 2009 (Florida): Two defendants convicted of offenses related to the theft of patient records from Palmetto General Hospital designed to further a credit card fraud scheme.

- September 2009 (Indiana): Defendant sentenced to 3 years in prison for stealing insurance records of over 800,000 individuals. The records included personally identifiable information, confidential medical information, and confidential email communications. The defendant had threatened to publish this personal information and confidential medical data on the Internet, unless each victim insurance company paid him $1,000 per week for four years.

STATE ATTORNEYS GENERAL (SAGS) ENFORCEMENT

- HITECH gave SAGs the authority to:
  - Bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules
  - Obtain damages on behalf of state residents
  - Enjoin further violations of the HIPAA Privacy and Security Rules

- Examples:
  - Connecticut AG - insurer Health Net, Inc. for $250,000 (July 2010)
    - Also settled with Vermont for $55,000 (1/2011) and New York
  - Massachusetts AG - South Shore Hospital for $750,000 (May 2012)
  - Minnesota Attorney General against business associate Accretive Health, Inc. (July 2012)

CLASS ACTION LAWSUITS

- HIPAA includes no private right of action

- Current class action lawsuits against covered entities for alleged failure to adequately protect individuals’ PHI
  - UCLA Health System - hard drive stolen from home of a former UCLA physician; reported breach (18,000 individuals)
  - Georgia hospital - loss of unencrypted PHI of >300,000 patients; reported breach (Owens, Healthcare, Inc., filed 6/4/2012)

- Must show: plaintiffs suffered an injury

- Recent court decisions - dismissed claims by plaintiffs based on finding that threat of future harm not enough
  - Paul v. Providence Health System-Oregon, 273 F.3d 106 (Or. 2012)

- Watch out: Court found “plausible injury” from breach of health plan in Florida
  - Curry v. AvMed Inc. (health plan in FL)
EVERYTHING WE LEARN AND DO FROM HERE ON IS TO HELP YOU WORK TOWARDS AN EFFECTIVE HIPAA COMPLIANCE PROGRAM

Willful neglect: "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated"

ADMINISTRATIVE SIMPLIFICATION

- Part 160 General Admin. Requirements
  + Subpart A: General Provisions
  + Subpart B: Preemption of State Law
  + Subpart C: Compliance & Enforcement
  + Subpart D: Imposition of CMPs (civil money penalties)
  + Subpart E: Procedures for Hearings

- Part 164 Security and Privacy
  + Subpart A: General Provisions
  + Subpart B: Reserved
  + Subpart C: Security Standards for the Protection of Electronic Protected Information
  + Subpart D: Reserved
  + Subpart E: Privacy of Individually Identifiable Health Information

Extra Subpart Changed under the Omnibus Final Rule except for Part 160; Subpart E

ADMINISTRATIVE SIMPLIFICATION (NOT PART OF TODAY’S DISCUSSION)

- Part 162 Administrative Requirements
  + Subpart A: General provisions
  + D: Standard Unique Health Care Identifier for Health Care Providers
  + F: Standard Unique Employer Identifier
  + I: General Provisions for Transactions
  + J: Code Sets
  + K: Health Care Claims or Equivalent Encounter Information
  + L: Eligibility for a Health Plan
  + M: Referral Certification & Authorization
  + N: Health Care Claim Status
  + O: Enrollment & Disenrollment in a Health Plan
  + P: Health Care Payment & Remittance
  + Q: Health Plan Premium Payments
  + R: Coordination of Benefits
PART 164 “PARTS”

SECURITY RULE
• Protects ELECTRONIC health information (E PHI)
• Organizations must ensure the availability, confidentiality, and integrity of that information

PRIVACY RULE
• Identifies what is to be protected
• Regulates what entities subject to HIPAA (covered entities) must do to safeguard information
• Outlines individual’s Rights regarding their PHI

BREACH NOTIFICATION RULE
• Requires WRITTEN NOTIFICATION to affected individual and federal government (and the media if >500 individuals affected) if a breach of unsecured PHI occurs

WHAT IS PROTECTED?

