

August 22, 1996 – President Clinton's signs the Health Insurance Portability and Accountability Act

Limits preexisting condition exclusions and for the first time makes the regulation of private health insurance a federal responsibility

Health Information Technology for Clinical Health Act (HITECH)

Kassebaum-Kennedy Bill

Amended by the American Recovery & Reinvestment Act of 2009 Final Omnibus Rule 9/23/2013

HIPAA PRIVACY & SECURITY 101

TODAY'S SESSION

- ✦ A Little Background and Context....
- ✦ Enforcement Overview
- ✦ The Privacy Rule
- ✦ Breach Notification Requirements
- ✦ The Security Rule
- ✦ Resources

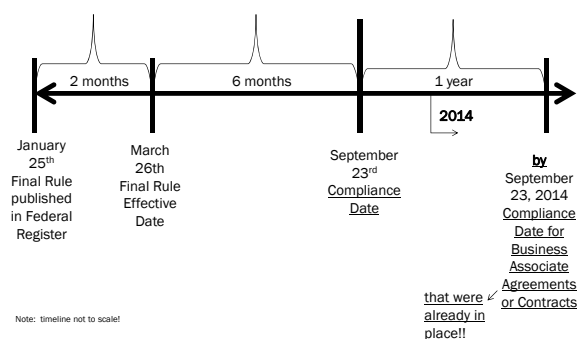
DISCLAIMER

The information provided in this presentation is intended for educational purposes only, does not constitute legal advice, and does not represent the official opinion of any individual, department, division or territory of the State of Colorado.

HOUSEKEEPING NOTES:

- ✖ This presentation incorporates changes to HIPAA from:
 - + Omnibus Rule – effective date of 9/23/2013
 - + CLIA update to HIPAA– effective date of 4/7/2014; compliance date of 10/6/2014 for CE labs
- ✖ Due to volume of information, please hold questions until the end!
- ✖ We will take a break at approximately 10:20am; please feel free to get up as needed. This is a LONG session.

WHERE WE ARE TODAY WITH THE FINAL RULE



STILL TO COME FROM ARRA/HITECH

- | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> ✖ Rulemaking: <ul style="list-style-type: none"> + Accounting of Disclosures Rule + Method for sharing Penalty Amounts With Harmed Individuals | <ul style="list-style-type: none"> ✖ Guidance <ul style="list-style-type: none"> + Breach Safe Harbor Update + Breach Risk Assessment Tool + Minimum Necessary + More on Marketing + More Factsheets on other provisions + Permitted Mental Health Disclosures + Security Rule Guidance Updates |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

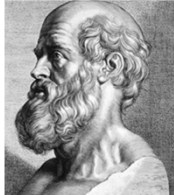
- Susan McAndrew, J.D. Deputy Director Health Information Privacy Division, HHS/OCR; 22nd National HIPAA Summit, February 5, 2014

A LITTLE BACKGROUND

The Hippocratic Oath:

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."

- 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

Sector-specific model for protecting personal data

Developed from attitude that allows business to police itself as a matter of its own self-interest - *"laissez-faire"*

Evolved over time into myriad of protection laws, often overlapping regulations, multitude of compliance regulations



FEDERAL	STATE
<ul style="list-style-type: none"> ✗ 42 CFR Part 2 (Part 2) ✗ 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) 	<ul style="list-style-type: none"> ✗ Security Breach Notification Laws ✗ Minors' Rights ✗ Sensitive health conditions <ul style="list-style-type: none"> + Mental health + Aids/HIV status + Psychiatric treatment ✗ Specific to certain entities <ul style="list-style-type: none"> + Regulates licensed providers + Insurance-specific regulations (DOI)

SECTOR SPECIFIC U.S. LAWS DEALING WITH PRIVACY

PRIVACY PROTECTIONS IN THE UNITED STATES

<ul style="list-style-type: none"> ✗ Fair Information Practices Approach <ul style="list-style-type: none"> ✗ Process-oriented ✗ Major concepts: Individual Participation, <u>Notice</u>, <u>Choice</u>, Security ✗ Example: Gramm-Leach-Bliley Act (GLBA) 	<ul style="list-style-type: none"> ✗ "Permissible Purpose" Approach <ul style="list-style-type: none"> + <u>Limits data use to purposes permitted under law</u> + Example: Fair Credit Reporting Act (FCRA)
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Newer Approach:
Combine the above to have elements of each!
Example: HIPAA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA"),

- ✗ Pub. L. No. 104-191, 110 Stat. 1936 (1996)
- ✗ First federal law addressing all types of healthcare information

```

graph TD
    HIPAA[HIPAA  
Health Insurance Portability and Accountability Act of 1996]
    TitleI[Title I  
Insurance Portability]
    TitleII[Title II  
Fraud and Abuse  
Medical Liability Reform]
    TitleIII[Title III  
Tax Related  
Health Provision]
    TitleIV[Title IV  
Group Health  
Plan Requirements]
    TitleV[Title V  
Revenue  
Offsets]
    
    HIPAA --> TitleI
    HIPAA --> TitleII
    HIPAA --> TitleIII
    HIPAA --> TitleIV
    HIPAA --> TitleV
    
    TitleII --> Privacy
    TitleII --> Security
    TitleII --> EDI
    
    Privacy --> Transactions
    Security --> Transactions
    Security --> CodeSets[Code Sets]
    Security --> Identifiers
    EDI --> Transactions
    EDI --> CodeSets
    EDI --> Identifiers
  
```

TWO OBJECTIVES OF HIPAA

✕ Portability

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



✕ Accountability

- + Combat fraud & abuse
- + Ensure Security and Confidentiality of individuals' information/data
- + Mandate uniform standards for electronic data transmission of patient health information

HIPAA'S ADMINISTRATIVE SIMPLIFICATION

✕ HIPAA of 1996

- + Designed to improve efficiency and effectiveness of health care system by **promoting electronic exchange** of health information
- + Established national, uniform baseline of **privacy and security protections** for individuals' health information



✕ HITECH Act (part of American Recovery and Reinvestment Act of 2009)

- + Strengthened and expanded HIPAA protections
- + Accelerated adoption of electronic health records (EHRs) among providers
- + Supported efforts to rapidly build capacity for exchanging health information

HIPAA ADMINISTRATIVE SIMPLIFICATION



PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

- Preemption (state law), Compliance, Investigations, Enforcement, Civil Money Penalties (CMPs)



