BEFORE AND AFTER:

DATA BREACH PREVENTION AND RESPONSE PREPAREDNESS CONSIDERATIONS FOR HEALTH CENTER LEADERSHIP

Tera T. Hambrick, JD

Tennessee Primary Care Association
Annual Leadership Conference
September 30, 2016

DISCLAIMER

The information and materials provided in this training were prepared by Tera T. Hambrick, JD. Such content is not legal advice. Participants are encouraged to seek legal advice or other assistance from their preference of competent professionals.

Opinions expressed in the presentation or written materials are solely those of the author/presenter and not necessarily the views of any other person or organization, including, but not limited to, Matthew Walker Comprehensive Health Center, Inc., the Tennessee Primary Care Association, and the National Association of Community Health Centers.

In the News . . . the Breach Epidemic . . .

- **Seagate** (March, 2016) – W-2 Forms for all current and past employees were compromised through a "phishing" scam perpetrated against an employee
- **ADP** (April, 2016) – approximately 12 clients of the major payroll processing company had its employees' W-2s leaked to an unauthorized party when unsecured registration codes and personal information was used to exploit its online portal registration features
- **IRS** (February, 2016) – massive data breach first reported May, 2015 expanded to reflect that 700,000+ individuals' SSNs and other information were accessed through the IRS's "Get Transcript" online functionality using personal information hackers likely obtained through breaches of IRS-approved tax preparer or other online accounts
- **FBI** and **Dept. of Homeland Security** ("DHS") (February, 2016) – hackers purportedly accessed and dumped nearly 30,000 FBI and 9,000 DHS employees' names, titles, and contact information and claimed to have access to an additional 200GB of files belonging to the federal agencies

In the News . . . the Breach Epidemic . . .

- **Office of Child Support Enforcement** (WA, April, 2016) – intruders believed to be using a key from a disgruntled former employee stole a laptop and portable hard drive from its offices containing the personal information (SSNs, DOBs, addresses, phone numbers) of 5M individuals
- **Democratic National Committee** ("DNC") (July, 2016) – intrusions resulted in leaked DNC e-mails and similar intrusions occurring around the same time resulted in access to an analytics program server used by the Hillary Clinton Campaign and the Democratic Congressional Campaign Committee
- **AZ and IL Voter Registration System Databases**

  (June and July, 2016, respectively) – intrusions into the state systems resulted in theft of the username and password for one election official in an AZ county and retrieval of a "small percentage" of the IL voter registration records

In the News . . . the Breach Epidemic . . .

- **LinkedIn** (May, 2016) – breach first uncovered during 2012 affected more data than originally suspected. As of 2016, it is suspected that 100M users' data, including e-mail addresses and passwords, were obtained through hacking and allegedly a hacker identifying himself/herself as "Peace" attempted to sell the data
- **Poway, CA Unified School District** (May, 2016) – through its outside counsel, responded to a public records request and accidentally sent the requesting parent and school system committee member data for 36,000+ children, some of which is protected from disclosure under FERPA. Including the data of the children's parents, the breach affected approximately 70,000 individuals. The data included children's names, nicknames, addresses, phone numbers, hearing and vision exam results, dates of birth, language fluency, academic test results and occupation of parents.
- **Verizon Enterprise Solutions** (March, 2016) – attacker exploited a security vulnerability on its enterprise client portal and obtained basic contact information on enterprise customers.

In the News . . . the Breach Epidemic . . .

- **South Sunflower Co. Hospital** (February, 2015) – MS merchant sent a package with packing material made from the hospital's shredded documents containing names, diagnoses, SSNs and DOBs of 19,345 individuals
- **Kaiser Permanente** (February, 2015) - documents containing PHI of 3,959 patients spilled onto the highway while being transported to storage
- **Hawkins Mental Health Center; Los Angeles Co. Dept. of Health Services** – 880 patients' confidential information found and seized by law enforcement during execution of a search warrant at the home of the County employee;
- **Community Mercy Health Partners** (OH) - Invoices for about 2,000 patients containing names, addresses, diagnosis and procedural codes, service dates and locations, and account balances were inadvertently sent to incorrect people (February, 2015) and, in a second incident, its contractor inadvertently disposed of 113,000 paper medical records in a public recycling bin (November, 2015)

In the News . . . the Breach Epidemic . . .

- **Rite Aid and Keystone Pharmacies** (April, 2015) – Baltimore pharmacies were broken into during several days of unrest and 2,345 filled prescriptions and 150 prescription bags with patient information on them were taken
- **Bixby Medical Center and Herrick Hospital** (both MI facilities within Ohio-based ProMedica's network) – seven employees improperly accessed 3,472 patients' medical records

In the News . . . the Breach Epidemic . . .

- **21st Century Oncology** (FL, October, 2015) – hackers infiltrated the cancer care provider's database accessing names, SSNs, physician names, diagnoses, treatment data, and insurance information for patients across all 50 states
- **Newkirk Products, Inc.** (subsequently acquired by Broadridge Financial Solutions, Inc.) (NY, May, 2016) – vendor of ID card printing and other services for health plans discovered unauthorized access to its server granting the hacker potential access to names, addresses, member and group ID numbers, PCP names, DOBs, and names of dependents for 3.3M members of its customer health plans
- **University Gastroenterology** (RI, July, 2016) – unauthorized individual gained access to practice's electronic file storage system and encrypted the data comprised of 14,000 patients' information (names, SSNs, DOBs, and other data)
- **Kansas Heart Hospital** (May, 2016) – paid ransom to hackers who launched a ransomware attack on the hospital's files; however, the hackers demanded more money rather than immediately restoring the hospital's access to the files

It ***CAN*** Happen to CHCs!

- Vendor's technical error in a mail merge process led to CHC's data breach resulting in improper disclosure of patients' treatment relationship with a physician assistant formerly associated with the CHC

  (ME, October, 2015);
- Identity theft ring accessed names, DOBs, and SSNs of nearly 8,000 patients of CHC (FL, July, 2014)
- Medical Informatics Engineering, which offered an EHR as well as a patient portal product and service through NoMoreClipboard, was hacked compromising the data of 239 health care provider clients, including CHCs such as Grace Community Health Center (KY) and an Indiana-based CHC. Affected data potentially included names, telephone numbers, mailing addresses, usernames, hashed passwords, security questions and answers, spousal information (names and potentially DOBs), e-mail addresses, DOBs, SSNs, lab results, health information, health insurance policy information, diagnoses, disability codes, doctors' names, medical conditions, and children's names and birth statistics. (May, 2015)
- CHC and its CEO filed suit against its former IT Director alleging that he improperly removed computer equipment and delivered a hard disk to the Attorney General claiming that the hard disk contained patient information; withheld vital encryption information and passwords; stole encrypted e-mails and posted them on YouTube©; and harassed and threatened the CEO and the CEO's wife and children (CT, June, 2014);

By the Numbers:

- 2015: According to the Office of Civil Rights ("OCR"), 253 breaches were reported that affected 500 or more individuals with a combined loss of more than 112M records
- 2015: Four of the Five largest health network breaches in history occurred
- Fines — since authorized by federal statute, have been minimally imposed – less than 40 times

Top 10 Healthcare Data Breaches 2015

Organization	Records Breached	Type of Breach
Anthem	78,800,000	Hacking / IT Incident
PREMERA BLUE CROSS	11,000,000	Hacking / IT Incident
Excellus BlueCross BlueShield	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
mie Medical Informatics Engineering	3,900,000	Hacking / IT Incident
CareFirst BlueCross BlueShield	1,100,000	Hacking / IT Incident
DMAS	697,586	Hacking / IT Incident
Georgia Department of Community Health	557,779	Hacking / IT Incident
BEACON HEALTH SYSTEM	306,789	Hacking / IT Incident
DJO GLOBAL	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)

http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#470e9b0a7fd5

By the Numbers:

- **$5.55M Settlement and Corrective Action Plan** - OCR announced on August 4, 2016 the largest government settlement with a single covered entity for a HIPAA violation in the amount of $5.55M. The covered entity is Advocate Health Care Network.
- Multiple potential violations involving electronic protected health information
- OCR began investigation of Advocate after receiving 3 breach notification reports within 4 months in 2013
  - 4 unencrypted laptops stolen (approx. 4 million patient records)
  - Breach to Business Associate's network (approx. 2,000 patients affected)
  - Breach to Advocate's ePHI system (approx. 2,000 patients affected)

By the Numbers: Costs

The source of this data is the 2016 Cost of Data Breach Study: United States conducted and published by Ponemon Institute, LLC during June, 2016.

- $7.01M is the average total cost of data breach
- $221 is the average cost per lost or stolen record, of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees
- Healthcare industry has a per capita data breach cost substantially above the overall mean of $221
- Incident response plans and teams in place, extensive use of encryption, employee training, BCM involvement or extensive use of DLP reduced the cost of data breach
- Data breaches due to third party error, extensive cloud migration or a rush to notify increased the cost

What is a breach?

Other laws applicable to disclosures of identifiable protected information often define "breach" differently or more broadly. For purposes of this discussion, we will primarily address PHI and rely on the HIPAA definition of "breach" unless otherwise noted.

Under the HITECH Act and the Breach Notification Rule, a "breach" is the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

(45 CFR § 164.402)

Breach Exceptions

In each circumstance, the incident must not result in further impermissible use or disclosure.

- Unintentional acquisition, access, or use by a covered entity's workforce member (or other person) acting in good faith and within the scope of authority
- Inadvertent disclosure to another person authorized to access PHI within the Covered Entity or Business Associate
- Disclosure of PHI where covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain the information

Presumption of Breach

All circumstances that meet the breach definition, but fail to meet the exceptions under the Rule are presumed to be a breach.

UNLESS

There is a low probability that the PHI has been compromised based on an analysis of the following factors:

- Nature and extent of PHI involved
- Identity of the unauthorized person(s) who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- Extent to which the risk to the PHI has been mitigated

Prevention

Understand the applicable law and what should take place ***BEFORE*** a security incident or breach

The Law: HIPAA & HITECH

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (Pub. L. 104-191) – enacted August 21, 1996, containing ***Administration Simplification Provisions***
- Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) - strengthened HIPAA's privacy and security protections and as of September, 2013 extended applicability to business associates of covered entities

HIPAA & HITECH

Comprehensive regulatory framework developed to implement HIPAA and the HITECH Act:

- Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164)
- Security Rule (45 CFR Part 160 and Subparts A and C of Part 164)
- Enforcement Rule (45 CFR Part 160, Subparts C, D, and E)
- Breach Notification Rule (Interim Final Rule 08/2009; Final Rule 01/2013) (45 CFR Part 160 and Subparts A and D of Part 164)

The Privacy Rule

- The Privacy Rule protects all ***"protected health information"*** **(*"PHI")***

- **PHI** is "individually identifiable health information" held or transmitted by a "covered entity" or its "business associate", in any form or media, whether electronic, paper, or oral

  (45 CFR § 160.103)

The Privacy Rule

Under the Privacy Rule, a covered entity may not use or disclose PHI, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

The Security Rule

- The Security Rule applies to **"e-PHI"**
- **e-PHI** is a subset of PHI
- More specifically, it is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form

The Security Rule: Required Safeguards

ADMINISTRATIVE

PHYSICAL

TECHNICAL

The Security Rule requires covered entities to maintain reasonable and appropriate safeguards for protecting e-PHI.

The Security Rule: Physical Safeguards

- Facility access and control
- Workstation and device security
- Building, data center, server room – consider key card access and video surveillance, unique keys, restrict access
- Secure laptops and desktops, monitor for unauthorized or unrecognized devices

The Security Rule

COVERED ENTITIES MUST:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce

The Security Rule: Administrative Safeguards

- ***Risk Analysis and Management***
- Security management process
- Security personnel
- Information access management
- Workforce training and management
- Evaluation
- Annual and periodic Risk Assessments are a MUST! Identify threats and vulnerabilities to e-PHI
- Policies and Procedures addressing all aspects of data security identified in the risk assessment
- HIPAA Privacy/Security Officer
- Onboarding and Ongoing Training Plans

The Security Rule: Technical Safeguards

- Access controls
- Audit controls
- Integrity controls
- Transmission security
- Firewalls
- Data Encryption
- Antivirus
- SPAM filtering
- Threat protection
- Backup and disaster recovery

Vulnerabilities/Risks

- Network
- Servers
- Mobile Devices
- Portable Storage
- Personnel
- Policies
- Printed/Paper Records
- Disposal
- Credentials
- E-mail
- Risk Assessments

Vulnerabilities/Risks

- Insecure storage of data
- Undefined data retention
- Failure to update policies as technology and operations evolve
- Inadequate training
- Turnover

What are the Threats?

Internal	External
□ Human error	□ Malicious outsider activity
□ Negligent insider activity	□ Negligent outsider activity
□ Intentional/malicious insider activity	□ Advanced Persistent Threat (APT)
□ Viruses/malware	□ Viruses/malware

Techniques/Modes of Compromise

- Phishing
- Spear phishing
- Brute Force
- Elicitation/Social Engineering
- Denial of Service
- Domain Name System (DNS) poisoning
- Sniffing Traffic

RANSOMWARE

RANSOMWARE:

What is ransomware?

It is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates data, or ransomware in conjunction with other malware that does so.

After the Risk Assessment . . .

Implementing Practical Methods to Prevent Ransomware Attacks and Other Incidents or Breaches

RANSOMWARE: OCR GUIDANCE

- OCR released new HIPAA guidance, known as the Ransomware Fact Sheet, on July 11, 2016 addressing:
  - the significant threat ransomware attacks pose to covered entities
  - how HIPAA compliance helps to PREVENT and RECOVER from such an attack; and
  - breach notification implications of such an attack

PREVENTING RANSOMWARE AND OTHER INCIDENTS: OCR GUIDANCE

- Develop Policies and Procedures that align with operations and technological realities; modify them as operations evolve and *implement* them
- Specifically address security incident procedures (45 CFR § 164.308(a)(6)) – detection, containment, eradication, mitigation/remediation, data restoration, continuity of operations, root cause analysis, legal/compliance review, process improvement
- Ensure network devices are not operating on obsolete ***firmware***, facilitate routine firmware updates when available to address known vulnerabilities
- Maintain frequent backups, consider storing them offline and unavailable from the network

PREVENTING RANSOMWARE AND OTHER INCIDENTS: OCR GUIDANCE

- Upgrade software and hardware at appropriate intervals
- Conduct disaster recovery planning, emergency operations planning and review those written plans with reasonable frequency
- Ensure security of portable electronic devices and that PHI that is stored and transported on them is properly safeguarded
- Where appropriate, ***encrypt*** – *at rest and in-transit*! Ensure encryption technology is not obsolete as well

PREVENTING RANSOMWARE AND OTHER INCIDENTS: OCR GUIDANCE

- Install/configure/monitor enterprise-grade firewall with IPS/IDS functionality that is
- Require strong passwords; where appropriate consider salting or hashing or implement two-step verification; de-provision credentials appropriately
- Physically secure data and implement physical access controls (thin clients; sign-in/out logs)
- Develop clear, strict policy and procedure for data retention/destruction and proper disposal of PHI

PREVENTING RANSOMWARE AND OTHER INCIDENTS: OCR GUIDANCE

- Train! Train! Train staff on policies, how to protect PHI
- Partner well with and monitor third party service providers; Ensure compliant business associates agreements are in place
- Privacy/Security Officer; Security Team/Committee

Detection

Proactive methods to increase the likelihood a ransomware attack or other security incident or breach will be detected.

Proactive Efforts to Detect a Breach

- Perform network monitoring
- Conduct system activity monitoring
- Reasonably log physical access and all access to e-PHI and monitor user access logs, sign-in/out logs
- Train users about malicious software and empower them to vigilantly be cautious and report suspicious occurrences

Detection: Activate and Investigate

- **Activate:** Upon learning of circumstances that are indicative of a security incident or breach, activate the security incident response plan
- **Investigate:** Launch and document every step of an investigation of the incident making the following initial inquiry:
  - As appropriate, notify your cyber liability insurer, cybersecurity professionals, law enforcement, legal counsel
  - Determine the scope of the incident to identify what networks, systems, or applications are affected
  - Determine what information/data was involved
  - Determine the origination of the incident (who/what/where/when)
  - Determine whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment
  - Determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited)

Correction

After the investigation: responsive actions to take if you experience a ransomware attack or other security incident or breach.

CORRECTION

- Contain the impact and propagation of the ransomware or other contain the infiltration/threat
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware or other attack and/or propagation
- Recover from the ransomware or other attack by restoring any data or functionality lost or unavailable during the attack and returning to "business as usual" operations
- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (***such as providing notification of a breach of PHI***, and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents)

Responsive Actions if the Incident is a HIPAA "Breach"

- Perform the analysis to determine whether the incident constitutes a breach as defined under the Breach Notification Rule and the HITECH Act

  Note: Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."

  See 45 C.F.R. § 164.402 and § 13402 of the HITECH Act.

Responsive Actions if the Incident is a HIPAA "Breach"

- OCR Guidance indicates that a ransomware attack is ***presumed*** to be a breach giving rise to breach notification and reporting and other remedial action ***UNLESS*** the Covered Entity can demonstrate that there is a low probability that PHI has been compromised.
- Analysis should consider four factors:
  - Nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - Extent to which the risk to the PHI has been mitigated

BREACH NOTIFICATION

- § 13402 of the HITECH Act requires covered entities and business associates under HIPAA to provide notification of breaches of ***unsecured*** protected health information (PHI) to affected individuals, the Secretary of HHS, and, in some cases, the media.
- Business associates are also required to notify covered entities following the discovery of a breach.
- 45 CFR §§ 164.404 – 164.410

Unsecured PHI

- § 13402(h) of the HITECH Act defines "unsecured PHI" unsecured protected health information" as protected health information that is not secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized persons. Encryption and destruction are the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons.

BREACH NOTIFICATION REQUIREMENTS

- Detailed documentation of every action in the process
- Individual Notice - written notification to affected individuals following the discovery of a breach of unsecured PHI by first-class mail or e-mail
- Notice without unreasonable delay and in no case later than 60 days following the ***discovery of a breach***

BREACH NOTIFICATION REQUIREMENTS

- Notices to affected individuals must include:
  - brief description of the breach
  - description of the types of information that were involved in the breach
  - steps affected individuals should take to protect themselves from potential harm
  - brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches
  - contact information for the covered entity

BREACH NOTIFICATION REQUIREMENTS

- Media Notice -
  - For breaches affecting > 500 individuals in a State or jurisdiction
  - Covered Entities must additionally provide notice to prominent media outlets serving the State or jurisdiction that contains same information required for the individual notice
  - Notice must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach
- Reports to the Secretary of HHS - covered entities must notify the Secretary of breaches of unsecured PHI
  - For breaches affecting < 500 individuals in a State or jurisdiction, notice can either be provided at the time notice is provided to affected individuals or on some other date, provided the report is submitted to the Secretary no later than 60 days after the end of the calendar year in which the breach(es) are discovered
  - For breaches affecting > 500 individuals in a State or jurisdiction, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach
  - Submissions are provided electronically through the breach report forms and portal on the HHS website

Monitoring & Enforcement

Monitoring and Enforcement

Covered Entity's Self Monitoring

- Annual Independent Audit of Systems, Policies, and Processes
- "Disaster/Incident Drill" – periodically test contingency plans (e.g., data restoration)
- Complaint Investigations

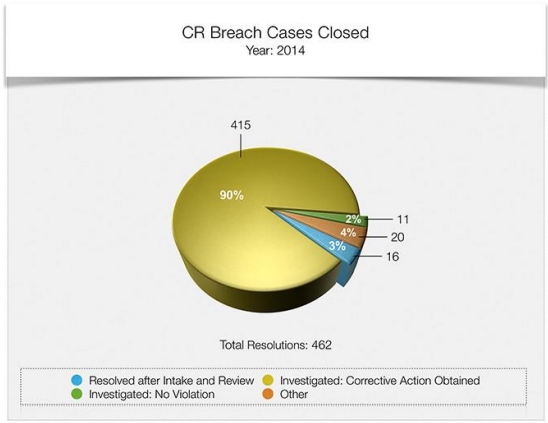
OCR Enforcement

- Complaint Investigations
- Compliance Reviews
- Referrals to DOJ of Suspected Criminal Violations
- Education and Outreach
- Annual Reports to Congress
- Audits

OCR ENFORCEMENT

- Compliance and Performance Improvement Based Resolutions:
  - Voluntary Compliance
  - Corrective Action
  - Resolution Agreements and Monetary Settlements
- Formal Punitive Resolutions – Imposition of Civil Monetary Penalties (CMPs)

OCR ENFORCEMENT



Courtesy of OCR: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#2014

OCR: Civil Monetary Penalties

Category	CMP Amount
Category 1- violation the CE was unaware of and could not have realistically avoided had a reasonable amount of care been taken to abide by HIPAA Rules	Minimum fine of $100 per violation up to $50,000
Category 2 - violation that the CE should have been aware of but could not have avoided even with a reasonable amount of care, but no willful neglect occurred	Minimum fine of $1,000 per violation up to $50,000
Category 3 - violation suffered as a direct result of "willful neglect" of HIPAA Rules where an attempt has been made to correct the violation	Minimum fine of $10,000 per violation up to $50,000
Category 4 - violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation	Minimum fine of $50,000 per violation

OCR: Civil Monetary Penalties

- Maximum fine per violation category: $1.5M
- In certain instances, OCR may decide to apply a penalty per day that the CE has been in violation of the law

OCR: Civil Monetary Penalties

- Intended to act as a deterrent and tool for accountability
- Set in OCR's discretion; can be waived in limited cases
- State Attorney Generals can file civil actions in federal courts
  - Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Sec. 701 of the Bipartisan Budget Act of 2015, Pub. L. 114-74)
  - HHS Interim Final Rule published on September 6, 2016, which adjusts for inflation CMP amounts under the authority of HHS

Criminal Liability

Category	CMP Amount
Tier 1: Reasonable cause or no knowledge of violation	Up to 1 year in jail, plus fines
Tier 2: Obtaining PHI under false pretenses	Up to 5 years in jail, plus fines
Tier 3: Obtaining PHI for personal gain or with malicious intent	Up to 10 years in jail, plus fines

OCR AUDITS

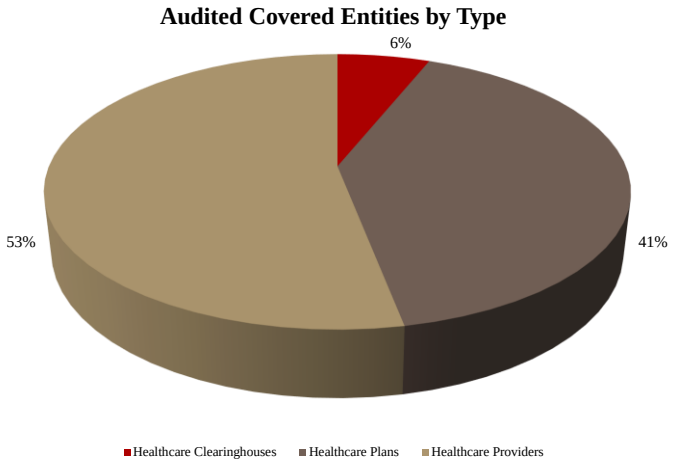
OCR AUDITS

- The HITECH Act mandates that OCR conduct periodic audits of covered entities and business associates to ensure compliance with the Privacy, Security, and Breach Notification Rules
- In 2011, OCR developed an audit pilot program and has adopted a phased approach to implementation

OCR AUDITS: PHASE 1

- Audits of Covered Entities only
- Conducted during 2012 by OCR's contractor, professional public accounting firm, KPMG LLP
- Primarily a compliance improvement activity
- Every audit included a site visit and resulted in an audit report

OCR AUDITS: PHASE 1

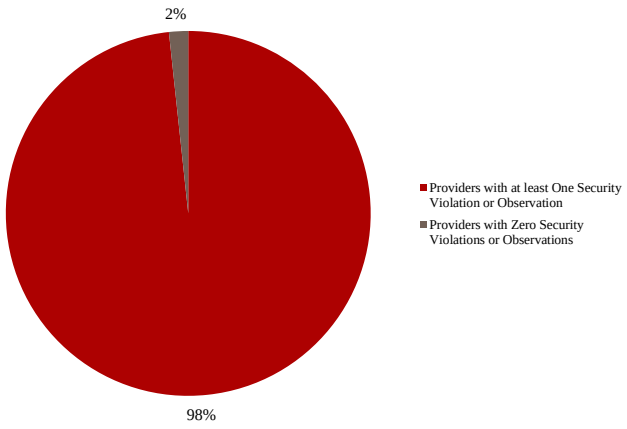


OCR AUDITS: PHASE 1

- Conducted during 2012 by OCR's contractor, professional public accounting firm, KPMG LLP
- Primarily a compliance improvement activity
- Every audit included a site visit and resulted in an audit report

OCR AUDITS: PHASE 1

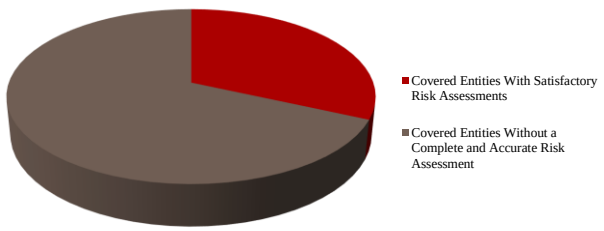
58 out of 59 Healthcare Providers had at least one Security Rule finding or observation.



OCR AUDITS: PHASE 1

- 47 of 59 providers
- 20 out of 35 health plans
- 2 out of 7 clearinghouses

Two thirds (2/3) of all entities audited for risk assessment compliance had no complete and accurate risk assessment.



OCR AUDITS: PHASE 2

- 200 – 250 Audits of Covered Entities and Business Associates
- Primarily desk audits (over 200) during 2016, but some onsite comprehensive audits will occur starting in early 2017
- A Covered Entity ***CAN*** be selected for both a desk audit and on-site audit
- Three Round Audit Process
  - Round 1: Covered Entities (Desk Audits)
  - Round 2: Business Associates (Desk Audits) – Beginning late September *(Ahem! NOW!)*
  - Round 3: Covered Entity and Business Associate (On-site Comprehensive Audits – Approximately 25)

OCR AUDITS: PHASE 2

- May, 2016 – Entity Contact Confirmation Requests and Screening Questionnaires sent
- July 11, 2016 – 167 randomly selected Covered Entities notified of their selection for desk audit
- Document requests were included with the notification with a ten business day response deadline (July 22, 2016)
- Auditor will review the information submitted and provide the Covered Entity with draft findings. Covered entities will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the Covered Entity's response. OCR will share a copy of the final report with the audited entity.

OCR AUDITS: PHASE 2

Covered Entity desk audits will continue through the end of this year. Business Associates will receive notifications of their selection for desk audits while Covered Entity audits are underway.

Notifications are sent via e-mail only. Check your spam and junk mail folders for OCR's communications form this e-mail address:

OSOCRAudit@hhs.gov

OCR ENFORCEMENT

- August 18, 2016 - OCR Announced: Breaches of PHI affecting fewer than 500 individuals are its next focus
- OCR's regional offices will now conduct investigations on smaller breaches "as resources permit.“
- Factors to identify smaller breaches to investigate:
  - size of the breach
  - whether theft or improper disposal of unencrypted PHI was involved
  - whether the breach involved unwanted intrusions to IT systems (such as hacking)
  - whether the same entity or business associate had filed numerous breach reports

Other Considerations

State Law Protection of PHI and PII and the Liability Exposure for Healthcare Providers

TN Law:

- One of 47 states with a breach notification statute
- Tennessee Identity Theft Deterrence Act of 1999 (Tenn. Code Ann. § 41-18-2101, *et seq.*)
- Amended March, 2016 to require breach notification within a specified time frame after discovery of the breach and to ***potentially*** require breach notification where the data compromised was ***encrypted***
- Exception carved out for entities and individuals covered by HIPAA as expanded by the HITECH Act such that the § 2107 breach notification provision does not apply
- Remain mindful of other provisions in this Act, i.e., § 2110's prohibition of certain actions with respect to consumers' SSNs

Other State Law Considerations

A growing number of state courts are allowing state law claims based on a HIPAA violation to proceed to trial on the merits or at least suggesting preemption is nuanced. One jurisdiction has established a precedent that has the health care community a little anxious.

	State	
1	NC	*Acosta v. Byrum*, 638 S.E.2d 246 (N.C. 2006)
2	WV	*R.K. v. St. Mary's Medical Center,* 735 S.E.2d 715 (W.Va. 2012), *cert. denied*, 133 S.Ct. 1738 (2013)
3	CT	*Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*, 2014 WL 5507439 (Conn. 2014)
4	MO	*I.S. v. Washington Univ.*, No. 4:11CV235SNLJ, 2011 WL 2433585, at *2 (E.D. Mo. June 14, 2011)
5	TN	*Harmon v. Maury County, TN*, No. 1:05 CV 0026, 2005 WL 2133697, at *3, *4 (M.D. Tenn. Aug. 31, 2005)

Jury Awards Patient $1.4M against Pharmacy

- *Walgreen Co. v. Hinchy*, 21 N.E.3d 99 (Ind. Ct. App. 2014), 29 N.E.3d 748 (Ind. Ct. App.), *transfer denied*, 2015 Ind. LEXIS 374 (Ind. 2015)
- The plaintiff, who had been romantically involved with the Walgreen pharmacist's boyfriend and eventual husband, alleged that the pharmacist accessed her prescription records and divulged information she obtained to him. Allegedly, the disclosed information related to birth control prescriptions and sexually transmitted diseases.

Jury Awards Patient $1.4M against Pharmacy

- Total Judgment of $1.8M – Liability allocated to the non-party Boyfriend/Husband at 20% and to the Pharmacy and Pharmacist jointly at 80%

- Court rejected Pharmacy's argument that the employee was acting outside of the scope of her employment and in contravention of company policy and held employer responsible for the employee's conduct

RECAP and TAKEAWAYS

Don't let breach prevention, detection, and correction OR compliance monitoring and enforcement be an ***AFTER***thought, plan and act ***BEFORE*** the breach.

Five Questions for CHC Leadership to Address

- Have we conducted an annual risk assessment and analysis?
- Have we developed, implemented, and provided thorough training for employees and independent contractors on reasonable policies and procedures addressing the findings of our risk assessment?
- Have we implemented administrative, physical, and technical safeguards?
- Have we amassed the additional support and resources (liability policies, trusted IT partners, counsel) necessary to succeed and maintain compliance?
- Are we testing our contingency plans and security incident procedures ("disaster/incident drills")?

QUESTIONS?

THANK YOU!

Tera T. Hambrick, JD
Director of Regulatory Affairs & Legal Counsel
Matthew Walker Comprehensive Health Center, Inc.
Nashville, TN
thambrick@mwchc.org
615-324-9685