Protected Health Information (PHI):
• Refers to individually identifiable health information maintained by certain entities
• Relates to the past, present, or future health condition, treatment, or payment of a client
• Identifies the individual, or could be used to identify the individual
• Can be transmitted or maintained in any form or medium
  • Paper, electronic, verbal

THE MANY FORMS OF PHI
• Paper copies / printed copies
• Telephone calls and voice mail
• Photos / videos
• Verbal communication conversations
• Fax transmissions
• CD’s, thumb drives
• E-mail
• Tattoos?
INDIVIDUAL IDENTIFIERS OF PHI

- Name
- Address
- Social Security number
- Family History
- Telephone number
- Fax number
- Account numbers
- Medical record number
- E-mail address
- Dates
- Medicaid Client ID #

Take all these out and you have de-identified data – not subject to HIPAA!

WHAT IT TAKES TO MAKE PHI

Examples:

A list of social security numbers is not PHI

A list of patients’ names and dates of service at a physician’s office is PHI

A list of patients’ full dates of birth (07/03/91) and their chief complaint when presenting to a hospital is PHI

A list of medical codes is not PHI

WHO IS COVERED UNDER HIPAA?*

- Covered Entities
  - Providers
    - Hospitals, physicians, allied health providers, mental health practitioners, etc.
    - WHO ELECTRONICALLY BILL A STANDARD TRANSACTION REGULATED BY HIPAA
  - Health plans
  - Health care clearinghouses

- Business Associates
  - Their subcontractors who handle PHI
**ORGANIZATIONAL OPTIONS**

- Organized Health Care Arrangement (OHCA)
- Affiliated Covered Entities (ACE)
- Hybrid Covered Entity

You don't have to be one of these, but you may be!

**KNOW YOUR STRUCTURE UNDER HIPAA – IT DOES MAKE A DIFFERENCE!**

---

**BUSINESS ASSOCIATE**

1. A person who creates, receives, maintains, or transmits PHI on behalf of a CE (or another BA) for a function or activity regulated by the HIPAA Rules

2. ...where the provision of the service involves the disclosure of PHI

---

**WHAT IS A BUSINESS ASSOCIATE?**

1. A person who creates, receives, maintains, or transmits PHI on behalf of a CE (or another BA) for a function or activity regulated by the HIPAA Rules

2. ...where the provision of the service involves the disclosure of PHI

Note: Does not include disclosures to providers for treatment purposes!
BUSINESS ASSOCIATES & THE PRIVACY RULE

- BA is a BA **by definition** not by act of contracting with a CE
- Directly liable for:
  - Uses and disclosures of PHI not in accord with its BAA or Privacy Rule
  - Failing to disclose PHI when required by Secretary to investigate and determine BA's compliance with HIPAA
  - Failing to disclose PHI to CE, individual, or individual's designee as necessary to satisfy CE's obligations with respect to individual's request for electronic copy of PHI
  - Failing to make reasonable efforts to limit PHI to minimum necessary to accomplish intended purpose
  - Failing to enter into BAA with subcontractors that create/receive PHI
- Contractually liable for all other Privacy Rule obligations included in their contracts with CEs

BUSINESS ASSOCIATES & THE SECURITY RULE

- Must comply with ALL of Security Rule
- Must review and modify security measures as needed and update security measures accordingly
  - Must enter into contract with any subcontractors to protect electronic PHI
    - Must report breaches of unsecured PHI to BA to report to CE
    - Requirements of BAAs apply to BAs and their subcontractors in SAME MANNER as between CEs and BAs

**Subcontractor** - a person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the BA's workforce.

WHAT MUST YOU DO WITH BUSINESS ASSOCIATES?

- Enter into an Agreement with them that they will appropriately and adequately safeguard PHI
- Commonly referred to as: Business Associate Agreement (BAA) or Business Associate Contract (BAC)

BAAs or BACs have specific requirements under the Privacy, Security, Breach and Enforcement Rules
BASIC TENETS OF HIPAA

- HIPAA **prohibits** a covered entity from using or disclosing protected health information (PHI) without written authorization from the individual.