PART 162—ADMINISTRATIVE REQUIREMENTS

- Standard Unique Identifiers (health plans, providers, employers), Transactions & Code Sets

PART 164—SECURITY AND PRIVACY

- Security, Breach Notification, Privacy including Patient Rights



PART 160 GENERAL ADMINISTRATIVE 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 162 ADMINISTRATIVE REQUIREMENTS

Subpart A	General Provisions
Subpart B-C	Reserved
Subpart D	Standard Unique Health Identifier for Health Care Providers
Subpart E	Standard Unique Health Identifier for Health Plans
Subpart F	Standard Unique Employer Identifier
Subpart G-H	Reserved
Subpart I	General Provisions for Transactions
Subpart J	Code Sets
Subpart K	Health Care Claims or Equivalent Encounter Information
Subpart L	Eligibility for a Health Plan
Subpart M	Referral Certification & Authorization
Subpart N	Health Care Claim Status
Subpart O	Enrollment & Disenrollment in a Health Plan
Subpart P	Health Care Electronic Funds (EFT) & Remittance Advice
Subpart Q	Health Plan Premium Payments
Subpart R	Coordination of Benefits
Subpart S	Medicaid Pharmacy Subrogation

NOT PART OF TODAY'S CONVERSATION!

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	Notification in the Case of Breach of Unsecured Protected Health Information
Subpart E	Privacy of Individually Identifiable Health Information

REGULATION TEXT

× Unofficial Version, as amended through March 26, 2013

+ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>

+ Does not include recent CLIA update to HIPAA Covered Entity-laboratories dealing with Patient Access to Records



ENFORCEMENT OF HIPAA



HIPAA ENFORCEMENT



Source: <http://www.hhs.gov/about/regionmap.html>

21

HIPAA ENFORCEMENT

× Civil Actions

+ By:

- × Office for Civil Rights (OCR) of Dept. of Health and Human Services (HHS)
- × State Attorney's General

+ Types:

- × Civil Money Penalties
 - ★ Settlements
 - ★ Resolution Agreements w/Corrective Action Plan



× Criminal Actions

- + Referred by OCR to U.S. Department Of Justice (DOJ)
 - × Against organizations subject to HIPAA
 - × Against individuals

Since April 2003 –
OCR has referred 495
cases of potential
criminal violations to
DOJ

CIVIL ENFORCEMENT OF HIPAA – CES & BAS

- × Secretary *will* impose a civil money penalty (CMP) for violation of Administrative Simplification Provision
- × Secretary *must* consider mitigating or aggravating factors
- × Given discretion to not impose CMP if violation is corrected and is NOT due to willful neglect

Violations occurring
prior to September 18,
2009: lower penalty
structure

Violations occurring on
or after 9/18/2009:
higher penalty structure
(due to ARRA/HITECH)



CIVIL ENFORCEMENT OF HIPAA – KEY TERMS

- × **Reasonable diligence** - the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances
- × **Reasonable cause** - an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect
- × **Willful neglect** - conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

CURRENT CIVIL MONEY PENALTY STRUCTURE

Violation Category	Each violation	All such violations of identical provision in Calendar Year
Did Not Know/Would Not Have Known	\$100 - \$50,000	\$1.5M
Due to Reasonable Cause	\$1000 - \$50,000	\$1.5M
Willful Neglect – Corrected	\$10,000 - \$50,000	\$1.5M
Willful Neglect – Not Corrected	\$50,000	\$1.5M

CIVIL ENFORCEMENT OF HIPAA

Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013 (\$150,000 and CAP)

Lesson: have policies and procedures in place to address breach notification provisions of HITECH Act

HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013 (\$1,215,780 and CAP)

Lesson: assess and identify potential security risks and vulnerabilities of EPHI stored in photocopier hard drives – i.e. include all electronic PHI in your security risk assessment

WellPoint Settles HIPAA Security Case for \$1.700.000 - July 11, 2013 (\$1.7M and CAP)

Lesson: ensure your web-based applications/databases are secured from unauthorized access

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CIVIL ENFORCEMENT OF HIPAA

Shasta Regional Medical Center Settles HIPAA Privacy Case for \$275,000 - June 13, 2013 (\$275,000)

Lesson: don't disclose PHI to multiple media outlets without a valid written authorization regardless of what an individual has disclosed about him/herself

Idaho State University Settles HIPAA Security Case for \$400,000 - May 21, 2013 (\$400,000 and CAP)

Lesson: don't disable firewall protections on servers without a really good reason – and perform a security risk assessment!

HHS announces first HIPAA breach settlement involving less than 500 patients - December 31, 2012 (\$50,000 and CAP)

Lesson: encrypt laptops – i.e. have policies or procedures in place to address mobile device security as required by the Security Rule

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CIVIL ENFORCEMENT OF HIPAA



Massachusetts Provider Settles HIPAA Case for \$1.5 Million – September 17, 2012 (\$1.5M and 3-year CAP)

Lesson: conduct a thorough analysis of the risk to confidentiality of ePHI maintained on portable devices and restrict access to ePHI to authorized users of portable devices

Alaska DHSS Settles HIPAA Security Case for \$1,700,000 – June 26, 2012 (\$1.7M and CAP)

Lesson: complete a risk analysis, implement risk management measures, complete security training for workforce members, implement device and media controls, addressed device and media encryption

HHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards – April 13, 2012 (\$100,000 and CAP)

Lesson: Secure cloud-based software that hosts PHI; take reasonable steps to be in compliance with the Privacy and Security Rules

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CIVIL ENFORCEMENT OF HIPAA



HHS settles HIPAA case with BCBST for \$1.5 million – March 13, 2012 (\$1.5M and CAP)

+ *Lesson:* implement appropriate administrative safeguards to adequately protect PHI and review this when things change in your environment (evaluation standard). Ensure adequate physical safeguards.

Resolution Agreement with the University of California at Los Angeles Health System – July 6, 2011

+ *Lesson:* ensure your employees know what 'snooping' is and why they shouldn't do it; enforce sanctions when they do.

Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc. – February 14, 2011

+ *Lesson:* Ensure appropriate safeguards and controls are in place with respect to employees removing and transporting PHI offsite (paper PHI counts)

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CIVIL ENFORCEMENT OF HIPAA



Civil Money Penalty issued to Cignet Health of Prince George's County, MD – February 4, 2011

Lesson: provide Individuals with ACCESS to their records, as required by HIPAA; COOPERATE with HHS when they are investigating you for HIPAA compliance!

