HIPAA Privacy & Security Overview for the Health Insurance Professional

1 Hour of CE Credit

Course Number 382755

Presented By:
Dorothy Cociu, RHU, REBC, GBA, RPA

President, Advanced Benefit Consulting & Insurance Services, Inc.

V.P. Communications, OCAHU

Advanced Benefit Consulting

What's All This Talk About Privacy?

- The privacy issue stems from recent state and federal-level actions to protect the privacy of consumers' personal information.
- All of the recent privacy measures impact insurance producers, providers, and the health insurance industry.
- Privacy is a very confusing topic, especially since it's really divided into two parts on a federal level, and many state laws also come into play.
- **Now, with HITECH, our daily work lives have changed, and we need to be prepared!**
  - *Smart Phones, Tablets, Portable Devices – A Whirl-Wind of Technology Rules!*

Privacy Laws - Summary

- Federal Laws
  - HIPAA Medical Records Privacy
  - Gramm-Leach-Bliley Act (GLBA) Financial Records Privacy
  - ARRA Creates HITECH Changes to HIPAA Privacy & Security
- State Laws (California)
  - *California Constitution* contains provision guaranteeing the right to privacy.
  - *Insurance Information and Privacy Protection Act* (California Ins. Code 791-791.27) applies to "insurance transactions" by "insurance institutions, agents or insurance-support organizations." Includes notice and authorization procedures. Needed in conjunction with GLBA.

Privacy Laws - Summary

- State Laws (California - Continued)
  - *California Department of Insurance's Final Regulations* (title 10, 26891-2689.24 of the Cal. Admin. Code) for GLBA 15 USC 6801-681
  - *The Confidentiality of Medical Information Act* (Cal. Civ. Code 56-56.37)
  - *Confidentiality of Social Security Numbers* (SB 168), Cal. Civ. Code 1798.85. Prohibits any individual or entity (not including a state or local agency) from using a person's SS# in certain designated circumstances. CA legislature passed and governor recently signed SB 1730 (now chaptered at 786) which amends 1798.85
  - *Health Care Service Plans*, Cal. Health & Safety Code 1364.5 & 1374.8. Specific laws for HMO's.
  - *Office of Privacy Protection*, Cal Bus. & Prof. Code 350-352
  - *Office of HIPAA Implementation*, Cal Health & Safety Code 130300-130317

California Privacy Laws - Continued

- Data Breach Notification Law (7-1-03)
  - Must provide notice "to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person)
  - Not required to send to govt. SB 20 would have required notice also be sent to state Attorney General
- Information Practices Act of 1977
  - CA Code Sections 1798-1798.78; Applies to Gov't Entities only
- Customer Records
  - Cal. Civ Code 1798.80-1798.84. Document shredding law. Applies to a "business with customer records" (written broadly) containing "personal information" and sometimes to broader categories of records, that could include employment and health records. Under the law, the following applies: Destruction, Security, Data Breach, Direct Marketing (see handout)

New California Privacy Law Effective January, 2020

- The California Consumer Privacy Act (CCPA)
- Signed into law June, 2018
- Effective for the most part Jan. 1, 2020
- Extends the protections and rights for California residents (defined later)
- Applies to businesses that both collect and process the Personal Information of CA residents and do business in the state of CA with $25 million in revenue
- Requires notices, web postings, etc.
- Vendors (like agents) may be asked to complete CCPA requirements (most similar to HIPAA)

Basic Concepts & How to Apply Them in the Workplace

- What does the HIPAA Privacy Rule Do?
- Generally, what does the HIPAA Privacy Rule Require the Average Covered Entity or Business Associate to Do?
- Key Terms & Concepts
- What Role Does the HR Dept of Your Clients Play?
- What Role Does the Agent Play?

HIPAA Medical Records Privacy – Summary Overview

- Privacy Rule Creates a "Federal Floor" of Privacy Protections
  - First comprehensive federal health privacy protections
  - "More stringent" state privacy protections remain in force
- Two Key Privacy Rule Goals
  - Provide strong Federal Protections for Privacy Rights
  - Preserve Quality of Health Care

What Does the HIPAA Privacy Rule Do?