- Allowable exceptions include:
  - Treatment
  - Payment
  - Health care operations
  - Other, more limited, public interest disclosures

---

USE VS. DISCLOSURE

<table>
<thead>
<tr>
<th><strong>Use:</strong></th>
<th>Sharing</th>
<th>Employing</th>
<th>Applying</th>
<th>Utilizing</th>
<th>Examining</th>
<th>Analyzing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information is used when it moves within an organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Disclosure:</strong></th>
<th>Releasing</th>
<th>Transferring</th>
<th>Providing access to</th>
<th>Divulging in any manner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information is disclosed when it is transmitted between or among organizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

KEY CONCEPT

- To the individual when he/she requests it
- To the Federal government when they are investigating an Entity’s compliance with HIPAA

**HIPAA requires** disclosure of PHI in only two instances:

- Every other disclosure is **permissible** under the Rule.
TREATMENT
The provision, coordination or management of health care for an individual by providers

+ Example: The sharing of information by a physician who is providing healthcare to a patient to a specialist at a neighboring hospital where the patient is scheduled for surgery

PAYMENT
Activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual
Also includes eligibility verification and collections activities

+ Example: a physician sending health information about a patient to the patient’s insurance company to get paid for the services he/she provided

HEALTH CARE OPERATIONS
Activities of a covered entity that are related to the functions they perform

+ Examples: quality assessment and improvement activities, case management, care coordination, provider performance evaluation, credentialing, accreditation, audits, fraud and abuse detection, etc.
USES AND DISCLOSURES BASED ON TPO

- CE may use or disclose PHI for its own treatment, payment and health care operations
- May disclose to health care provider for provider’s treatment purposes
- May disclose to CE or provider for payment of CE or provider
- May disclose to another CE for that CE’s health care operations WITH CERTAIN RESTRICTIONS!

ALLOWABLE “PUBLIC INTEREST DISCLOSURES”

- Required by Law
- Authorized public health activities
- Victims of abuse, neglect, or domestic violence
- Health care oversight activities (i.e. audits)
- Workers’ compensation
- Judicial and administrative proceedings
- Law enforcement purposes
- Avert serious threat to health and safety
- Specialized government functions (i.e. national security issues)

Caution: these exceptions are narrowly defined under HIPAA.

OPPORTUNITY FOR INDIVIDUAL TO AGREE OR OBJECT

- Facility directories
- For involvement in the individual’s care and notification purposes
  + With individual present
  + When individual is not present
  + For disaster relief purposes
- About decedents to family members and others involved in care
  + “Care or payment for care”

*“in the exercise of professional judgment”
HOW HIPAA WORKS...

INCIDENTAL USE OR DISCLOSURE

- Defined: 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 HIPAA
- HIPAA permits certain incidental uses and disclosures IF:
  - You have put in place:
    - reasonable safeguards
    - minimum necessary standard policies, procedures & training

An incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule

AUTHORIZATIONS

All other disclosures require a valid written authorization from the individual
PERSONAL REPRESENTATIVES

- Person authorized under state/other law to act on behalf of individual for healthcare-related decisions
- Personal representative has ability to act for individual and exercise individual’s Rights under HIPAA
- There is an abuse, neglect, or endangerment exception

MINIMUM NECESSARY PRINCIPLE

- Requires Covered Entities to always limit any use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose

Handle PHI specific to your daily job functions on a need-to-know basis

Always consider minimum necessary when sharing individual’s PHI, even with co-workers
NOTICE OF PRIVACY PRACTICES

- Applies to providers and health plans
- Certain content requirements
  - How entity may use and disclose PHI about an individual
  - Individual's rights and how individual may exercise these rights
  - Entity's legal duties with respect to the information, including statement that entity is required by law to maintain privacy of PHI
  - Whom individuals can contact for further information about entity's privacy policies
  - An effective date

- Revisions
  - Must promptly revise and distribute Notice whenever a material change is made to its privacy practices

PROVIDERS

- All providers
  - On request
  - If maintain a website, must be posted there
- Providers with direct treatment relationship
  - By date of first service delivery
  - If have physical service delivery site:
    - Have available at site for individuals to request to take with them
    - Post Notice in clear and prominent location
  - If emergency - as soon as reasonably practicable after emergency
- Must make good faith effort to obtain written acknowledgment of receipt of Notice

HEALTH PLANS

- To new enrollees at time of enrollment
- At least every 3 years - must notify individuals then covered of availability of Notice and how to obtain a copy
NOTICE – MISCELLANEOUS

