



# HIPAA PRIVACY, SECURITY AND HITECH TRAINING

## State of Delaware

Statewide Benefits Office and Participating Groups in the Group Health Insurance Program

Copyright ©2013 by The Segal Group, Inc., parent of The Segal Company. All rights reserved.



# What is HIPAA?

## Health Insurance Portability & Accountability Act of 1996

- ▶ First enacted in 1996
- ▶ The privacy rule established, for the first time, a set of national standards for the protection of certain health information. A major goal of the privacy rule is to assure that individuals' health information is properly protected while allowing for the flow of needed health information.
- ▶ Interim final regulations under the American Reinvestment and Recovery Act (ARRA) were issued August 17, 2009
- ▶ Final regulations under HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Nondiscrimination Act (GINA) were issued January 25, 2013

# What is HITECH?

- ▶ Originally passed as part of ARRA in 2009. Omnibus rule issued January 25, 2013, amended the existing privacy and security rules effective September 23, 2013
- ▶ The final rule states that PHI that is used or disclosed in violation of the Privacy Rule is presumed to be compromised, and therefore, requires breach notification
  - However, this presumption may be overcome if the group health plan or business associate can show “there is a low probability that the information has been compromised”
- ▶ Business Associates (who are similar to subcontractors) are now directly liable for compliance with the Security Rule’s administrative, physical, and technical safeguards, and documentation requirements.
  - It now includes subcontractors and storage providers
- ▶ Enhanced penalties and enforcement

# HIPAA Privacy/Security Compliance Dates

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

**Privacy Rule:**  
April 14, 2003

**Security Rule:**  
April 21, 2005

**Health Information Technology for Economic and Clinical Health (HITECH)—Interim Final Rule on Breach Notification:**  
September 23, 2009

**Electronic Data Interchange Rules (EDI):**  
October 16, 2003 (if compliance plan was filed in October 2002)

**HIPAA/HITECH Omnibus Rule of 2013:**  
September 23, 2013

# HIPAA Privacy Rule In A Nutshell

- ▶ Requires covered entities (health care providers, health plans/issuers and clearinghouses) to implement reasonable policies and procedures to keep “protected health information” (PHI) confidential
- ▶ Gives individuals certain rights with regard to access to, and use and disclosure of, their “individually identifiable health information”
- ▶ Does not prohibit the exchange of PHI for treatment, payment or healthcare administrative operations

A hand in a dark suit jacket and white shirt cuff is pointing upwards with the index finger. Above the hand is a blue hand-drawn rounded rectangle containing the word "PRIVACY" in blue, uppercase, sans-serif letters.

PRIVACY

# Where Does Everyone Fit?

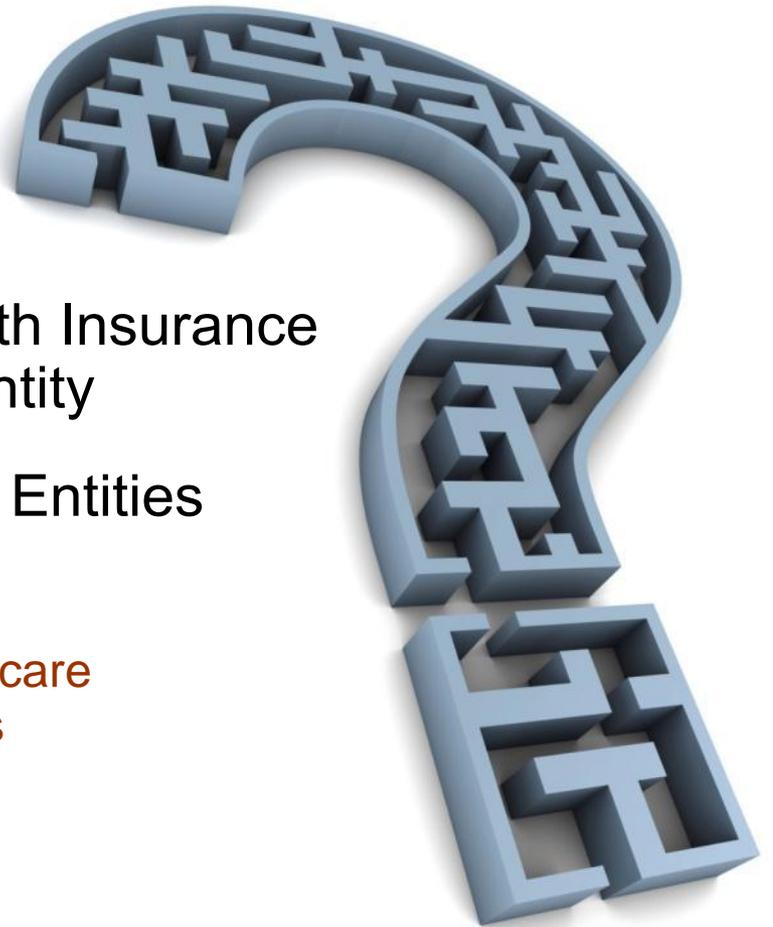
## ▶ Covered Entities

- Health care providers
- Health care clearinghouses\*
- Health plans and health insurance carriers

## ▶ The State of Delaware's Group Health Insurance Program ("the Plan") is a Covered Entity

## ▶ "Business Associates" help Covered Entities administer health plans

\*Health care clearinghouses process health care transactions on behalf of providers and plans



# Protected Health Information (PHI)

- ▶ **Protected health information**, or PHI, includes individually identifiable health information that is transmitted or maintained by a covered entity in any form or media
- ▶ Includes electronic, oral and written information



# Individually Identifiable Health Information

- ▶ **Individually identifiable health information** is health information that either must identify the individual or with a reasonable basis to believe that an individual can be identified using the information
- ▶ The privacy rule lists 18 ways to identify a person, including social security number, name, member identification number, email and postal addresses, phone number, account number, license number, picture, etc.
- ▶ Having just one of these 18 identifiers is enough to make the data “individually identifiable!”



# Types of PHI



- ▶ Typical Types of PHI You and our Business Associates May Handle:
  - Eligibility information
  - Enrollment information
  - Claims information
  - Claims appeals
  - Reports from third-party administrators or other vendors (such as, pharmacy benefit managers, preferred provider organizations, utilization review companies, etc.) may contain PHI
  - Coordination of benefits determinations
  - Quality assessment information (audits)
  - Medical condition information

# PHI and the State's Human Resource Departments

- ▶ PHI must NOT be used by the employer/plan sponsor for discipline, hiring, firing, placement, promotions/demotions, etc.
- ▶ This means that HR staff who deal with hiring/firing typically should not have access to PHI
- ▶ Benefits staff cannot share PHI with the HR staff without the individual's written authorization
- ▶ **KEY POINT:** Employees' employment files that HR staff need access to, such as performance reviews, job application, FMLA, workers' compensation, or disability (i.e., non-HIPAA regulated files), should be separated from HIPAA-regulated files

# Use and Disclosure of PHI

- ▶ Group health plans (technically, the staff that administer these plans) must protect PHI and ONLY use or disclose/release PHI for these five reasons:
  - To the individual — about that individual
  - For treatment, payment and health care operations
  - For legally permissible reasons (such as, for public health reasons, in response to a court order or subpoena, to a coroner, medical examiner or funeral director, etc.)
  - With a signed HIPAA authorization form from the individual
  - To the Federal and/or State Department of Health and Human Services for enforcement purposes

# Benefits That HIPAA Regulates

- ▶ Group health plans
- ▶ Dental plans
- ▶ Employee assistance programs (EAPs)
- ▶ Vision and hearing plans
- ▶ Claims administrators
- ▶ Pharmacy benefit managers (PBMs)
- ▶ Flexible spending accounts (FSAs)
- ▶ Health reimbursement arrangements (HRAs)
- ▶ Consolidated Omnibus Budget Reconciliation Act (COBRA)



# Benefits HIPAA Does NOT Regulate

Although this information is confidential, HIPAA does not cover:

- ▶ Life and Accidental Death & Dismemberment (AD&D) insurance
- ▶ Workers' Compensation (WC)
- ▶ Short-term disability (STD)
- ▶ Long-term disability (LTD)
- ▶ Pension plans



# Employment Records

▶ Although employment records held by the State in its capacity as an employer are confidential, they are not subject to HIPAA. Examples include:

- FMLA requests
- ADA records
- Workers' Compensation records and OSHA reports
- Disability records
- Sick leave requests or justifications
- Return-to-work data
- Drug screening results/alcohol and drug free workplace
- Fitness for duty exam results



# Audits

- ▶ The U.S. Department of Health and Human Services conducts periodic and sometimes unannounced reviews of covered entities to ensure correct measures are being taken!

**AUDIT**

# Penalties For HIPAA Violations

- ▶ New tiered penalty structure for civil monetary penalties is based on the intent behind the violation
- ▶ Old penalties maxed out at \$25,000 per year per standard violated
- ▶ New penalties can reach \$1.5 million per year per standard or higher
- ▶ Penalties will be mandatory in situations involving “willful neglect” and a formal investigation is required
- ▶ Covered Entities and Business Associates are liable for their employees’ actions and employees may be subject to criminal charges



## Penalties For HIPAA Violations *continued*

Entity	Incident	Result
<b>WellPoint Inc.</b> (July 2013)	Security weaknesses in online application database left electronic PHI of 612,402 individuals accessible to unauthorized individuals over the Internet	Failure to implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule; \$1.7 million resolution
<b>University of California at Los Angeles Health System</b> (July 2012)	Employees repeatedly and without permissible reason looked at patients' electronic PHI	Failure to implement appropriate policies and procedures and conduct regular trainings; \$865,500 resolution
<b>Alaska DHSS Settlement</b> (June 2012)	Portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from vehicle of DHSS employee	Lack of safeguards; \$1.7 million resolution
<b>Phoenix Cardiac Surgery Settlement</b> (April 2012)	Physician practice posted clinical and surgical appointments for patients on an internet-based calendar that was publicly accessible	Lack of safeguards; \$100,000 resolution
<b>BCBS of Tennessee Settlement</b> (March 2012)	57 unencrypted computer hard drives stolen from leased facility in Tennessee. Hard drives included PHI of over 1 million individuals	Lack of safeguards; \$1.5 million resolution and corrective action plan

## Minimum Necessary / Need to Know

- ▶ Plan's use and disclosure of PHI is limited to the minimum necessary PHI to accomplish the legitimate business purpose
- ▶ Under HITECH, minimum necessary is “limited data set” information, unless more information is needed in compliance with the pre-HITECH standard
- ▶ Not all Plan staff will need routine access to all PHI



# Releasing PHI With An Authorization Form

- ▶ Unless allowed by the privacy rule, the Plan must obtain an individual's permission to use/disclose PHI
- ▶ Authorization: Signed form that permits use/disclosure of identified PHI; for a specific reason; states to whom PHI may be disclosed/used by; and gives an expiration date
  - Example: Some providers require an authorization form before they will release patient's health information to their employer for FMLA, workers' comp, etc.
- ▶ Plan will need a signed authorization form:
  - To use health plan PHI to administer any other benefit plan
  - To disclose PHI to non-health office staff
  - To disclose PHI to non-health carrier (e.g., to life insurer considering application)
  - To disclose PHI to employer for employment reason (e.g., to assess need for reasonable accommodations)
  - To disclose PHI for marketing purposes (e.g., to drug companies), or related to sale of PHI

# Releasing PHI For Legally Permissible Reasons

- ▶ A covered entity may legally release PHI without an authorization for certain reasons, such as:
  - For public health reasons (e.g., disease outbreaks, to track FDA-regulated products)
  - Individual may be victim of abuse, neglect or domestic violence
  - In response to a court order or subpoena
  - To the coroner, medical examiner or funeral director
  - For certain research purposes
  - To avert a serious threat to health or safety
  - To organ/tissue procurement firms to assist with transplants
  - To comply with workers' compensation laws



# Family Members and Friends

- ▶ Staff can discuss general coverage and eligibility rules with participants' family members—NOT PHI
- ▶ Generally, PHI may NOT be discussed by a covered entity with anyone outside the covered entity except the individual (not even the spouse) without an authorization form
- ▶ Individual may file a written form with the Plan to designate a personal representative with whom a covered entity can discuss PHI
- ▶ Exception: “Friends and Family Rule”
  - If the individual is present and the individual is given an opportunity to object and does not object
  - If not present or if incapacity/emergency, the Plan may use reasonable discretion to determine if disclosure is in individual's best interests (e.g., in a worksite emergency or accident)

# Personal Representatives

- ▶ The Privacy Rule requires health plans to adopt policies and procedures to recognize individuals' personal representatives (PRs)
- ▶ Personal representatives must be treated the same as the individual
  - The Plan lets individuals designate someone as their personal representative
  - The Plan has procedures to follow to verify authority and identity
- ▶ Plans must generally treat certain people as personal representatives:
  - Parents of minor children under age 18
  - Persons holding a health care Power of Attorney
  - Executors of deceased individuals
  - Persons authorized by state law to act on an individual's behalf (e.g., legal guardian, conservator, etc.)

# Privacy Official

- ▶ Under the HIPAA Privacy Rule, we are required to designate a privacy official who is responsible for the development and implementation of HIPAA privacy policies and procedures.
- ▶ Brenda Lakeman, Director of Human Resources Management and Benefits Administration, Office of Management and Budget is the Privacy Official for the State of Delaware.



# Administrative Requirements

## ▶ Policies and Procedures

- Maintain (written or electronic) policies and procedures governing how the Plan will use, disclose and safeguard PHI
- Example: “Non-health staff to have no access to PHI. Only those health staff who have need to access PHI to perform a legitimate business function relating to the health plan will have access to PHI”

## ▶ Training

- Train staff, managers, supervisors and employees on HIPAA privacy and security. Document that HIPAA training has taken place by taking attendance and having attendees certify, in writing, participation in the privacy training

## ▶ Complaints

- Develop a process for individuals to complain about policy and procedure violations

## ▶ Sanctions

- Impose sanctions against staff who do not adhere to policies and procedures

# Administrative Requirements *continued*

## ▶ Safeguards

- Adopt administrative, technical and physical safeguards for PHI

## ▶ Mitigate Harmful Effects

- Mitigate harmful effects of any non-permitted use or disclosure of PHI

## ▶ No Retaliation

- Plan cannot intimidate, coerce or retaliate against an individual exercising his/her HIPAA Privacy rights

## ▶ Maintain HIPAA Documentation

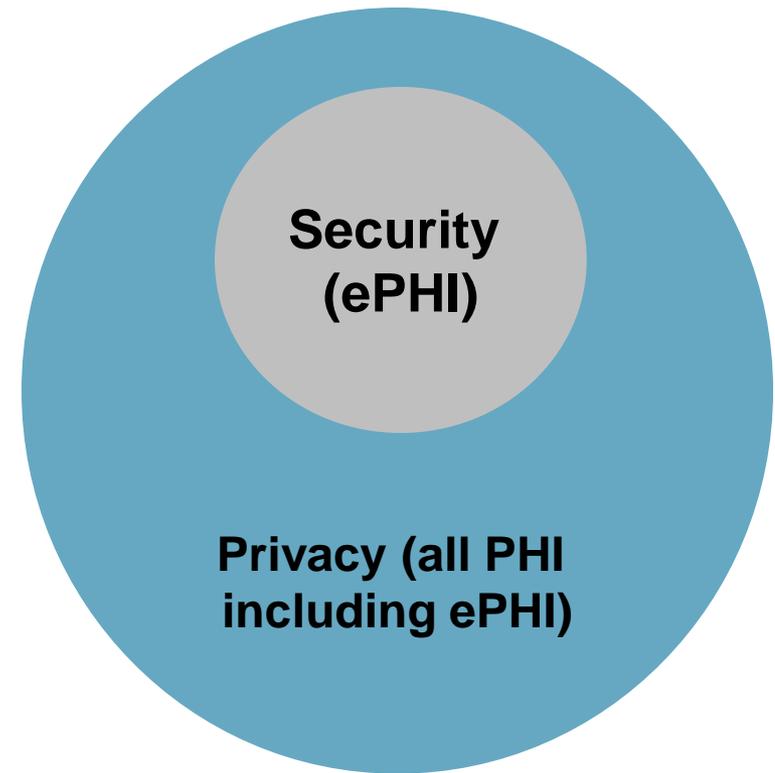
- Maintain for six years from its creation or date when it was last in effect, whichever is later

# Individual Rights

- ▶ HIPAA's privacy rule gives individuals the following Federal rights with respect to their PHI:
  - Right to receive a notice of privacy practices
  - Right to access own PHI (to inspect and copy)
  - Right to confidential communication of PHI
  - Right to restrict the use and disclosure of PHI
  - Right to amend PHI
  - Right to accounting of certain disclosures of PHI
  - Right to request that PHI be transmitted by alternative means
  - Right to complain about a HIPAA privacy violation (without repercussions)
    - Plan must develop a complaint process for individual to challenge use or disclosure of PHI (e.g., “file a written complaint with the HIPAA privacy official”)
    - Plan has an obligation to investigate all complaints and document any corrective actions taken
    - Individuals also have the right to complain directly to the Federal and/or State Secretary of Health and Human Services (HHS) regarding suspected HIPAA privacy violations

# Information Subject to HIPAA Security Rule

- ▶ Security Rule only covers **Electronic** Protected Health Information (ePHI) – PHI that is maintained or transmitted electronically
- ▶ Examples:
  - PHI sent/received via e-mail
  - PHI stored in computers, networks, and servers
  - PHI stored on portable electronic media (CDs, disks, tapes)



# HIPAA Security Requirements

- ▶ Ensure the **Confidentiality, Integrity** and **Availability** of all ePHI
- ▶ Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- ▶ Protect against reasonably anticipated uses or disclosures of such information that are not permitted under the HIPAA Privacy Rule
- ▶ Ensure compliance with HIPAA Security Rule by workforce



# The HIPAA Security Rule & Security Official

- ▶ The Security Rule requires Covered Entities to formally document their security management program, as reflected in the HIPAA Security Policies and Procedures manual
- ▶ The Rule also requires Covered Entities to assign the responsibility of overseeing the program to a Security Official. Jim Sills, the Chief Information Officer of the Department of Technology and Information (DTI) is the Security Official for the State of Delaware.
- ▶ The Security Official also manages the staff security training program:
  - HIPAA Security must be a topic within a new hire orientation
  - Periodic (refresher) HIPAA Security Training must be offered to the Plan employees at regular intervals
  - Plan employees must periodically receive security reminders

# The HIPAA Security Safeguards

- ▶ The HIPAA Security Rule is broken down into three (3) categories of Standards: **Administrative**, **Physical**, and **Technical**
- ▶ The **Administrative** Safeguards include: risk analysis and management; training programs; handling of security incidents and sanctions; account access and management; and disaster recovery planning
- ▶ The **Physical** Safeguards include: a security plan for the Plan's location(s); access to offices and professional spaces (e.g., data center) based on job needs; visitor control; workstation use and security; and disposal/re-use of hardware and media
- ▶ The **Technical** Safeguards include: systems access, protection, and monitoring; data integrity; data encryption/decryption; and transmission security



# How Do Safeguards Impact Daily Operations?

## ▶ Workstation use

- Authorized business purposes
- Perform job duties

## ▶ Workstation security (this includes systems, network, media, and portable devices that access ePHI)

- Unique user IDs
- Complex passwords that age at regular intervals
- Sessions time-out due to inactivity
- Account lockouts due to failed login attempts
- Access to ePHI according to job class
- Limited access to the Internet
- Limited access to laptops and portable devices
- Limited access to remote connections
- Monitoring of activity



# How Do Safeguards Impact Daily Operations? *continued*

## ▶ Plan Office Space

- Controlled access to areas where ePHI is stored and transmitted
- Access monitored by IDs (such as badges) and access control devices (such as swipe cards or keypads)
- Monitoring of activity
- Visitor control

## ▶ Electronic Transmissions

- Encrypted messaging
- Encrypted secure file transfer protocol (SFTP) uploads and downloads

## ▶ Disposal of Old Equipment

- Provide IT with all old equipment, media, and portable devices for proper data wiping and disposal



# Disposal

- ▶ Equipment should be wiped with Department of Defense (DOD) quality wiping software, which makes any data permanently irretrievable
- ▶ In cases where equipment will not be destroyed, such as donation to a non-profit organization, data wiping is the only acceptable option
- ▶ In cases where the equipment is malfunctioning, magnetic bulk-erasing (“degaussing”) is an acceptable option
- ▶ Data destruction, both physical and electronic, is covered in detail in the document for NIST standard 800-88
- ▶ Once the equipment has been wiped in accordance with NIST guidelines, it can be discarded or recycled

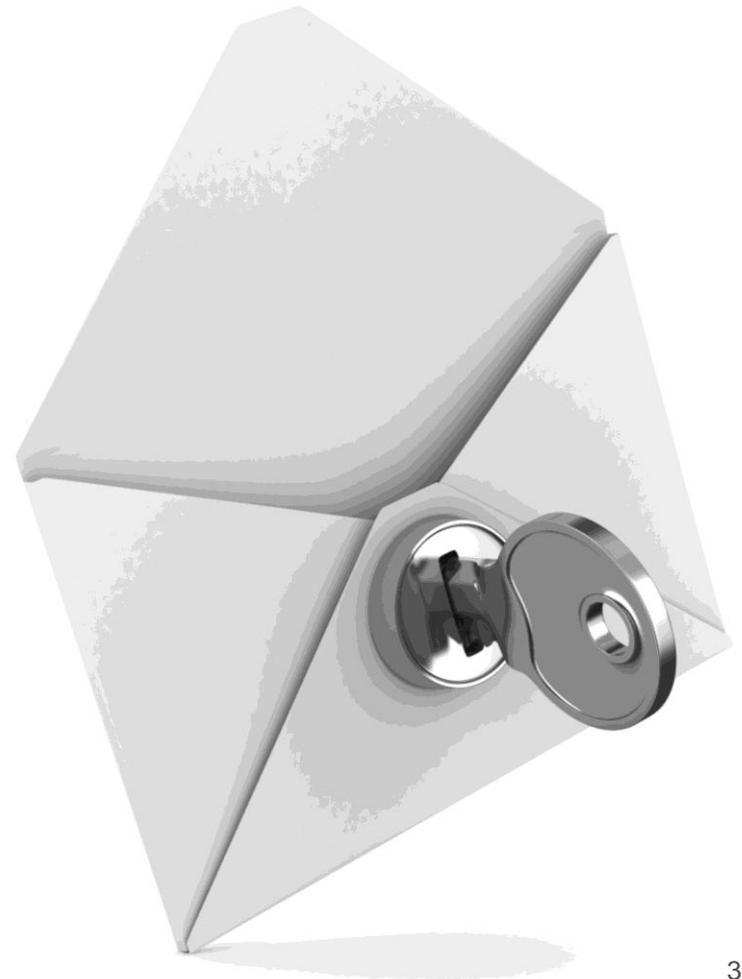
# HITECH Safe Harbor Guidance

- ▶ There are two exclusive methods to make ePHI unusable, unreadable or indecipherable to unauthorized individuals (i.e., to make it secure) and therefore avoid the breach notification requirements:
  - Encryption
    - Applies to data in motion (e.g., e-mail sent via Ironport, online transmissions, secure websites, etc.)
    - Applies to data at rest (e.g., backups tapes, flash drives, databases, laptops, PDAs, etc.)
  - Destruction
    - Electronic equipment, portable devices, and media must be cleared, purged or destroyed consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88 such that ePHI cannot be retrieved



# E-mail and Encryption

- ▶ Determine if e-mail is a permissible means of transmitting sensitive info
- ▶ Determine when encryption is required
- ▶ Don't forward e-mail trains with embedded data
- ▶ Make sure recipient's e-mail address is valid before clicking "send"
- ▶ Watch out for e-mail sensitive auto-complete feature
- ▶ Don't put passwords in the text of an e-mail message when sending an encrypted file attachment



# Breach Notification

- ▶ Covered entities (including group health plans) must notify individuals when there is a breach of “unsecured PHI”
- ▶ Applies to all PHI (i.e., oral and paper, not just ePHI)
- ▶ Effective for incidents occurring on or after September 23, 2009
- ▶ Also requires notice to the State and/or Federal HHS and perhaps the media
- ▶ Business associates must notify the covered entity



## Breach Notification *continued*

### To determine if notice is required:

- ▶ Was the PHI “unsecured”?
- ▶ Was the privacy and/or security rule violated?
- ▶ The final rule states that PHI used or disclosed in violation of the Privacy Rule is presumed to be compromised, and therefore, requires breach notification. However, this presumption may be overcome if the Plan or business associate can show “there is a low probability that the information has been compromised”
- ▶ Does an exception apply (e.g., certain limited, inadvertent conduct)?
- ▶ If notice is required, it must be issued without “unreasonable delay”—no later than 60 days after breach discovery

## Breach Notification *continued*

- ▶ Individual notice: To each affected individual, no later than 60 days after discovery of breach, via USPS first class mail; if urgent, may also provide by telephone (following up with written notice)
- ▶ To prominent media outlets: If breach affects > 500 people
- ▶ To Federal HHS #1: If 500 or more people, notify HHS at same time as affected individuals; use HHS-approved e-form (HHS posts these breaches on its website)
- ▶ To Federal HHS #2: If < 500 people affected, keep a log and report breaches annually, no later than 60 days after end of year, using HHS e-form

# Examples of Breaches

Entity	Incident	Result
Henry Ford Health System in Detroit, MI (May 2013)	Old X-rays received between 1996 and 2003 were stolen from a contracted storage warehouse; 15,417 patients were affected	Storage warehouse employee was arrested with others being investigated – pending resolution
Clark Memorial Hospital in Jeffersonville, IN (July 2013)	A contractor that processes and mails billing statements sent statements to the wrong name and address; 1,087 patients were affected	Contractor quickly identified and fixed the cause of the processing error, but the hospital is assessing its current relationship with the vendor
Oregon Health & Science University – OHSU (July 2013)	OHSU health information was stored on an internet-based email and/or document storage service, with which OHSU does not have a business associate agreement; 3,044 patients were affected	All OHSU patient health information found on the internet-based service has been removed, and all residents have been re-educated about the critical importance of using OHSU-approved tools for securely sharing and updating patient information. A 1-800 number has been established to answer patient questions and concerns
MO HealthNet, a Medicaid program serving St. Louis and more than 50 counties in Missouri (June 2013)	The program learned in June 2013, that a software programming error by contractor resulted in correspondence to the beneficiaries being sent to the wrong address between Oct. 16, 2011 and June 7, 2013	The program is offering affected beneficiaries two years of credit and identity theft protection services

# How Can I Protect PHI and Enforce the HIPAA Regulations?

- ▶ Do NOT share your password with anyone!
- ▶ Lock file cabinets that contain sensitive information
- ▶ Think before you click “send”
- ▶ Use secure email!
- ▶ Keep it “quiet”



# How Can I Protect PHI & Enforce the HIPAA Regulations? *continued*

- ▶ Don't store PHI on laptops, but if you do, ensure that laptop is encrypted to avoid breaches if stolen
- ▶ Don't access emails or documents containing PHI from mobile devices (PDA's, Cell Phones, Blackberries, etc.)
- ▶ Shred trash containing PHI instead of throwing away/placing in recycle bin
- ▶ Ensure that electronic media containing PHI is erased/sanitized before reuse
- ▶ **Employees should be referred directly to the Statewide Benefits Office for assistance with all inquiries and/or questions involving PHI. HR personnel and supervisors should not act as a "middle" person!**

## Resources & New Online HIPAA Seminar!

- ▶ Updated HIPAA Privacy & Security Manuals are posted on the secure ben rep site under “HIPAA”. The user ID is “benrep” and the password is the 8 digit date you are logging onto the site (i.e., 10032013)
- ▶ The Statewide Benefits Office and HRM’s Training Division worked together to create an online HIPAA Privacy & Security seminar that will be available by the end of October.
- ▶ Questions regarding HIPAA should be directed to
  - Leslie Ramsey
  - Statewide Benefits Office
  - 500 W. Loockerman Street
  - Suite 320
  - Dover, DE 19904
  - Tel: (302) 739-8331
  - Fax: (302) 739-8339
  - Email: [Leslie.Ramsey@state.de.us](mailto:Leslie.Ramsey@state.de.us)

# Questions?