- Most health plans and providers must comply with the new requirements by April 14, 2003 (small plan exception)
- For the first time the Privacy Rule creates national standards to protect individual's medical records and other personal health information
  - Gives patients more control over their health information
  - Sets boundaries on the use and release of health records
  - Establishes safeguards that providers and others must achieve to protect the privacy of health information
  - Holds violators accountable with civil and criminal penalties
  - Strikes a balance when public responsibility supports disclosure of some forms of data

OCR HIPAA Privacy, December 3, 2002

Generally, What Does the HIPAA Privacy Rule Require the Average Provider or Plan/Covered Entity to Do?

- Notify patients about privacy rights and how their information can be used
- Adopt and implement privacy procedures for its practice, hospital, or plan
- Train employees so that they understand the privacy procedures
- Designate an individual to be responsible for implementation
- Secure patient records containing individually identifiable health information
  - Administrative, physical and technical security
  - Additional levels of security now needed for paper and electronic health information

OCR HIPAA Privacy, December 3, 2002

Generally, What Does the HIPAA Privacy Rule Require the Average Insurance Agency or Plan/Covered Entity to Do?

- Notify your employees about privacy rights and how their information can be used (HR NPP)
- Adopt and implement privacy procedures for its practice, hospital, or plan (HR/Managers/Producers/Customer Service/PWG/Admin)
- Train employees so that they understand the privacy procedures (train company needs-specific)
- Designate an individual to be responsible for implementation

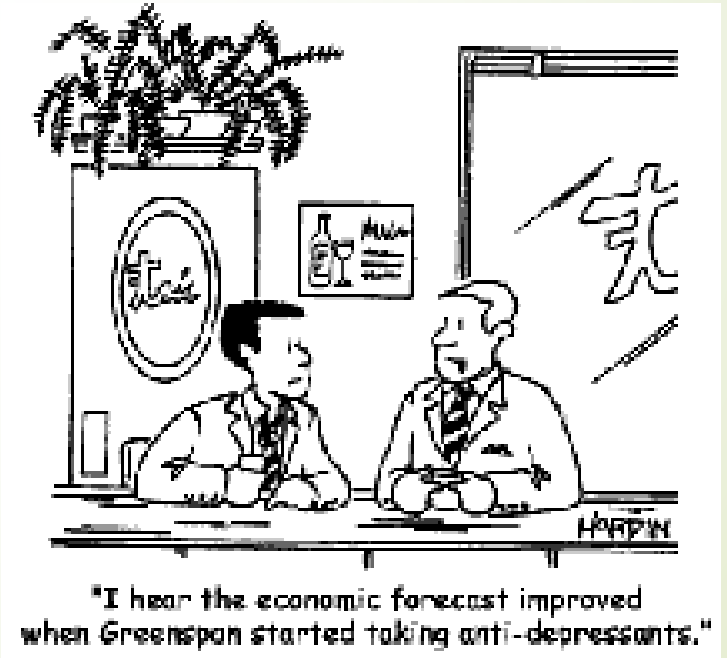
(your privacy officer, security officer, PWG team)

- Secure employee records containing individually identifiable health information
  - Administrative, physical and technical security
  - Additional levels of security now needed for paper and electronic health information

OCR HIPAA Privacy, December 3, 2002

Key Terms & Concepts

- Protected Health Information
- Covered Entities
- Permitted Uses
- Business Associates
- TPO



Definition – Protected Health Information (PHI)

- Individually Identifiable Information
- Held or Disclosed by a Covered Entity
  - Electronically (any electronic files containing PHI; includes email and smart phones)
  - Paper (e.g. enrollment form, EOBs, physicals)
  - Orally (e.g. claims issues)
- De-Identified Health Information is NOT PHI

Protected Health Information

- Individually Identifiable Health Information
  - Relates to an individual's past, present or future physical or mental health condition, to the provision of health care to that person, or to the past, present, or future payment of that person's health care
  - Specifically identifies individual or reasonable belief that individual may be covered
- Created or Received by a Covered Entity
  - Not limited to information electronically stored or transmitted

EPHI

- Electronic PHI is now referred to as EPHI
- ARRA and HITECH bring new meaning to protecting EPHI!

Examples of PHI and EPHI In Your Office?

- What are examples of PHI and EPHI you have in your office that meet the definitions discussed?

What Role Does the Human Resources Department of Your Employer Clients Play?

- Privacy Officer & Privacy Work Group Designations
- Training and it's Importance
  - Who, what, why, how long?
  - Tracking training sign-in sheets, tests (if required), new hire training, re-training
- Development of Policies & Procedures
  - Privacy Work Group Policies
  - HR Policies
  - Electronic Policies
  - Clinical (if applicable) Policies
  - General Staff Policies
  - General Firewalls

What Role Does the Insurance Agent Play?

- As an insurance agent, you are a Business Associate to Your Clients, who are covered entities if they sponsor a group health plan
- As such, you must comply with all of the same HIPAA Privacy & Security elements as the covered entity
- If you have employees and sponsor a group health plan, you are also a covered entity, and must do not only the BA functions but also the covered entity/HR functions for HIPAA Privacy & Security
- You must protect all client data, with administrative, physical and technical security
- You must be trained and train your staff

What Role Does the Insurance Agent Play?

- Privacy Officer & Privacy Work Group Designations
  - Who's Responsible for Forms, Notices, Training, Etc?
  - Do you have an Agency Set of HIPAA Policies, HR Policies, etc.?
  - Do you sponsor a group health plan? If so, you're a covered entity, so all applies.
    - HR & Agency Applications
    - What Firewalls do you have in place?
- Training and it's Importance
  - Who, what type, how often?
  - How do you track and maintain records?
  - Are all of your ducks in a row for a potential audit?
- Development of Policies & Procedures for the Agency
  - Sales
  - Service Team/Account Management
  - Open Enrollment Team
  - Recordkeepers/clerical staff

Core Privacy Requirements

- Use & Disclosure Rules
- Minimum Necessary
- Individual Rights & Privacy Notices
- Administrative Safeguards

Permitted Uses for PHI

- Treatment
- Payment
- Health Care Operations (auditing, credentialing, obtaining reinsurance, etc)
- Certain **Public Policy Exceptions** (partial list)
  - Most common Workers Comp (authorization still encouraged to protect covered entity), Matters of Public Health and Safety, Judicial and Administrative Proceedings from the court system (see next slide on Subpoenas)
- *Other uses (other than TPO) require individual authorizations*
- *Note: California Law requires authorizations and wipes out federal TPO exception in many cases*

Minimum Necessary

- What does Minimum Necessary Mean to an Insurance Agent?
- What does Minimum Necessary Mean to your Employer Clients?

Minimum Necessary

- The HIPAA Privacy Rule states that you can only provide the **Minimum Amount of Information Necessary to Get Today's Job Done**
- *New audit protocols are requiring a written list of minimum necessary definitions/standards for all job titles involved with the handling of PHI, ePHI, and related*
  - Identify job functions, evaluate minimum necessary access for each, why and how to protect – for each job!
  - Be sure to have these in writing!

Disclosure of PHI

- As required by HHS regs
- Individual Authorizes
- Treatment, Payment, Plan Operations
- "Minimum Necessary" Rule
  - Auditors Taking it Seriously! Newer rules for minimum necessary by job function!
- Exception to Providers for Treatment

Risk Analysis

- It is the responsibility of every covered entity and business associate to conduct regular risk analyses to address the risks and vulnerabilities of the organization regarding the PHI it is obligated to protect
- *Numerous cases which resulted in CMPs or Settlements have included failures to conduct one or more risk analyses*
- Should be done on a regular basis; not just once
- Needed for HIPAA Privacy & HIPAA Security
- HHS has a new internal security risk assessment tool (SRA Tool) available to assist

Insurance Industry – Business Associate Functions

- Execute compliant BA Agreements with employer clients if your clients haven't provided you with their BA Agreement (they are the covered entity & you are the BA)
- You are a BA of carriers/TPAs (agents) or employers
- Protect all client data while quoting, servicing, claim handling
- Provide E-Security for all devices, emails, phones, etc.
- Remember, as a Business Associate, you are just as liable and responsible as a health care provider!

Administrative, Physical & Technical Security

- Types of Administrative Security
  - Forms, Policies, Procedures, Training & Training Records, Etc.
- Types of Physical Security
  - Locks, Barriers, Alarm Systems, Etc.
  - What is the difference between single and double locks?
- Types of Technical Security
  - IT Department & It's Role
  - Levels of Authority, Permissions
  - Password Protection and Encryption
  - Remote Wipe & Other Technical Methods for Protecting Data

Core Privacy Requirements

- Use and Disclosure Rules
  - Minimum necessary standard (definitional changes 02-2010)
    - (MINIMUM NECESSARY TO GET TODAY'S JOB DONE!)
  - Required disclosures
    - Disclosures required to be made to individuals who exercise their individual rights
    - Disclosures must be made to DHHS for enforcement and compliance review actions
  - Use or Disclosure Pursuant to Authorization
    - Authorizations must be voluntary and informed, and must meet requirements set forth in regulations
- Individual Rights and Privacy Notice
  - Individual Rights- Inspect and make copy of PHI, amend or correct PHI, obtain accounting of disclosures of PHI, receive notice of privacy practices, request additional restrictions (listed in NPP)
  - Privacy Notice- Covered entities required to provide individuals with a notice of privacy practices

Core Privacy Requirements

- Administrative Safeguards
  - Covered entities must take the following actions to protect the privacy of PHI
    - Designate a privacy officer responsible for the development and implementation of privacy policies and a contact person for receiving complaints and providing additional information
    - Train workforce on privacy policies and procedures
    - Establish appropriate safeguards for protecting the privacy of PHI
    - Create a process to lodge complaints and a system for handling, and keep a record of complaints and their resolutions
    - Design a system of written disciplinary rules for persons who violate the privacy rules
    - Mitigate any harmful effects known resulting from improper use of PHI
    - Refrain from intimidation or retaliation for exercising rights
    - Not requiring individuals to waive rights
    - Implement policies and procedures designed to comply with the privacy standards
    - Documentation policies and procedures and retain for a minimum of 6 years (7 years in CA)

Covered Entity Basic Firewalls

- Arrange computers so that passersby cannot see the screens
- Paper shredders near copy machines; cross-cut for mental health
- Mental Health Double Lock-downs required
- Restrict fax machines and designate privacy office/confidential fax areas
- In-baskets should be protected
- Signage
- Use restricted area signs or barriers if necessary to keep private records private
- Confidential Communication Designated Areas
- Relocate personnel if necessary
- Lock up files with PHI; again, double-lock mental health records
- Key Inventory – Re-assess who has access
- Update or increase alarm and other security features

Real World Simple & Inexpensive Firewalls That Work

- Providers - Common Therapy Areas – Fans, Music or TV playing to muffle sound (for confidential communications)
- Patient Rooms in Dr's offices or hospitals – can others see or hear discussions, have access to patient charts? Locked cabinets inside patient rooms, color codes and de-identifiable charts can help; nursing procedures to protect patient data
- Agents – OE meetings – announce health personal information should be discussed in private after OE Meetings
  - Ask for a private room for one-on-one claims assistance, health discussions
- Moving in-baskets away from arms reach of walkways and common areas
- Barricades, counters, private offices
- Escort only through common areas
- Visitor Name Badges, Sign-In
- Signage – restricted access
  - Don't need expensive signage

Privacy Notices

- Distribute at Enrollment and at least Every Three Years
- No later than compliance date of health plan
- Add to SPD?
- Amend as Provisions Change (within 60 days of change)
- Re-Distribute New Notices
- Provider requirements - no later than the date of first service delivery, or as soon as reasonably practicable after emergency, acknowledgement of receipt, post notice in clear and prominent location
- Add new Breach and Genetic Information language required under Final Rule; effective 3-23-13, must comply by 9-23-13!

Who Handles Your Complaints?

- Human Resources Complaints (employees)
- Clinical/Agency Complaints
- Do you have a process and compliant forms and resolution forms?
- What do you do if a call comes in from a government official about a compliant? Is your staff trained to handle this?

Public Policy Exceptions

- For Public Policy Exceptions, you can generally throw the Privacy Rule out the Window….

Public Policy Uses and Disclosures

- Public Policy Purposes
  - As required by law
  - For public health
  - About victims of abuse, neglect or domestic violence
  - For health oversight activities
  - For judicial & administrative proceedings
  - For law enforcement purposes
  - About decedents (to coroners, medical examiners, funeral directors)
  - For cadaveric organ, eye or tissue donations
  - For research purposes
  - To avert a serious threat to health or safety
  - For specialized gov't functions (military, veterans, national security, protective services, State Dept, correctional)
  - For workers' compensation

HITECH Overview

- Mobile Device and Encryption Overview
  - Encryption
  - Remote Wipe
  - Wipe before giving to friend of family member
  - Passwords (strong) and time-out features
  - Secured Home Networks – 2 networks are best
  - Avoid Public Wifi if you are a Business Associate or you maintain PHI anywhere, even your email!
    - VPN connections are available at reasonable pricing! Connect securely from anywhere!
- Smart Phones (too smart?) – Beware of texting
- Tablets
- Laptops
- USB Drives, CD's
  - Close off USB ports?

Electronic Security

- Electronic Security is one of the most important elements that an insurance agency should be concerned with!
- Review of your desktop computers, laptops, tablets, phones, is essential.
- A large percentage of the CMP's and settlements with HHS/OCR have been because of the failure of covered entities and business associates to properly protect electronic data.
- Encryption is easy, inexpensive and necessary, yet many covered entities and business associates fail to implement it!
- Do you have email forwarded to your cell phones? Are those phones properly encrypted (or just password protected – there is a difference!)? What kinds of apps are you downloading on phones that are being used for business?

Permitted Uses & Disclosures

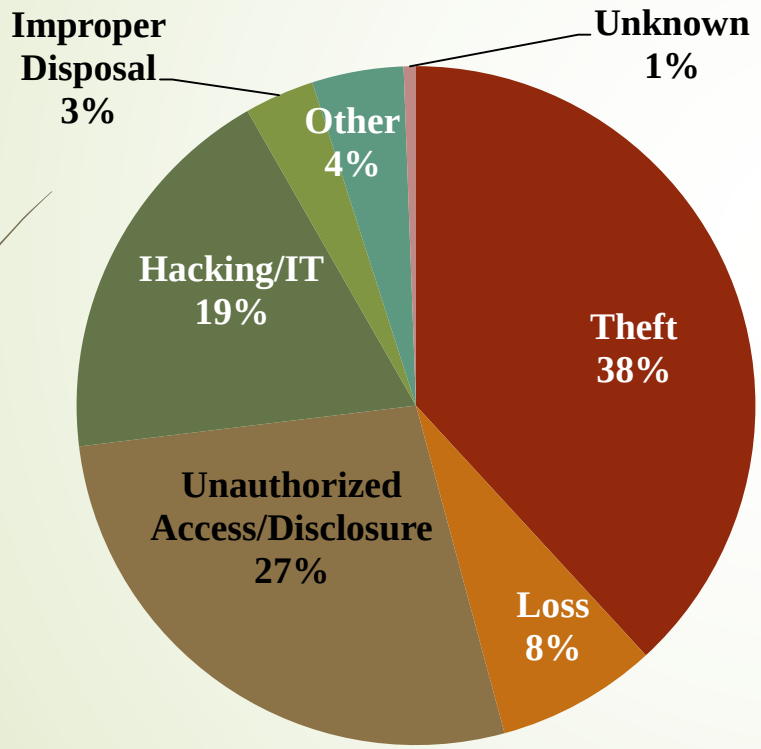
- Treatment, Payment & HealthCare Operations
- Public Policy Exceptions
- Subpoenas

Subpoenas –HHS Clarification

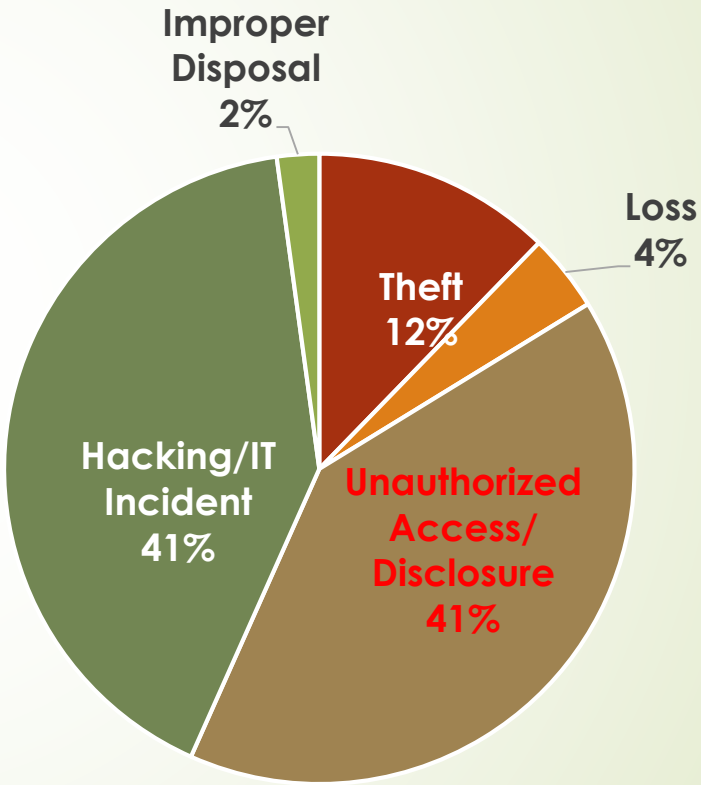
- A covered health care provider or health plan may disclose protected health information required by a court order, including the order of an administrative tribunal. However, the provider or plan may only disclose the information specifically described in the order.
- A subpoena issued by someone other than a judge, such as a court clerk or an attorney in a case, is different from a court order. A covered provider or plan may disclose information to a party issuing a subpoena only if the notification requirements of the Privacy Rule are met. Before the covered entity may respond to the subpoena, the Rule requires that it receive evidence that reasonable efforts were made to either:
  - notify the person who is the subject of the information about the request, so the person has a chance to object to the disclosure, or to
  - seek a qualified protective order for the information from the court.

HIPAA Breach Highlights thru 9/30/18

500+ Breaches by Location of Breach



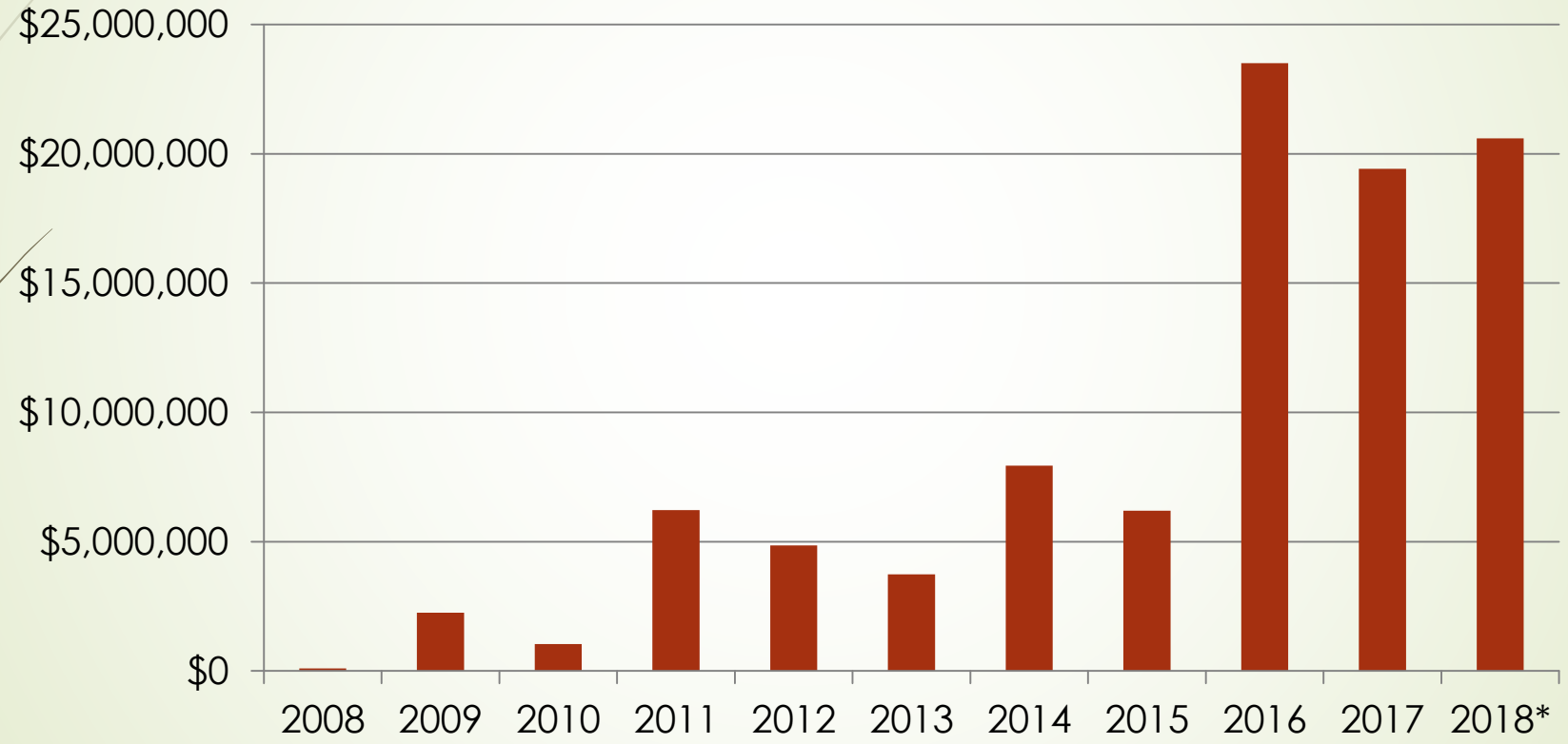
Sep 23, 2009 through Dec 31, 2017



January 1, 2018 through September 30, 2018

Serena Mosley-Day, OCR

HIPAA Resolution Agreements & Civil Monetary Penalties



56 settlements and 3 civil money penalties through Oct 15, 2018

*Year To Date

Serena Mosley-Day, OCR

HIPAA Enforcement

Settlements Since 2017 OCR NIST Conference ~

Dec. 2017	21st Century Oncology	$2,300,000
Feb. 2018	Fresenius Medical Care North America	$3,500,000
Feb. 2018	Filefax	$100,000
Aug. 2018	Boston Medical Center	$100,000
Sep. 2018	Brigham and Women's Hospital	$384,000
Sep. 2018	Massachusetts General Hospital	$515,000
Oct. 2018	Anthem, Inc.	$16,000,000

Total $22,899,000 collected 10-17 to 10-18

Serena Mosley-Day, OCR

Recent Enforcement Actions 2018-2019

When	Who	How Much
9/2018	Brigham & Women's Hospital (ABC case)	$384,000
9/2018	Mass General Hospital (ABC Case)	$515,000
9/2018	Advanced Care Hospitalists (No BA Agreement)	$500,000
10/2018	Allergy Associates of Hartford (Complaint w/ provider – provider talked to media	$125,000
10/2018	Anthem – Largest breach in US History	$16,000,000
11/2018	Pagosa Springs Medical Center	$111,400
12/2018	Cottage Health – 2 breaches, both servers on internet	$3,000,000
4/2019	Touchtone Medical Imaging	$3,000,000
4/2019	Medical Informatics Engineering	$100,000
9/2019	Bayfront Health St. Petersburg	$85,000

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Serena Mosley-Day, OCR, 10-17-19

Further Training (outside of this 1 Hour CE class) is necessary!

- This class is a one-hour CE program. It is an overview only.
- This is only one of 3 classes (4 hours total) of CE available to local chapters and CAHU that have been created.
- HIPAA Enforcement details are covered in a separate CE class.
- We highly encourage PRIVACY OFFICER TRAINING, which is much more extensive, for insurance agents as well as employer clients, which are covered entities.

Questions?

- I'm happy to answer questions….
- Copies of today's slides can be found on the OCAHU website

Disclaimer

- The information contained herein is not intended to be legal advice. Advanced Benefit Consulting has gathered public information to present to OCAHU and CAHU members to assist them with their HIPAA Compliance. Situations vary. We always recommend that you consult a qualified attorney as situations vary.

To Contact Today's Speaker

- Dorothy Cociu is the president of Advanced Benefit Consulting, Anaheim, CA
- She can be reached at 714 693-9754 x 3 or by email at dmcociu@advancedbenefitconsulting.com

Advanced Benefit Consulting