- Material revisions to Notice require:
  - Providers
    - Revise Notice & remove all copies of old Notice; replace with new Notice
    - Provide new Notice to individuals upon request or at first treatment opportunity
  - Health plans
    - Post revised Notice on website by effective date
    - If no website, must send out to all members covered by plan within 60 days of revision (or send information on how to obtain copy)
- Electronic Notice
  - Allowed if individual agrees to receive it in this manner
- Joint Notice of Privacy Practices
  - If part of an Organized Health Care Organization (OHCA) you may have one of these
  - Further requirements on content

MARKETING

- Definition:
  - To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service...
- Includes other important definitions:
  - Financial remuneration
  - Direct payment
  - Indirect payment
- 3 Pronged-test; must meet all 3 to be marketing:
  1. Is it a communication that encourages an individual to purchase or use a third party’s product or service?
  2. Do you receive payment (financial remuneration) from the 3rd party for making the communication?
  3. Are you certain that an exception DOES NOT APPLY?

MARKETING

Five (5) Exceptions:

1. Communication promotes health in general – i.e., encouraging annual mammograms
2. Communication is face-to-face - health care operations or treatment (“or other marketing communication”)
3. The communication is a promotional gift of nominal value provided by the CE
4. The communication is related to refill reminders about a drug that is currently prescribed and any payment is reasonably related to the cost of making the communication
5. Is about government and government-sponsored programs (as there is no commercial component to these communications)
MARKETING, CONT.

> Financial remuneration – direct or indirect payment from or on behalf of a third party whose product or service is being described

> Does not include any direct or indirect payment for the treatment of an individual!

> Does not include non-financial benefits, such as in-kind benefits, provided to CE in exchange for making communication about product/service

> Only includes payments made in exchange for making the communication

IN ORDER TO MARKET TO INDIVIDUALS

> Must obtain valid authorization before using/disclosing PHI for marketing

> Authorization must disclose that CE is receiving financial remuneration from 3rd party

> If individual signs authorization to receive such communications, CE may send them until individual revokes it

> If individual doesn’t sign authorization, CE may not send these types of communications

MARKETING AND BUSINESS ASSOCIATES

> Remember, BAs cannot use PHI in a manner that CE couldn’t

> If BA receives financial remuneration from a 3rd party in exchange for making a communication about product/service, this would be marketing and require authorization!
SALE OF PHI

Definition:
+ "a disclosure of PHI by a CE where the CE directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI"

Note: any remuneration, not just "financial"

Exceptions:
+ Treatment and Payment
+ Public health purposes
+ Transfer, merger or consolidation of CE & related due diligence
+ Required by Law
+ To Business Associates for their contracted activities

Exceptions with RESTRICTIONS:
+ Research
+ To the individual
+ Reasonable cost-based remuneration to cover cost to prepare and transmit PHI

MARKETING VS. SALE

MARKETING
- For a written communication
- Financial remuneration (payment)
- Applies to a "use or disclosure"
- Requires valid authorization stating that CE is receiving payment for making communication
- Exceptions exist

SALE OF PHI
- For anything regarding PHI
- Any remuneration
- Applies to a "disclosure"
- Requires valid authorization stating CE will receive remuneration from sale of PHI
- Exceptions exist

IN ORDER TO ‘SELL’ AN INDIVIDUAL’S PHI

+ Must obtain an individual’s authorization before CE may disclose PHI in exchange for remuneration
  - even if disclosure is for an otherwise permitted disclosure under the Privacy Rule
+ Notice of Privacy Practices must mention the prohibition on sale of PHI without the express written authorization of the individual
FUND RAISING

- May use or disclose to BA or institutionally related foundation:
  1. Demographic information relating to individual (name, address, other contact information, age, gender, date of birth)
  2. Dates of health care provided
  3. Department of service information*
  4. Treating physician*
  5. Outcome information*
  6. Health insurance status*

- ...for the purpose of raising funds for its own benefit, without an authorization

Requirements:
- Include statement in Notice of Privacy Practices
- Provide individual with clear & conspicuous opportunity to opt out of further fundraising communications with each communication
- Method may not cause individual undue burden or more than nominal cost
- May not condition treatment or payment on individual’s choice
- May not make fundraising communications to an individual who has opted out

GENETIC INFORMATION NON-DISCRIMINATION ACT OF 2008

- GINA required Secretary of HHS to revise Privacy Rule
- Genetic information is health information
- HIPAA prohibits all health plans that are CEs under HIPAA from using or disclosing PHI that is genetic information for underwriting purposes
  - Excepts: long-term care plans from underwriting prohibition
- Note: an authorization CANNOT be used to permit a use or disclosure of genetic information for underwriting purposes!
  - Not like “sale” of PHI

RESEARCH

- Defined: a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge

Can be considered “sale of PHI” if remuneration received by the CE or BA exceeds a reasonable cost-based fee to cover cost to prepare & transmit the PHI
**RESEARCH**

- Requires:
  - Written authorization from the individual
  - Waiver of authorization from an IRB or Privacy Board
  - Only sharing of a LDS of data with DUA (for research, public health or health care operations only)

- Authorizations
  - Can be compound
    - Example: combining an authorization for the use or disclosure of PHI for a research study with an authorization for the creation or maintenance of a research database
  - Conditioned and non-conditioned activities can be combined on same form
    - Must clearly differentiate between the conditioned and unconditioned components and provide individual with opportunity to opt in to the research activities described in unconditioned authorization
    - Gets tricky; consult the regulations or an expert in this area

**RESEARCH - LIMITED DATA SET**

- LDS excludes following identifiers
  - Names
  - Postal address information, other than town or city, State, and zip code
  - Telephone numbers
  - Fax numbers
  - Electronic mail addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - Web Universal Resource Locators (URLs)
  - Internet Protocol (IP) address numbers
  - Biometric identifiers, including finger and voice prints
  - Full face photographic images and any comparable images

- A CE may exchange a LDS of PHI for the purposes of research, public health or health care operations if they enter into a Data Use Agreement (DUA) with the recipient

- The DUA ensures that the recipient of a LDS will only use or disclose the PHI for limited purposes

- The DUA must contain certain required elements

**DE-IDENTIFIED DATA**

- Health information can be de-identified by removing anything that identifies the individual

- De-identified data is not subject to HIPAA law

- Two Methods:
  1. “Safe Harbor” approach
    - Permits a CE to consider data to be de-identified if it removes 18 types of identifiers (e.g., names, dates, and geocodes on populations with less than 20,000 inhabitants) and has no actual knowledge that remaining information could be used to identify an individual, either alone or in combination with other information.
  2. Statistical approach
    - Permits covered entities to disclose health information in any form provided that a qualified statistical or scientific expert concludes, through the use of accepted analytic techniques, that the risk the information could be used alone, or in combination with other reasonably available information, to identify the subject is very small

[Link to HIPAA de-identification guidance page]
PATIENTS’ RIGHTS UNDER HIPAA

- The right to access, copy, and inspect their health-care information
- The right to request an amendment to their healthcare information
- The right to obtain an accounting of certain disclosures of their health-care information
- Rights to request privacy protection for protected health information
  + Includes absolute Right to restrict information from insurer if individual pays for item/service out-of-pocket & in full
- The right to complain about alleged violations of the regulations and the entity’s own information policies
- The right to be notified when a breach of their unsecured PHI occurs

PATIENTS’ RIGHTS VIDEO FROM OCR

TRAINING

- Must train:
  + All workforce members on policies and procedures regarding PHI safeguards in order for them to carry out their duties
  + Each new workforce member within a reasonable period of time after he/she joins the entity
  + Each workforce member whose functions are affected by material change in policies or procedures – within a reasonable period of time after the material change
SANCTIONS

* Required that you have them and apply them to workforce members who violate your policies and procedures

* Must train workforce to understand sanctions may apply

* Must document sanctions taken

* One of the first things you may be asked for in an audit!

POLICIES AND PROCEDURES “MUSTS”

* Implement policies and procedures to comply with standards, implementation specifications, or other requirements

* Be reasonably designed to ensure compliance

* Change as necessary and appropriate to comply with changes in the law

* Document it all

WHAT IS A BREACH?