Rodriguez: "one of our most important cases"; "blatant disregard of the [right of an individual to obtain a copy of his or her health information] by a Covered Entity"

Resolution Agreement with Management Services Organization Washington, Inc. – December 13, 2010 (\$35,000 and 2-year CAP; OIG & DOJ involved; potential False Claims Act violations)

Lesson: don't market using PHI (MSO disclosed PHI to Washington Practice Management, LLC, owned by MSO, which used the information for marketing purposes)

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CIVIL ENFORCEMENT OF HIPAA



Resolution Agreement with Rite Aid Corporation--July 27, 2010 (\$1M and CAP and FTC consent order for 20 years)

Lesson: don't dispose of PHI in unsecured dumpsters

Resolution Agreement with CVS Pharmacy, Inc.--January 16, 2009 (\$2.25M and CAP and FTC consent order for 20 years)

Lesson: don't dispose of PHI in unsecured dumpsters

Resolution Agreement with Providence Health & Services--July 16, 2008

Lesson: Ensure appropriate safeguards and controls in place with respect to employees removing and transporting PHI offsite

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

CRIMINAL ENFORCEMENT OF INDIVIDUALS

- × *"Knowingly"* obtain or disclose PHI
 - + up to \$50K fine;
 - + imprisonment up to 1 year

- × Commit offense *under false pretense*
 - + up to \$100K fine
 - + Imprisonment up to 5 years



- × 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

CRIMINAL ENFORCEMENT

- × Codified at 42 U.S.C. § 1320d-6
- × DOJ's three general categories of HIPAA privacy violations that warrant criminal enforcement:
 1. Cases where medical records and identities are stolen to commit massive health care frauds
 2. Cases where medical records are stolen for the purpose of embarrassing or threatening to embarrass a particular patient or health care entity
 3. Cases where criminal records are stolen to commit financial fraud against financial institutions or other businesses



STATE ATTORNEYS GENERAL (SAGS) ENFORCEMENT



× HITECH gave SAGs the authority to:

- + Bring civil actions on behalf of state residents for violations of HIPAA
- + 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)
- + Massachusetts AG - South Shore Hospital for \$750,000 (May 2012)
- + Minnesota Attorney General against business associate Accretive Health, Inc. (July 2012)

<http://www.hhsipaasagtraining.com/> - 2011 Training for State AGs

OTHER CONCERNS:

× HIPAA has no private right of action



× **Meaning:** a private individual cannot sue a health care provider or health plan for breaching their medical privacy



However...

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 (16,000 individuals)
- × Georgia hospital - loss of unencrypted PHI of >300,000 patients; reported breach (*Bombardier v. Emory Healthcare, Inc.*, filed 6/4/2012)



THIRD PARTY LAWSUITS

Plaintiffs using HIPAA violation as a breach of duty by the health care professional in negligence cases, fiduciary duty cases, and straight forward violation of privacy cases

- ✖ **Prior court decisions** - dismissed claims by plaintiffs based on finding that *threat of future harm* not enough
 - + *Paul v. Providence Health System-Oregon*, 273 P.3d 106 (Or. 2012)
- ✖ **Watch out:**
 - + *LS v Washington Univ* (E.D. Mo 2011) - Court found "plausible injury" from breach against health plan in Florida
 - + *R. K. v St. Mary's Med Ctr*, (2012) - R. K. v St. Mary's Med Ctr, (2012) - Court found that HIPAA does not preempt state laws and may be used as basis of negligence claim (used as the standard of care to which a breach of duty is judged)

KEY DEFINITIONS UNDER PART 160

- | | |
|-------------------------------------------------------|---------------------------------------------|
| ✖ Covered entity | ✖ Organized Health Care Organization (OHCA) |
| ✖ Business associate | ✖ Protected health information |
| ✖ Electronic protected health information | ✖ Subcontractor |
| ✖ Disclosure | ✖ Use |
| ✖ Individually identifiable health information (IIHI) | ✖ Workforce |
| ✖ Genetic information | |



KEY CONCEPT – PREEMPTION OF STATE LAW

State laws **contrary** to HIPAA are preempted (trumped) by HIPAA unless:

1. Secretary determines it is necessary – example: to prevent fraud or abuse
2. State law relates to privacy of individuals and is more stringent
3. State law provides for reporting of disease, injury, child abuse, for public health surveillance, investigation, intervention, etc.

If not contrary, must comply with **both!**

PREEMPTION DEFINITIONS

Contrary = *it would be impossible to comply with both state and federal laws; state 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, increases privacy protections, provides for retention or reporting of more detailed information or for a longer duration, **provides greater privacy protection for the individual....**

RESPONSIBILITIES OF CES AND BAS

- ✕ Maintain, and provide when asked, records showing your compliance with HIPAA
- ✕ Cooperate with investigations and compliance reviews of your policies, procedures, or practices
- ✕ Permit access to your facilities, books, records, accounts, etc. to ascertain compliance



Avoid "**conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated**" – and you'll never have to worry about any other parts of the Enforcement Rule...



EVERYTHING WE LEARN AND DO FROM HERE ON IS TO HELP YOU WORK TOWARDS AN EFFECTIVE HIPAA COMPLIANCE PROGRAM

PART 164: SECURITY, BREACH NOTIFICATION AND PRIVACY RULES

PART 164 "PARTS"

SECURITY RULE

- ✕ Protects ELECTRONIC health information (EHI)
- ✕ 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

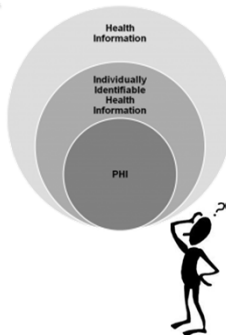
BREACH NOTIFICATION RULE

- ✕ 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 and conversations
- ✖ Fax transmissions
- ✖ CDs, thumb drives
- ✖ E-mail
- ✖ Tattoos?



INDIVIDUAL IDENTIFIERS OF PHI

- | | |
|--------------------------|---------------------------------------------------------|
| ✖ Name | ✖ Drivers' license numbers |
| ✖ Address | ✖ Vehicle ID |
| ✖ Social Security number | ✖ Pharmacy ID # |
| ✖ Family History | ✖ Personal Assets |
| ✖ Telephone number | ✖ Device identifiers and serial numbers |
| ✖ Fax number | ✖ Biometric (finger or voice print) |
| ✖ Account numbers | ✖ Photographs |
| ✖ Medical record number | ✖ Geographic indicators |
| ✖ E-mail address | ✖ Any unique identifying number, code or characteristic |
| ✖ Dates | |
| ✖ Medicaid Client ID # | |

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

HEALTH INFORMATION - PAST, PRESENT, FUTURE

- ✖ United Health Care health plan member ID# 34-457633
- ✖ Chief diagnosis: diabetes
- ✖ Member of Elderly, Blind & Disabled Waiver program
- ✖ Dx code 780.79
- ✖ Medical record #HO-934578
- ✖ Eligibility paperwork for CHP+ program

WHAT IT TAKES TO MAKE PHI



Examples:

- A list of social security numbers ONLY 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

- + And their subcontractors who handle PHI



KNOW WHO AND WHAT YOU ARE UNDER HIPAA

ARE YOU A COVERED ENTITY?

✱ Not sure?

- ✱ <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAgenInfo/Downloads/CoveredEntitycharts.pdf>

A Health Care Provider

This includes providers such as:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

A Health Plan

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

A Health Care Clearinghouse

This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

ARE YOU A BUSINESS ASSOCIATE?

- 1) Do you **create, receive, maintain, or transmit** PHI on behalf of a CE (or another BA) for a function or activity regulated by the HIPAA Rules?

...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.

WRITTEN REQUIREMENT BETWEEN CEs AND BAs AND BAs AND SUBCONTRACTOR BAs

- ✖ Must enter into an Agreement to ensure BA will appropriately and adequately safeguard PHI
- ✖ Commonly referred to as: Business Associate Agreement (BAA) or Business Associate Contract (BAC)



BAs or BACs have specific requirements under the Privacy, Security, Breach and Enforcement Rules

KEY CONCEPT: 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!

KEY CONCEPT: USE VS. DISCLOSURE

Use :

Sharing
Employing
Applying
Utilizing
Examining
Analyzing



Information is used when it moves within an organization

Disclosure :

Releasing
Transferring
Providing access to
Divulging in any manner



Information is disclosed when it is transmitted between or among organizations

KEY CONCEPT: REQUIRED DISCLOSURES

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

KEY CONCEPT: 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

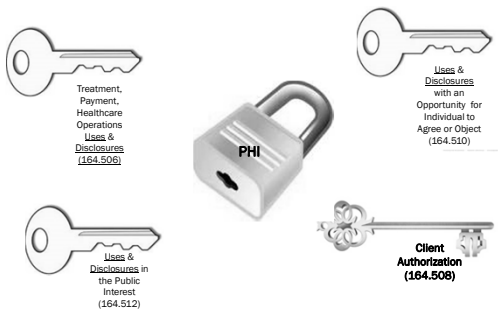


BASIC TENETS OF HIPAA

- ✕ Patients have a right to access their health information and to control where it goes (with exceptions); otherwise requires "Authorization"
- ✕ Covered entities may use patient information for certain treatment and business operations (payment, health care operations) = "TPO"
- ✕ They must tell patients how they will use the information and implement safeguards to protect it = "Notice of Privacy Practices"



HOW HIPAA WORKS...



And....incidental uses & disclosures

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 schedule for surgery



PAYMENT

Activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual

Includes eligibility verification and collections activities

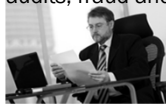
- + Example: a physician sending health information about a patient to the patient's insurance company to get paid for the services he/she provided



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
- ✖ Reporting on 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.

(Known as 164.512 exceptions)

OPPORTUNITY FOR INDIVIDUAL TO AGREE OR OBJECT



- ✖ Facility directories
- ✖ For involvement in the individual's care and notification purposes
 - + With individual is 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



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

164.502(a)(1)(iii)

AUTHORIZATIONS

All other disclosures require a valid written authorization from the individual

Form 3081 AUTHORIZATION TO DISCLOSE, RELEASE AND USE PROTECTED HEALTH INFORMATION (HIPAA COMPLIANT)
PLEASE PRINT OR TYPE

Requesting Party _____ Telephone Number _____
Address _____ Fax _____
TO _____ (Medical Provider as listed on Form 3075)

This authorization permits you to release a copy of records in your possession regarding any medical treatment and/or hospitalization of:

Name of Patient _____ Date of Birth _____
Social Security Number _____
Date(s) of Injury/Onset/Initial Disease _____

I, **AUTHORIZE** you to disclose any information and records regarding the above named individual in your possession. This includes but is not limited to: your medical history, diagnosis, treatment, treatment outcomes, prognosis, clinical notes, diagnostic reports or pathology tests, physical therapy records, pharmacy records, or any other health information in your records for the past 10 years (10 years of dates being electronically transferred based on the information released it may include information related to any substance abuse).

I **UNDERSTAND AND AGREE** that the information furnished may be used to evaluate and verify my claim for benefits for a work-related injury or occupational disease. The information released is not to be used for any other purpose (including but not limited to: your medical history, diagnosis, treatment, treatment outcomes, prognosis, clinical notes, diagnostic reports or pathology tests, physical therapy records, pharmacy records, or any other health information in your records for the past 10 years (10 years of dates being electronically transferred based on the information released it may include information related to any substance abuse)).

THIS AUTHORIZATION will expire 90 days following a resolution of the workers' compensation claim(s) that may be received by you or your estate. Revocation of this authorization will not be valid if the requesting party has taken action to enforce your authorization. Please note that the information disclosed is not subject to this authorization may be subject to re-disclosure and would, therefore, no longer be protected under the terms of this authorization.

A **PROXIMATE COPY** of this authorization shall be deemed to have the same authority as the original.

I hereby certify that I have read the provisions in this authorization. I understand and agree to its terms, and authorize disclosure of the information described above.

Print _____ Date _____
Please fax or mail back to the requesting party at the above fax/address.

Official Form 3081
State of Utah • Labor Commission • Division of Industrial Accidents
200 East 500 South • P.O. Box 16016 • Salt Lake City, UT 84116-0160 • Telephone: (801) 533-6880
Fax: (801) 533-6880 • Toll Free: (800) 545-5594 • www.laborcommission.state.ut.us

AUTHORIZATION CHECKLIST

Authorization Form Checklist		<input checked="" type="checkbox"/>
A specific description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.		
A description of the purpose of the disclosure (may state "at the request of the individual").		
The name or other specific identification of the person or class of persons authorized to make the requested use/disclosure.		
The name or other specific identification of the person or class of persons to whom the C.E. may make the requested use/disclosure.		
An expiration date or event (must relate to the individual or the purpose of the use/disclosure).		
A statement of the individual's right to revoke the authorization (normally in writing), the exceptions to the right to revoke and a description of how the individual may go about revoking the authorization.		
A statement that information used or disclosed under the authorization may be re-disclosed by the recipient and no longer protected by the Privacy Rule.		
A statement that the covered entity will not condition treatment or payment on the individual's authorization; if health plan – may not condition enrollment or eligibility on authorization.		
Signature of the individual and date.		
The authorization is conspicuous and separate from any other document, including any other written legal permission from the individual.		
If authorization is signed by a personal representative, a description of the representative's authority to act on behalf of the individual.		
If for marketing purposes, authorization must include a statement that the covered entity will be paid for the marketing activity if the marketing involves direct or indirect remuneration by a third party.		
If for fundraising purposes, authorization must include a statement that the covered entity will be paid for the fundraising activity if the fundraising involves direct or indirect remuneration by a third party.		
Note: more than one authorization may be necessary for certain purposes. For example, an authorization for the release of an individual's emergency information can't be used for marketing purposes unless it also includes a statement that the covered entity will be paid for the marketing activity if the marketing involves direct or indirect remuneration by a third party.		

WHEN HIPAA REQUIRES AN AUTHORIZATION

1. Psychotherapy Notes
 - + Definition matters; Exceptions exist
 2. Marketing
 - + Definition matters; Exceptions exist
 3. Sale of PHI
 - + Definition of "sale" key
- ✗ **Note:**
AUTHORIZATIONS MUST BE VALID!
- ✗ **Restrictions**
around
combining for
different
purposes

PSYCHOTHERAPY NOTES

- ✱ Specific definition – know it if you think you deal with these notes
- ✱ Almost always require special Authorization to release
 - + Note: Authorization may not be combined with any other Authorization



Right of access to these notes by the individual (patient) is NOT REQUIRED by HIPAA

HIPAA does NOT restrict disclosure of these notes to individuals/patients

CE has discretion as to whether to disclose to individual upon request or withhold

MARKETING

...to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service



- ✱ Must be a communication (written or verbal)
- ✱ Must involve PHI

REQUIRES WRITTEN AUTHORIZATION

✱ Unless

1. Face-to-face for health care operations, treatment, "or other marketing communication"

Even if you get paid for these!

2. Promotional gift of nominal value provided by the CE



- ✱ If marketing involves financial remuneration to CE from a 3rd party, the Authorization must state this!

STATUTORY EXCEPTION WITHIN DEFINITION**✖ ARRA HITECH exception (2009):**

+ *Communication made to provide refill reminders or communicate about a drug or biologic currently being prescribed to patient, IF any financial remuneration received by CE in exchange for making the communication is reasonably related to the CE's cost of making the communication*



★ *reasonable = they are reasonably related to the CE's cost of making the communications, such as postage*

OTHER EXCEPTIONS WITHIN DEFINITION**✖ If CE does NOT receive financial remuneration in exchange for making the communication:**

1. *Treatment by health care provider*
2. *To describe health-related product or service (or payment for) provided by or included in plan of benefits of CE making communication*
3. *For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions (not treatment)*



SO: If CE does receive financial remuneration in exchange for making communication – requires Authorization

FINANCIAL REMUNERATION**✖ Direct or indirect payment from or on behalf of a 3rd party whose product/service is being described**

- + Doesn't include any payment for treatment
- + Non-financial remuneration (pizza, donuts, tickets) doesn't count
- + If financial remuneration received by CE is for any purpose other than for making the communication, marketing doesn't apply



MARKETING – YES OR NO?

1. A national laboratory pays a hospital \$110,000 to send a letter to every address in its 7-county service area
2. A non-profit foundation pays for a physician group to send a letter to all of its patients encouraging them to eat healthy, exercise and get their annual physical exams
3. A state Medicaid agency sends a mailing about expanded eligibility benefits to all current Medicaid clients
4. A breast cancer foundation funds a hospital's mailing to patients to encourage the use of new mammography screening equipment developed by Siemens AG.



MARKETING – YES OR NO?

5. A woman living in Orland receives a letter from a drug company promoting a treatment for her high cholesterol a few weeks after visiting with her doctor
6. A consumer products company pays a national hospital chain to send a flyer, including a coupon, to a list of names and addresses of elderly incontinent women
7. A Utah-based pharmaceutical benefits management firm uses patient data it received after taking a hospital CEO to the Super Bowl to solicit business for its owner, a drug store
8. A speculator bids \$4000 for patient records of a family practice in South Carolina; among other uses or records, businessman hopes to sell purchased records back to the former patients



MARKETING FINAL REMINDERS

- + Must obtain valid Authorization before using/disclosing PHI for marketing
- + If individual signs Authorization to receive communications, CE may send them until individual revokes it. If individual doesn't sign Authorization, CE may not send these types of communications
- + If BA receives financial remuneration from a 3rd party in exchange for making communication about product/service, this still counts as marketing
- + Caution: state laws may be more strict than HIPAA when dealing with marketing
(e.g. California's Confidentiality of Medical Information Act)



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



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



MARKETING

- × For a communication
- × Financial remuneration (payment)
- × Applies to a "use or disclosure"
- × Requires valid authorization stating that CE is receiving payment for making communication
- × Exceptions exist
- × No note necessary in NPP

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
- × NPP must state Authorization required for Sale of PHI

MARKETING VS. SALE

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

*new under HITECH

FUND RAISING, CONT.



- ✱ Requirements:

- + Include statement in Notice of Privacy Practices
- + Provide individual with clear & conspicuous opportunity to opt out of further fundraising communications with each communication
- + Op-out 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 CE's under HIPAA from using or disclosing PHI that is genetic information for underwriting purposes
 - ★ Expects: 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!

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:

1. Written Authorization from the individual
2. Waiver of Authorization from an IRB or Privacy Board
3. Only sharing of a LDS of data with DUA (for research, public health or health care operations only)



✖ Authorizations

+ Can be compound

+ Conditioned- and non-conditioned activities can be combined on same form

✖ Must clearly differentiate between two and provide individual with opportunity to opt in to research activities

+ 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.



RESEARCH - LIMITED DATA SET



- ✦ A CE may exchange LDS of PHI for purposes of research, public health or health care operations IF they enter into a Data Use Agreement (DUA) with recipient
- ✦ The DUA ensures that recipient of LDS will only use or disclose the PHI for limited purposes
- ✦ The DUA must contain certain required elements

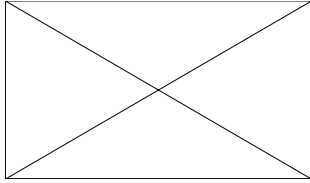
DE-IDENTIFIED DATA

- ✦ Health information can be *de-identified* by removing anything that identifies the individual
- ✦ De-identified data is not subject to HIPAA
- ✦ Two Methods:
 1. "Safe Harbor" approach
 - ✦ Remove 18 identifiers AND have no knowledge that remaining information could be used alone or with other information to identify an individual
 2. Statistical approach
 - ✦ Qualified statistical or scientific expert concludes that risk of re-identification is very small

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>

PATIENTS RIGHTS UNDER HIPAA

PATIENTS' RIGHTS VIDEO FROM OCR



RIGHT TO RECEIVE NOTICE OF USES AND DISCLOSURES OF INDIVIDUAL'S PHI

- ✖ Right to adequate notice of uses and disclosures of PHI that may be made by the CE
- ✖ Right to notice of individual's rights
- ✖ Right to know CE's legal duties with respect to PHI
- ✖ Exceptions for group health plans and inmates



NOTICE OF PRIVACY PRACTICES

- ✖ Applies to providers and health plans
- ✖ Certain content requirements
 - + How entity may use and disclose PHI
 - + Individual's Rights and how to exercise these Rights
 - + CE's legal duties with respect to information, including statement that entity is required by law to maintain privacy of PHI
 - + Whom individuals can contact for further information about CE'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 you have 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

PROVIDING THE NOTICE TO INDIVIDUALS

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



PROVIDING THE NOTICE TO INDIVIDUALS

NOTICE – MISCELLANEOUS

- | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> ✖ Material revisions to Notice require: <ul style="list-style-type: none"> + Providers <ul style="list-style-type: none"> ✖ Revise Notice & remove all copies of old Notice; replace with new Notice ✖ Provide new Notice to individuals upon request and at first treatment opportunity (or electronically) + Health plans <ul style="list-style-type: none"> ✖ 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) | <ul style="list-style-type: none"> ✖ Electronic Notice <ul style="list-style-type: none"> + Allowed if individual agrees to receive it in this manner ✖ Joint Notice of Privacy Practices <ul style="list-style-type: none"> + If part of an Organized Health Care Organization (OHCA) you may have one of these + Further requirements on content |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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
- ✖ Exceptions:
 - + Parents usually Personal Representative of their minor, unemancipated children UNLESS minor has ability under state law to consent for care
 - + Abuse, neglect, or endangerment exception



RIGHT TO ACCESS, COPY, AND INSPECT HEALTH CARE INFORMATION

- ✖ Right to inspect and obtain copy of PHI about individual in CE's designated record set (DRS)
 - + Must document your DRS
 - + Must document titles of persons or office responsible for receiving and processing requests
 - + Right to access exists for as long as CE maintains it or until 50 years after death
- ✖ Exceptions
 - + Psychotherapy notes
 - + Information prepared for litigation
 - + CLIA records no longer exempted!
- ✖ CE may deny access
 - + Unreviewable & Reviewable reasons exist
- ✖ Otherwise, must provide within 30 days (one 30 day extension possible)

RIGHT TO ACCESS, COPY, AND INSPECT HEALTH CARE INFORMATION

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> ✖ CE may deny access <ul style="list-style-type: none"> + Unreviewable Reasons to Deny + Reviewable Reasons to Deny | <ul style="list-style-type: none"> ✖ Timeliness <ul style="list-style-type: none"> + Must provide within 30 days + One 30 day extension possible |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

RIGHT TO ACCESS, COPY, AND INSPECT

- × Form of Access
 - + "Form and format" requested by individual, if readily producible
 - + If not, in readable hard copy form or other form and format as agreed to by CE and individual
 - + **If maintained in one or more designated record sets electronically and individual requests an electronic copy CE, must provide in electronic form!**
- × Manner of Access
 - + Individual may direct CE to send DRS to a 3rd party
 - + Individual's request must be 1) in writing, 2) signed by the individual, and 3) clearly identify person and where to send PHI

RIGHT TO ACCESS, COPY, AND INSPECT

- × Allowable Fees
 - + Must be reasonable and cost-based
 - + Can only include:
 1. Labor for copying PHI (paper or electronic)
 2. Supplies for creating paper copy or electronic media (if individual requests portable media)
 3. Postage
 - + May prepare explanation or summary if individual agrees to this - instead of providing DRS
- × **Be Careful: state law may allow fees that aren't considered reasonable and cost-based by HHS!**

RIGHT TO AMENDMENT

- × Right to amend information in CE's DRS
- × CE has right to deny amendment under certain circumstances
 - + Was not created by CE (unless originator no longer available)
 - + Isn't part of DRS
 - + Restricted from right to access
 - + Is accurate and complete
- × CE has 60 days to respond; can extend 30 more if necessary
- × If amend, CE has duty to inform others
 - + persons identified by individual and business associates
- × If deny, denial can be lengthy and allows for disagreement by Individual to be kept with DRS

RIGHT TO REQUEST PRIVACY PROTECTIONS

- ✖ Right of Individual to Request Restriction of Uses and Disclosures
 - + Must permit individuals to request restrictions for:
 - ✖ Uses or disclosures of PHI to carry out TPO
 - ✖ Disclosures for involvement in individual's care and notification purposes
 - + CE does not have to agree but if CE does agree, bound by that restriction
- ✖ EXCEPTION: CE PROVIDER MUST restrict information from going to insurer if individual pays for item/service out-of-pocket & in full and requests this!

**RIGHT TO REQUEST PRIVACY PROTECTIONS.
CONT.**

- ✖ Right to Confidential Communications
 - + Must permit individuals to request...
 - + Must accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations
- ✖ CE Provider may not ask why
- ✖ Health plans may require individual to state doing so would endanger the individual

RIGHT TO OBTAIN ACCOUNTING OF DISCLOSURES

- ✖ Right to receive an accounting of disclosures of PHI made by CE in prior 6 years
- ✖ Exceptions:
 - + Treatment, payment and health care operations
 - + To individuals of PHI about them
 - + Incident to a use/disclosure otherwise permitted or required by HIPAA
 - + Pursuant to an Authorization
 - + For facility's directory
 - + To persons involved in individual's care or notification purposes
 - + For national security or intelligence
 - + To correctional institutions or law enforcement officials
 - + Disclosures of limited data sets
- ✖ Still to come: implementation of HITECH's change to HIPAA to require the accounting to include disclosures for "treatment, payment and health care operations" from an "electronic health record"

RIGHT TO OBTAIN ACCOUNTING OF DISCLOSURES

- ✖ Content of Accounting
 - + Date of disclosure
 - + Name of entity or person who received PHI and address, if known
 - + Brief description of PHI
 - + Brief statement of purpose
- ✖ Grouping allowed for routinely occurring and research disclosures
- ✖ Timeliness
 - + CE has 60 days to provide accounting, may have 30 day extension
- ✖ Fees
 - + CE may charge reasonable, cost-based fee after providing 1 copy for free - for each subsequent request by same individual in 12 month period

Where is your LOG? Is it up-to-date?

RIGHT TO COMPLAIN

- ✖ ...about alleged violations of the regulations and CE's own policies
- ✖ CE must provide a process for individuals to make complaints
- ✖ CE must document all complaints received, and their disposition, if any

RIGHT TO BE NOTIFIED WHEN A BREACH OCCURS

- ✖ CEs must state in Notice of Privacy Practices that it will notify affected individuals following a breach of unsecured PHI



KEY CONCEPT: 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

KEY CONCEPT: SANCTIONS

- ✖ Required that you have them and apply them to workforce members who violate your policies and procedures
- ✖ One of the first things you may be asked for in an audit!
- ✖ Must train workforce to understand sanctions may apply
- ✖ Must document sanctions taken



KEY CONCEPT: RETALIATION

- ✖ Privacy Rule:
 - + CE may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for...
 - + The exercise by the individual of any Right established under HIPAA
- ✖ Enforcement Rule
 - + CE may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for...
 - + Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part
 - + Opposing any act or practice made unlawful by HIPAA
 - ✖ ...provided individual has good faith belief that practice opposed is unlawful, and manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA

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



BREACH NOTIFICATION RULE

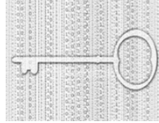
WHAT IS A BREACH?

- ✖ “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



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?

3 statutory exceptions listed in IFR stay the same in Final Rule

#1

#2

#3

119

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!

120

RISK ASSESSMENT - 4 FACTORS			
<div></div>	<div></div>	<div></div>	<div></div>
TYPE? <ul style="list-style-type: none"> The nature and extent of the PHI involved Consider types of identifiers and likelihood of re-identification 	WHO? <ul style="list-style-type: none"> The unauthorized person who used the PHI or to whom the disclosure was made 	HOW OR HOW MUCH? <ul style="list-style-type: none"> Whether the PHI was actually acquired or viewed 	MITIGATION! <ul style="list-style-type: none"> The extent to which the risk to the PHI has been <i>mitigated</i>

121

REPORTING OBLIGATIONS - INDIVIDUALS
<ul style="list-style-type: none"> ✗ Within NO LATER than 60 days, regardless of number affected) ✗ Written letter, by first-class mail (email ok if individual has agreed to it) ✗ Certain elements are required in letter – KNOW THEM! ✗ “Substitute Notice” required if you have insufficient contact information <ul style="list-style-type: none"> + If involves 10 or more – special provisions apply such as posting on website for 90 days



REPORTING OBLIGATIONS. CONT.
<ul style="list-style-type: none"> ✗ To Department of Health and Human Services (through OCR website) <ul style="list-style-type: none"> + 500 or more individuals = “immediate reporting” + <500 individuals affected = reporting may be delayed until 60 days after end of calendar year in which breach was discovered ✗ To Media outlets <ul style="list-style-type: none"> + ...if more than 500 individuals in a state or jurisdiction are affected + “immediate reporting” = concurrent with letters and report to HHS + jurisdiction = a geographic area smaller than a state such as a county, city, or town ✗ Reporting required to “prominent media outlets” serving the State or jurisdiction

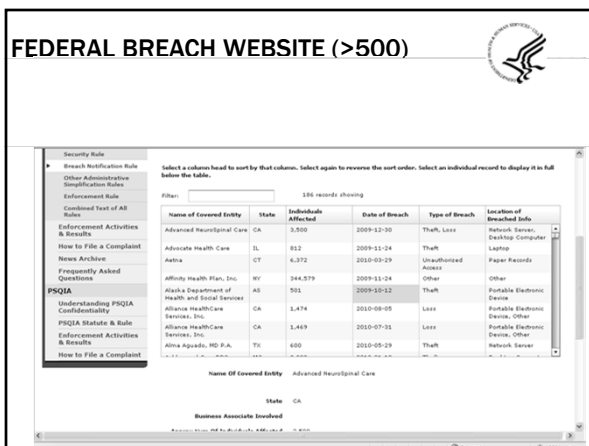
MITIGATION

- ✖ Covered entities have a duty to mitigate harmful effects due to uses or disclosures of PHI
- ✖ It is only possible to mitigate what is know!
- ✖ As a Privacy/Compliance 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

BUSINESS ASSOCIATES AND BREACH REPORTING

- ✖ Must report to CE (or upline business associate) within NO LATER THAN 60 days
- ✖ Stricter timeframes almost always called for in business associate agreements
- ✖ BEWARE (OR BE HAPPY?!) – HHS is going straight to BAs when breaches occur!

FEDERAL BREACH WEBSITE (>500)



Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.


Filter: 195 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Info
Advanced Neurological Care	CA	3,500	2009-12-30	Theft, Loss	Network Server, Desktop Computer
Advocate Health Care	IL	812	2009-11-04	Theft	Laptop
Aetna	CT	4,372	2010-03-29	Unauthorized Access	Paper Records
affinity Health Plan, Inc.	NY	344,579	2009-11-04	Other	Other
Alaska Department of Health and Social Services	AK	501	2009-10-12	Theft	Portable Electronic Device
Alliance HealthCare Services, Inc.	CA	1,474	2010-08-05	Loss	Portable Electronic Device, Other
Alliance HealthCare Services, Inc.	CA	1,469	2010-07-31	Loss	Portable Electronic Device, Other
Alma Aguado, MD P.A.	TX	400	2010-05-29	Theft	Network Server

Name Of Covered Entity: Advanced Neurological Care

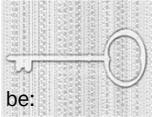
State: CA

Business Associate Involved:



SECURITY RULE


Electronic systems and devices which *create, receive, maintain or transmit* information about a person's health records must be protected



✖ Intended to be:

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

HIPAA'S SECURITY RULE



Confidentiality - ensuring that only those individuals who are supposed to access electronic PHI (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 EPHI



SECURITY RULE CONT.

× Standards (18):

- + CE or BA **must** **comply** with Standards
- + Examples: Integrity, Workforce Security, Encryption

× Implementation Specifications (36)

- + Required
 - × You must implement it!
- + Addressable:
 - × You must:
 - ★ Assess if it is a reasonable and appropriate safeguard in your environment and 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
- + Examples: Data backup plan, unique user identification, access control

STANDARDS - ADMINISTRATIVE

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> × Security management process <ul style="list-style-type: none"> + Risk analysis ⓘ + Risk management ⓘ + Sanction policy ⓘ + Information system activity review ⓘ × Assigned security responsibility × Workforce security <ul style="list-style-type: none"> + Authorization and/or supervision ⓘ + Workforce clearance procedure ⓘ + Termination procedures ⓘ × Information access management <ul style="list-style-type: none"> + Isolating health care clearinghouse functions ⓘ + Access authorization ⓘ + Access establishment and modification ⓘ | <ul style="list-style-type: none"> × Security awareness and training <ul style="list-style-type: none"> + Security reminders ⓘ + Protection from malicious software ⓘ + Log-in monitoring ⓘ + Password management ⓘ × Security incident procedures <ul style="list-style-type: none"> + Response and reporting ⓘ × Contingency plan <ul style="list-style-type: none"> + Data backup plan ⓘ + Disaster recovery plan ⓘ + Emergency mode operation plan ⓘ + Testing and revision procedures ⓘ + Applications and data criticality analysis ⓘ × Evaluation × Business associate contracts and other arrangements <ul style="list-style-type: none"> + 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 logoff ▲
 - + 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 ■
 - + Workforce members who have responsibility for implementing security must have access to P&P ■
 - + 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!



✖ You must review and modify security measures, as needed, to continue provision of reasonable and appropriate protection of EPHI

✖ Training is required!

✖ How else are you going to: "ensure compliance with the Security Rule by 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 error, accidental deletions)
- + Environmental (e.g., power surges and spikes, hazmat 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 on EPHI by exploiting a vulnerability



Rank your risks as part of your Risk Analysis!

- ✖ Risk Analysis
164.308(a)(ii)(A)
- ✖ Risk Management
164.308(a)(ii)(B)

RISK ASSESSMENT/RISK MANAGEMENT

- ✖ 9 Steps of Risk Analysis (OCR guidance)
 - + Scope of the Analysis
 - + Data Collection
 - + Identify and Document Potential Threats and Vulnerabilities
 - + Assess Current Security Measures
 - + Determine the Likelihood of Threat Occurrence
 - + Determine the Potential Impact of Threat Occurrence
 - + Determine the Level of Risk
 - + Finalize Documentation
 - + Periodic Review and Updates

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskfinalguidancepdf.pdf>

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?

COVERED ENTITIES

- ✦ Sign business associate agreements (BAAs) & maintain documentation
- ✦ Consider a checklist, audit or other function to monitor their compliance??
- ✦ Ensure BAs are entering into "at least as strict" agreements for uses and disclosures of your PHI with Subcontractor BAs

BUSINESS ASSOCIATES

- ✦ Make sure you understand what you are binding your organization to when you sign BAAs
- ✦ Have them in place with any subcontractors who handle PHI

BUSINESS ASSOCIATE MANAGEMENT

PASSWORD MANAGEMENT

- ✖ At least 9 characters

- + Require:

- ✖ Upper case
 - ✖ Lower case
 - ✖ Numbers
 - ✖ Symbols

- ✖ Examples of complex passwords:

- + RockiesSI@#
 - + NeverBeenRockedEnough:)
 - + NewStarWarsMay19!
 - + "Francisco,that'sfuntosay"

- ✖ Never, ever, ever share your password



2011 WORST
PASSWORDS

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. Dragon
11. Baseball
12. 1111111
13. iloveyou
14. master
15. sunshine

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 responsibility 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 outside your organization - 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 any unauthorized person in work area



MOBILE DEVICES

- ✗ Only use organization-approved and ENCRYPTED devices
- ✗ Install remote-wipe capabilities
- ✗ Require complex passwords
- ✗ Ensure workforce knows who to notify and by when 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
- Implement system patches ASAP
- Hire a consultant to periodically pen test your 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

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 place in shredder should be given to IT Support for appropriate destruction
- ✖ Semi-annual 'shredding day' at your organization!



WHAT YOU SHOULD BE WORRIED ABOUT

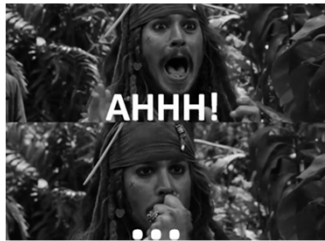
1. Your data -- where is it?
2. Any data that can move that isn't encrypted
3. Vendors -what are they doing with your data?
4. Buy in from the top
 - + Are you telling the C-Suite & Board when major incidents happen? Do they care?
5. State laws that allow people to sue for HIPAA violations

WHAT YOU SHOULD BE WORRIED ABOUT. CONT.

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

BUT REMEMBER...

- + Privacy regulations changing constantly
- + Security “best practices” evolving exponentially with technology
- + Nobody has enough resources



PRIVACY AND SECURITY COMPLIANCE IS A JOURNEY, NOT A DESTINATION

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



THE END

RESOURCES - GENERAL

- + Federal Register for the Final Omnibus Rule
 - × <https://www.federalregister.gov/>
- + Office for Civil Rights
 - www.hhs.gov/ocr/
- + Office of National Coordinator
 - www.healthit.gov
 - Check out: HIT Policy Committee Privacy & Security Tiger Team Virtual Hearing on Accounting for Disclosures 9/30/2013

RESOURCES - SECURITY RISK ASSESSMENTS

RESOURCES - SECURITY RULE STANDARDS

- × <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, others
- × Addresses 45 implementation specifications identified in HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues