PRIMA 2014
WEBINAR SERIES

Public Risk Management Association (PRIMA) Presents:

A Webinar on HIPAA and the Affordable Care Act

May 2014

Presented by:
David Sanders, JD, LLM

HIPAA and the Affordable Care Act

- Overview of the HIPAA Privacy Rule
- Covered Entities Subject to HIPAA Privacy Rule
- Protected Health Information
- Use and Disclosure of Protected Health Information
- Individual Rights Under HIPAA
- HIPAA Data Security
- Affordable Care Act
- Questions

HIPAA Overview – Key Effective Dates

Privacy

Rules that safeguard the privacy of individually identifiable health information by putting limits on its use and disclosure (Effective April 14, 2003)

Electronic Data Interchange

Rules that standardize transactions and code sets for the electronic data interchange of health information (Effective October 16, 2003)

Electronic Data Security

Rules that protect the confidentiality and integrity of data in electronic media, including the prevention of unauthorized use and restriction of physical access to such data (Effective April 20, 2005)

HITECH Act

Economic stimulus legislation has significant impact on the policies and procedures used by healthcare providers, health plans and their Business associates (Effective March 26, 2013; General Compliance Date September 23, 2013)

HIPAA Terminology

- **There are important terms related to HIPAA that you need to understand:**

  - ❑ Covered Entity
  - ❑ Protected Health Information
  - ❑ Business Associate
  - ❑ Permissible Uses and Disclosures



What Are Covered Entities?

Health Plans

- Medical plans
- Dental plans
- Vision plans
- HMOs
- Prescription drug plans
- Health FSA plans
- EAPs
- Long-term care insurance
- Health insurance issuers
- Certain Wellness and executive plans

Health Care Providers that engage in certain electronic transactions

- Doctors
- Dentists
- Hospitals
- Optometrists
- Medical Clinics/Offices
- Pharmacists
- Nurses
- Other health care providers

Health Care Clearinghouses

- Entities that convert electronic data for HIPAA compliance

What are NOT Covered Entities?

- HIPAA **generally does not cover** non-Health Plans or programs including:

  - Life insurance
  - Workers' compensation
  - FMLA leave
  - Pre-employment testing
  - STD and LTD programs
  - Health fairs
  - Fitness for duty exams



HIPAA - Protected Health Information (PHI)

- Health Information about an Individual that is:
  - Created or received by a Covered Entity or employer
  - Transmitted or maintained in any form or medium
  - Identifies the individual (directly or indirectly), and
  - Relates to the individual's:
    - Physical or mental health condition (past, present or future)
    - Provision of health care, or
    - Payment for the individual's health care (past, present or future)

NOTE: Protected Health Information (PHI) may be in oral, paper or electronic format. It includes demographic information collected from the Individual.

Types of Personal Information We Need to Protect

- Social Security Numbers / Medicare ID Numbers
- Home address and other contact details
- Specific benefits, including:
  - Health plan enrollment
  - Claims details emails from Aetna
- Health status
- Account numbers

Remember that "protected" doesn't mean you are forbidden from using the data – but it does mean use with care and only share with individuals within the "Firewall"!

NOTE: Diagnostic information does not have to be present in order to have Protected Health Information.

What is NOT Protected Health Information?

De-identified or summary health information

To de-identify must remove all identifiers - 18 Identifiers defined by HIPAA:

- ☑ Name
- ☑ Postal Address
- ☑ All elements of dates except year
- ☑ Telephone number
- ☑ Fax number
- ☑ Email address
- ☑ URL address
- ☑ IP address
- ☑ Social security number
- ☑ Account numbers
- ☑ License numbers
- ☑ Medical record number
- ☑ Health plan beneficiary #
- ☑ Device identifiers and their serial numbers
- ☑ Vehicle identifiers and serial number
- ☑ Biometric identifiers (finger and voice prints)
- ☑ Full face photos and other comparable images
- ☑ Any other unique identifying number, code or characteristics

What is a Business Associate?

- A "business associate" is a person or entity that performs or assists in the performance of a function or activity on behalf of a covered entity and uses PHI in the process of performing that function or activity.
- Examples:
  - A third party administrator that assists in the payment of claims.
  - An attorney whose legal services to an employer involves access to protected health information.
  - A pharmacy benefits manager that manages a health plan's pharmacist network.

When May PHI Be Used or Disclosed?



As Long As You Follow The Rules …

- HIPAA allows a Health Plan to use or disclose PHI:
  - For treatment, payment or health care operations ("TPO")
  - As permitted or required by law
  - When an individual authorizes release to others
  - When an individual asks for own health information

Plan Sponsor – PHI Disclosure

- Disclosure of PHI to designated Plan Sponsor personnel for treatment payment or health care operations are permissible
  - Plan Document must establish separation (i.e., "firewall") between Health Plan and Plan Sponsor
  - Access to PHI limited to designated Plan Sponsor personnel within Health Plan's "firewall"
    - Common categories of personnel within "firewall"
      - Privacy Official, Security Official, and Contact Person
      - Corporate Health Plan administrative personnel
      - Benefit Managers
    - Personnel outside the "firewall" are denied access to PHI (except by authorization)

NOTE: Disclosures are generally subject to a "minimum necessary" disclosure standard.

Uses and Disclosures Permitted by Law

- Health Plan may disclose PHI without an authorization for any of the following reasons:

- Public health activities
- Judicial proceedings
- Law enforcement
- About decedents
- Health oversight activities
- Cadaveric organ, eye or tissue donation
- Research
- As required by law
- Special government functions
- To avert serious threat to health or safety
- Workers' compensation
- About victims of abuse or domestic violence

Plan Sponsor - PHI Disclosure

- Unacceptable Uses of PHI by Plan Sponsor - Some Examples:
  - Using Health Plan claims data to suspend an employee for drug use
  - Using Health Plan records to check information given by an employee requesting FMLA leave for a serious health condition
  - Giving medical plan information to staff to support denial of related disability benefits
  - Receiving compensation for an individual's health information without his or her authorization
  - Using health information for marketing and fundraising activities



IMPORTANT: Disclosure of PHI in each of these cases would not be permissible unless a written authorization was obtained from the employee.

HIPAA - Authorization

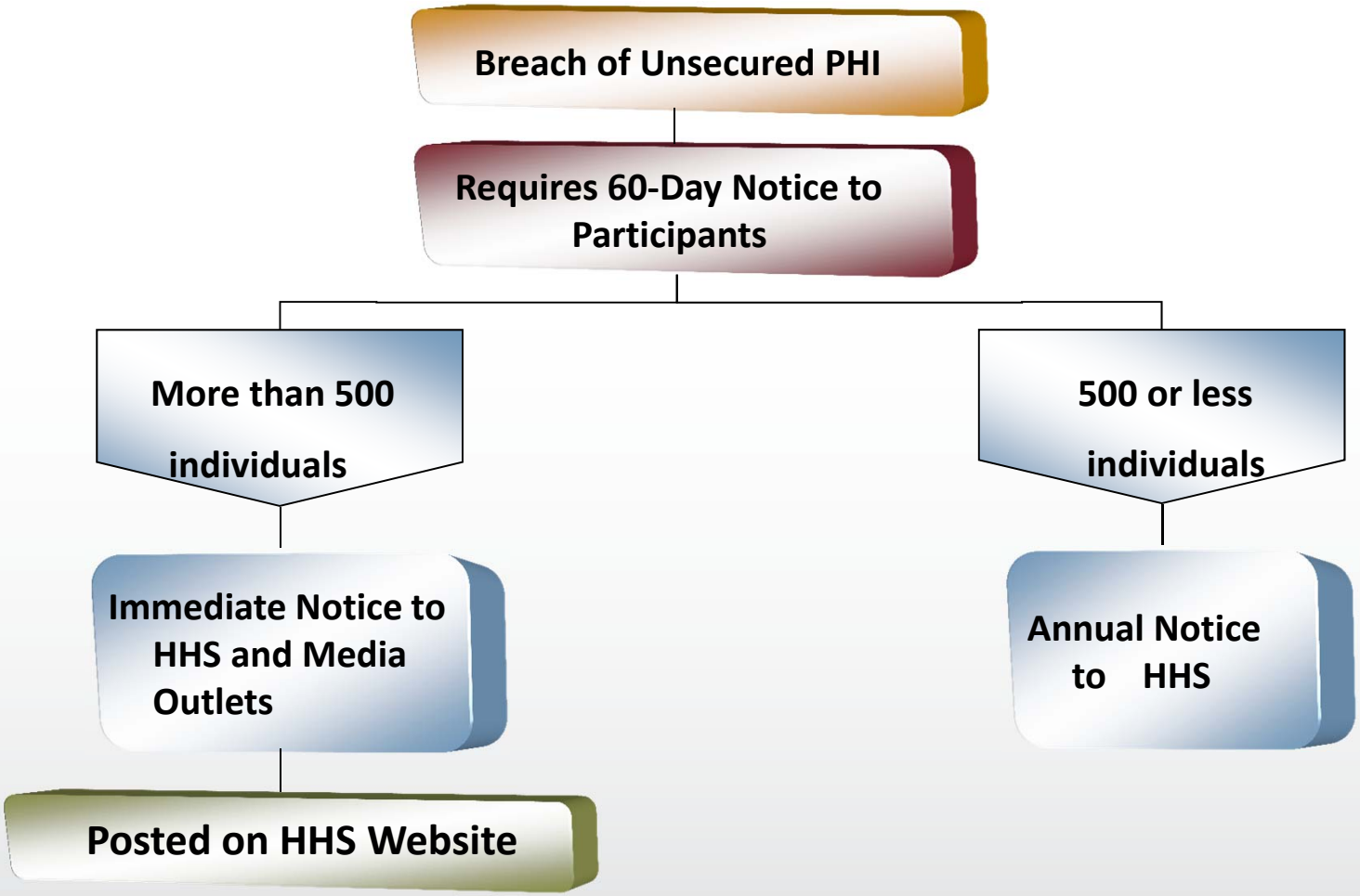
- Health Plan may use or disclose PHI pursuant to written authorization from an individual.

- Authorization must:
  - Describe information to be used or disclosed and purpose of the request
  - Identify the person authorized to request and receive access to the PHI
  - Acknowledge right to revoke the authorization
  - Describe the consequences (if any) of refusal to sign the authorization
  - State that PHI will no longer be protected by HIPAA after disclosure
  - Specify an expiration date or event (Open-ended authorizations are not permitted)

Rights of Individuals Under HIPAA

- Right to receive a HIPAA Privacy Notice
- Right to inspect and copy PHI
- Right to amend PHI
- Right to request restrictions on use or disclosure of PHI
  - Restriction required if non-treatment related and fully paid by individual [New]
- Right to request accounting of prior three-year electronic disclosures of PHI [New]
- Right to alternative communications of PHI
- Right to an accounting of non-routine disclosures
- Right to file a complaint
- Right to written notice within 60 days after disclosure breach [New]

HIPAA/HITECH – New Notice Requirements



HIPAA/HITECH – Unsecured PHI

- Unsecured PHI
  - PHI that is not safeguarded by an American National Standards Institute (ANSI) technology standard that makes PHI unusable, unreadable, or indecipherable to people who do not have permission to access it
  - Unsecured PHI can include information in **any** form or medium including electronic, paper or verbal form
- Breach
  - Someone without permission accessed, used or disclosed protected health information and now you believe the privacy and/ or security of a participant's health information has been compromised
- Examples of Possible Breaches
  - A Benefits Manager leaves PDA on a store counter and then someone else picks it up
  - A thief breaks into a car and steals a HR staff member's laptop
  - Someone retrieves shredded paper and tapes it together

HIPAA/HITECH – New Notice Requirements

- Notice of Breach – Covered entity to provide:
  - Description of breach
  - Type of unsecured PHI disclosed
  - Steps individuals should take to avoid harm
  - Description of covered entity's mitigation, investigation, and prevention efforts
  - Contact information for covered entity

HIPAA - Privacy Notice

- HIPAA Privacy Notice to be distributed
  - Self-insured health plans
  - Fully insured plans – vendor notice if “hands-off” PHI
- HIPAA Privacy Notice should be provided to new employees at time of employment
- Notice posted on employee benefits intranet web site
- Reminder of entitlement to Notice must be communicated once every three years



NOTE: Individuals are entitled to a copy of the Notice upon request, even if not a participant in the Health Plans.

HIPAA Record Retention Requirements

- Retain copies of documents for a period of six (6) years after the later of:
  - When document is created; **or**
  - When PHI is no longer in effect
- Documents to be retained include:
  - Health information complaints and responses
  - Authorizations received
  - Designation of Privacy Official and Contact Person
  - Health Plan documents
  - Business Associate privacy agreements
  - Notices of Privacy Practices issued
  - Training records

Training Requirements



HIPAA training required for:

- Employees who have access to **P**rotected **H**ealth **I**nformation (PHI)
- Senior executives involved with PHI
  - Claim and appeal reviews
- Privacy Official and HIPAA Contact Person
- New members of staff having access to PHI
- Temporary employees who do not enter into a Business Associate Agreement

HIPAA training must be documented

- Maintain Training Log
- Maintain copies of training materials

HIPAA Civil Money Penalties

Civil Money Penalties That May Be Imposed After Enactment of HITECH

Penalties for Violations Occurring Before February 18, 2009			Penalties for Violations Occurring On or After February 18, 2009			
Penalty Per Violation		Maximum Penalty Per Calendar Year for Identical Violations	Level of Culpability	Penalty Per Violation		Maximum Penalty Per Calendar Year for Identical Violations
Minimum	Maximum			Minimum	Maximum	
None	$100	$25,000	Covered Entity Did Not Know and By Exercising Reasonable Diligence Would Not Have Known of Violation	$100	$50,000	$1,500,000
NOTE: • Penalty Rules for Violations Occurring Before February 18, 2009, Make No Distinction as to the Covered Entity's Level of Culpability • All Minimum and Maximum Penalty Amounts Are Per Covered Entity			Violation Due to Reasonable Cause	$1,000	$50,000	$1,500,000
			Violation Was Due to Willful Neglect and Corrected Within 30 Days of When Covered Entity Knew or Would Have Known of Violation	$10,000	$50,000	$1,500,000
			Violation Was Due to Willful Neglect and Not Corrected Within 30 Days of When Covered Entity Knew or Would Have Known of Violation	$50,000	-----	$1,500,000

HIPAA Privacy "Check List"

- ☑ Conduct compliance assessment
- ☑ Amend Health Plan documents and create "firewalls" between Health Plans and Plan Sponsor; obtain Plan Sponsor certification
- ☑ Adopt health information policies and procedures
- ☑ Formally designate Privacy Official and Contact Person
- ☑ Conduct HIPAA training (initial and ongoing) for those employees with access to PHI as part of their jobs
- ☑ Provide Notice of Privacy Practices to all applicable active and retired employees
- ☑ Execute Business Associate Agreements
- ☑ Implement PHI safeguards
- ☑ Establish record retention procedures
- ☑ Develop administrative forms and authorizations
- ☑ Establish complaint procedure
- ☑ Develop sanctions for noncompliance

Overview Of The HIPAA Data Security Rule and ePHI



What Is Electronic PHI (ePHI)?

- **Electronic Protected Health Information (ePHI) is PHI that is transmitted or maintained in electronic media**
  - **Electronic media** includes:
    - **Electronic storage media** such as memory devices in computers or any removable or transportable digital memory
    - **Transmission media** used to exchange PHI already in electronic storage media



Critical Question: Did the health data exist in electronic form prior to its transmission?

What Is ePHI? *(Continued)*

Protected Health Information that is in:	Why is it ePHI?
▪ E-Mails and attachments	➤ The PHI existed in electronic form prior to transmission
▪ Computer to paper facsimiles	
▪ Internet and Extranet	
▪ Hard Drives	➤ The PHI is held in electronic storage media
▪ Network servers	
▪ Floppy discs and CD-ROMs	
▪ Magnetic tapes	
▪ Digital memory cards	

What Is ePHI? *(Continued)*

Protected Health Information that involves:	Why is it ePHI?
▪ Transmission media used to exchange information already in electronic storage media (e.g., leased lines, private networks)	➤ The PHI existed in electronic form prior to transmission
▪ Physical movement of removable/transportable electronic storage media	➤ The PHI is held in electronic storage media

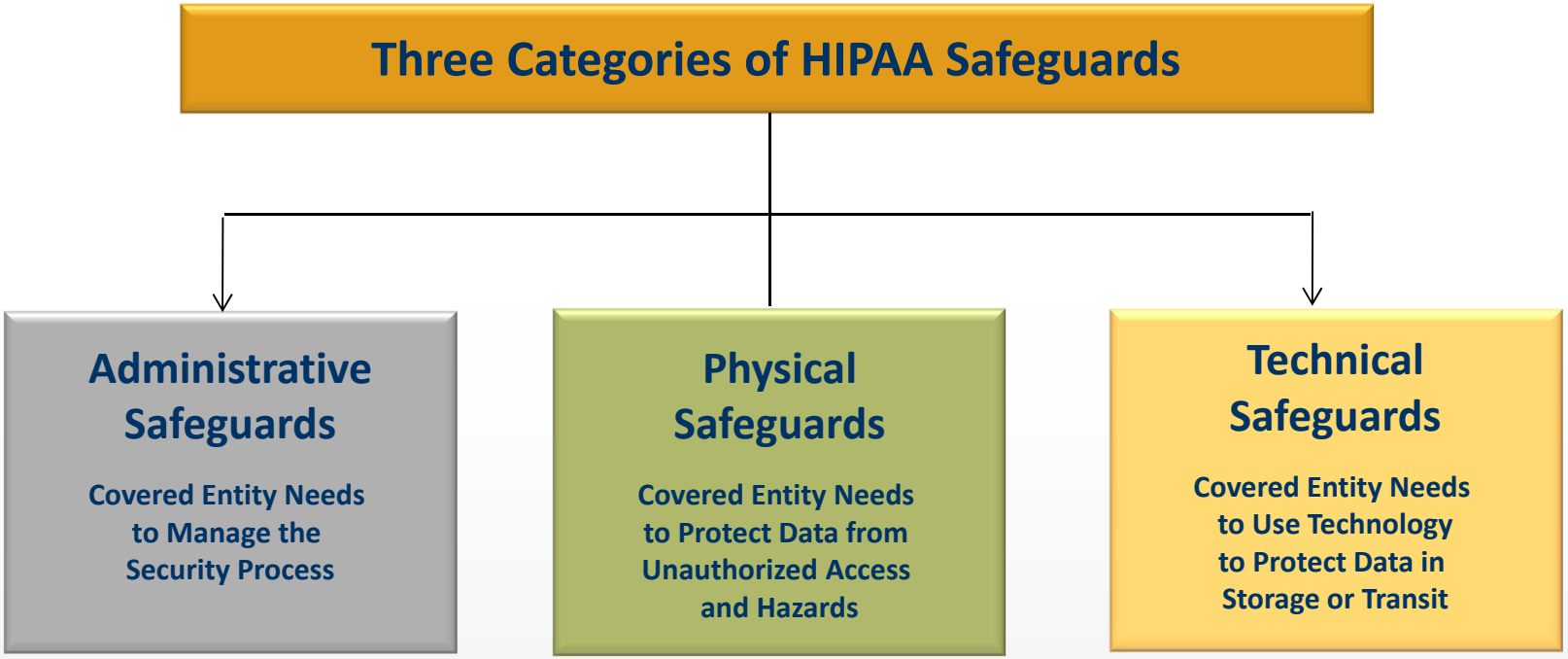
What Is Not ePHI?

Protected Health Information in:	Why?
▪ Telephone conversations	➢ PHI is not in electronic form prior to transmission
▪ Voice mail messages	
▪ Paper-to-paper facsimiles	
▪ Hand-written notes	➢ The PHI does not involve electronic media
▪ Verbal conversations	
▪ Paper files and records	



All Protected Health Information must be safeguarded under the HIPAA privacy rules even if it is not ePHI.

HIPAA Data Security - Safeguards



HIPAA under the Affordable Care Act

Health Plan Identifier

- ACA requires HHS to issue rules creating a Health Plan Identifier (HPID)
  - Rules issued in September, 2012 require health plans to obtain HPID by November 5, 2014
    - Small plans (annual receipts of $5 million or less) have until November 5, 2015
- "Controlling Health Plans" (CHP) and "Subhealth Plans" (SHP) must submit HPID application via CMS website
  - CHP is one which controls its own business activities, actions, or policies
  - SHP is one whose business activities, actions or policies are directed by CHP
  - CHP is permitted to obtain HPID for SHP
- Once obtained, HPID must be referenced in all standard transactions between the plan and covered entities starting on November 7, 2016
  - Standard transactions include eligibility transmissions, claims, authorizations/referrals, enrollment/disenrollment, EFT, remittance advice

Health Plan Standard Transactions Certification

- ACA requires health plans to file two certifications with HHS that demonstrate compliance with standard transaction requirements
  - Certifications must be submitted by December 31, 2015
    - Rules not yet issued for second certification, so deadline may be delayed
  - First certification applies to eligibility, claim status and EFT/remittance advice
  - Second certification applies to claims/encounter information, enrollment/disenrollment, premium payments, claims attachments and authorization/referrals
- "Controlling Health Plan must file certification on behalf of "Subhealth Plans
- Penalties may be assessed for compliance failures
  - $1 per covered life per day until certification is complete up to a maximum penalty of $20 per covered life
  - Plan may also be assessed penalty of up to $40 per covered life if inaccurate or incomplete information is knowingly provided

Final Thoughts

- Assess health plan compliance status with privacy and data security rules
- Ensure workforce has been adequately trained and PHI safeguards are in place
- Ascertain health plan responsibilities for HPID and standard transaction certifications and establish a game plan for complying