* “The unauthorized acquisition, access, use or disclosure of PHI...which compromises the security or privacy of the PHI.”
  + ie when we lose information, it is stolen from us, etc.

* HITECH requires us to tell:
  + The client(s)
  + The federal government
  + The media (sometimes)
    + >500 clients’ data = immediate notification to the feds and notification to prominent media outlets

>500 clients’ data = immediate notification to the feds and notification to prominent media outlets
NOT A BREACH IF:

- Electronic PHI is encrypted (per federal standards)
- Paper PHI is shredded so that it cannot be read or otherwise reconstructed

THE BASICS OF BREACH REPORTING

- Are you dealing with PHI as defined in HIPAA?
- Is there a Violation of the Privacy Rule?
- Does an exception apply?

#1 #2 #3

RISK ASSESSMENT OPTION

- Presumption is that an acquisition, access, use, or disclosure of PHI in a manner not otherwise permitted is a reportable breach unless...
- CE or BA must demonstrate that there is a low probability that the PHI has been compromised based on an assessment of at least 4 factors in order to NOT notify

Note: you do not have to do a risk assessment if you are going to report the breach as per the regulations!
RISK ASSESSMENT - 4 FACTORS

- **TYPE?**
  - The nature and extent of the PHI involved
  - Consider types of identifiers and likelihood of re-identification

- **WHO?**
  - The unauthorized person who used the PHI or to whom the disclosure was made

- **HOW OR HOW MUCH?**
  - Whether the PHI was actually acquired or viewed

- **MITIGATION!**
  - The extent to which the risk to the PHI has been mitigated

MITIGATION

- Covered entities have a duty to mitigate harmful effects due to uses or disclosures of PHI

- It is only possible to mitigate what is known!

- As a Privacy Officer, you must train your workforce members and business associates on the importance of detecting and reporting incidents, breaches and violations of HIPAA to the CE (or upline BA) as soon as possible

FEDERAL BREACH WEBSITE (>500)
Electronic systems and devices which create, receive, maintain or transmit information about a person’s health records must be protected.

SECURITY RULE OVERVIEW

- Intended to be:
  - Technology neutral
  - Scalable
  - Protect the confidentiality, integrity and availability of electronic PHI (E PHI)
  - Protect E PHI against any reasonably anticipated threats, hazards, improper uses or disclosures

- Confidentiality – ensuring that only those individuals who are supposed to access E PHI do
- Integrity – ensuring that the E PHI input today is the E PHI that is retrieved tomorrow, next week, next year, etc.
- Availability – ensuring that E PHI is available to those who need it when they need it

WHEN DECIDING ON SECURITY MEASURES, YOU NEED TO CONSIDER:

- Your size, complexity, and capabilities
- Technical infrastructure, hardware, and software security capabilities
- Costs of security measures (not your security budget)
- Probability and criticality of potential risks to E PHI
**SECURITY RULE CONT.**

- Structure of Rule
  - Standards:
    - CE or BA must comply with Standards
  - Implementation specifications

- Required
  - You must implement it

- Addressable:
  - You must
    - Assess if it is a reasonable and appropriate safeguard in your environment
    - Implement it if it is
  - If it isn’t - you must document why it isn’t AND implement an equivalent alternative measure if reasonable and appropriate

---

**STANDARDS - ADMINISTRATIVE**

- Security management process
  - Risk analysis
  - Risk management
  - Sanction policy
  - Information system activity review

- Assigned security responsibility

- Workforce security
  - Authorization and/or supervision
  - Workforce clearance procedure
  - Termination procedures

- Information access management
  - Isolating health care clearinghouse functions
  - Access establishment and modification

- Security awareness and training
  - Security reminders
  - Protection from malicious software
  - Log-in monitoring
  - Password management

- Security incident procedures
  - Response and reporting

- Contingency plan
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
  - Testing and revision procedures
  - Applications and data criticality assessment

- Evaluation

- Business associate contracts and other arrangements
  - Written contract or other arrangement

---

**STANDARDS - PHYSICAL**

- Facility Access Controls
  - Contingency operations
  - Facility security plan
  - Access control and validation procedures
  - Maintenance records

- Workstation Use

- Workstation Security

- Device and Media Controls
  - Disposal
  - Media re-use
  - Accountability
  - Data backup and storage
## STANDARDS - TECHNICAL

- **Access Control**
  - Unique user identification
  - Emergency access procedure
  - Automatic logout
  - Encryption and decryption
- **Audit Controls**
- **Integrity**
  - Mechanism to authenticate EPHI
- **Person or Entity Authentication**
- **Transmission Security**
  - Integrity controls
  - Encryption

## MISCELLANEOUS

- **Policies and Procedures**
  - Implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications and other requirements
  - Documentation Requirements
    - Maintain P&P in written form
    - Maintain written documentation of any required action, activity or assessment
    - Make certain that workforce members who have responsibility for implementing security have access to P&P, etc.
    - Review periodically
    - Update in response to environmental or operational changes that affect security of EPHI

  **Keep it all for 6 years from date of creation or date last in effect (whichever is later)**

## WATCH OUT:

- **Maintenance is required!**
- **Training is required!**
- **You must review and modify security measures, as needed, to continue provision of reasonable and appropriate protection of EPHI**
- **How else are you going to: “ensure compliance with this subpart [Security Rule] by its [your] workforce”**
SECURITY OF INFORMATION

- Threats are active, evolving, continuously moving target
- Control by implementing reasonable and appropriate security measures
  - Identify these through your risk analysis and risk management processes

THREAT
- Anything that can have a negative impact on EPHI
  - Intentional (e.g., malicious intent)
  - Unintentional (e.g., misconfigured server, data entry error)
- Sources:
  - Natural (e.g., floods, earthquakes, storms, tornados)
  - Human (e.g., intentional such as identity thieves, hackers, spyware authors; unintentional such as data entry errors, accidental deletions)
  - Environmental (e.g., power surges and spikes, hazardous contamination, environmental pollution)

VULNERABILITY
- A flaw or weakness in a system security procedure, design, implementation, or control that could be intentionally or unintentionally exercised by a threat

KEY SECURITY DEFINITIONS

THE DIFFERENCE BETWEEN THE TWO...

- An organization may be vulnerable to damage from power spikes
- Threats that could exploit this vulnerability may be overloaded circuits, faulty building wiring, dirty street power, or too much load on the local grid

Security controls could range from installing UPS systems, additional fuse boxes, or standby generators, or rewiring the office

These additional security controls may help to mitigate the vulnerability but not necessarily for each threat
**RISK**

The potential impact that a threat can have on the confidentiality, integrity, and availability of EPHI by exploiting a vulnerability

- Risk Analysis
- Risk Management

164.308(a)(ii)(A)  164.308(a)(ii)(B)

**SECURITY POLICIES AND PROCEDURES**

- Categories, Ideas, Suggestions, Templates, etc...

**ACCESS TO SYSTEMS CONTAINING PHI**

- New Workforce User Access Request
  - How is access requested? What forms are used?
  - What safeguards are put in place to ensure minimum necessary access?
- Acceptable Use Agreement
  - Have one and make sure workforce members sign it and you maintain this documentation!
  - Best policy - no access to electronic systems until signed and trained in it
- Workforce User Modification/Termination
  - How do you do this in your organization to ensure access is terminated ASAP when an employee leaves?
  - What about hostile terminations?
  - How do you ensure when an individual changes roles within your organization that their system access is reevaluated to ensure compliance with minimum necessary?
BUSINESS ASSOCIATE MANAGEMENT

- Make sure your business associates sign business associate agreements
- Maintain documentation of this
- Make sure your BAs enter into similar agreements with any subcontractor who touches your PHI
  - Must be at least as strict as the BAA between the CE and BA

PASSWORD MANAGEMENT

- At least 8 characters
  - (16 recommended)
  - Require:
    - Upper case
    - Lower case
    - Numbers
    - Symbols
- Examples of complex passwords:
  - RockiesS!@#
  - NeverBeenRuckedEnough:)
  - NewStarWarsMay19!
  - "Francisco,that'sfuntooay"
- Never, ever, ever share your password

WORKSTATION USE

- Automatically employed safeguards
  - Automatic screensaver after 15 minutes
  - No administrative rights except for specific, authorized individuals
  - Easy notification system for user issues
  - User acceptance of understanding of appropriate workstation policies upon log-in each time
  - Security banners
- Employee responsible safeguards
  - Minimize PHI when possible
  - No use of workstation another user has logged onto, no use of another user's ID/password
  - Lock computer when leaving for any period of time
  - Log off at conclusion of each day
  - Save PHI to network drives if necessary and only for as long as necessary
EMAILING

- Confirm address before sending
- Confidentiality clause attached to all externally sent emails
- **BE VERY CAREFUL WITH SOCIAL SECURITY NUMBERS**
- Email to many individuals at once – use “BCC”
- Limit amount of information to minimum necessary
- When sending externally – **ENCRYPT!**

VISITOR POLICY

- All Visitors must sign a Visitor log & receive a badge
- Visitors should be monitored while in your facility
- Employees should be trained and reminded to question identity and authority of unauthorized person in work area

MOBILE DEVICES

- Only use organization-approved and **ENCRYPTED** devices
- All devices will have remote-wipe capabilities
- You must notify your security officer immediately if a device is lost or stolen!
SYSTEM INTEGRITY

- Safeguards such as firewalls, anti-virus, anti-malware, etc. will be employed and routinely checked to ensure effectiveness
- System patches will be implemented ASAP
- A consultant will be hired annually to pen test the organization’s systems
- Security awareness for workforce members
  - Everyone needs to be aware!
  - Must have high alert for malicious emails or spam
  - Must be trained to contact IT support immediately if they suspect something is amiss with their workstations

ENCRYPTION OF WORKSTATIONS, LAPTOPS, EMAIL, ETC.

- Best practice – everything containing PHI must be encrypted if it leaves your facility
  + Emails
  + Information on CD ROMs
  + Laptops
  + Thumb drives
- Paper PHI still an issue
  + Must safeguard appropriately when transferring out of organization for site visits, etc.
  + Electronic PHI is preferred as can be protected through encryption

A PAIR OF UNENCRYPTED MALE THUMB DRIVES....
DESTRUCTION AND DISPOSAL OF ELECTRONIC PHI

- If you’re shredding paper PHI, make sure you’re using a cross-cut shredder!
- Media containing PHI that can’t be placed in shredder should be given to IT Support for appropriate destruction
- Semi-annual ‘shredding day’ at your organization!

WHAT YOU SHOULD BE WORRIED ABOUT

1. Your data – where is it?
2. Any data that can move that isn’t encrypted
3. Vendors - what are they doing with your data?
4. Buy in from the top
   + Are you telling the C-Suite & Board when major incidents happen? Do they care?
5. State laws that allow people to sue for HIPAA violations

WHAT YOU SHOULD BE WORRIED ABOUT, CONT.

6. Your “Designated Record Set” and where it exists
7. HIEs/Connectivity
8. Your Workforce
   + Intentional and unintentional acts
9. Minimum Necessary
10. Forgetting about the Patient in all of this.
BUT REMEMBER...

- Privacy and security compliance is a journey, not a destination
  - Privacy regulations changing constantly
  - Security “best practices” evolving exponentially with technology
  - Nobody has enough resources

It’s not possible to be 100% compliant – but you do need to always keep working toward that goal!

RESOURCES

- Federal Register for the Final Omnibus Rule
  - [https://www.federalregister.gov/](https://www.federalregister.gov/)
- Office for Civil Rights
  - [www.hhs.gov/ocr/](http://www.hhs.gov/ocr/)
- Office of National Coordinator
  - [www.healthit.gov](http://www.healthit.gov)
- For policies and procedures
  - The Privacy / Data Protection Project website of the University of Miami School of Medicine
  - [http://privacy.med.miami.edu/index.htm](http://privacy.med.miami.edu/index.htm)

Erika M. Bol
State of Colorado’s Department of Health Care Policy & Financing
Erika.bol@state.co.us

THE END
NIST HIPAA SECURITY RULE TOOLKIT

- http://scap.nist.gov/hipaa/ (desktop-based application)
- Goal: help organizations better understand, implement and assess requirements of HIPAA Security Rule,
- Target users: HIPAA covered entities, business associates, other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services
- Addresses the 45 implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues