Incident Response:
Best Practices in Breach Management

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB, VP of Privacy, Compliance and HIM Policy, MRO

Melissa Landry, RHIA, Assistant Vice President of Health Information Management, Ochsner Health System

MRO

Agenda

- Current Environment and Statistics related to Healthcare Breaches
- Breaches under HIPAA and State Law
- HIPAA Security Rule Safeguards that Address Incident Response Plans
- Best Practices for Incident Response Plans
- The First 24 Hours Following a Breach
- Questions

MRO

Data Breach Landscape

Statistics

- Data breaches cost companies an average of $221 per compromised record
  - $145 pertains to indirect costs, which include abnormal turnover or churn of customers
  - $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees
- Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221
- The total average organizational cost of a data breach is $7.01 million

The Cybersecurity Threat to Healthcare

- 89% of healthcare organizations surveyed by the Ponemon Institute report suffering at least one data breach in the past 2 years
- Data breaches could be costing the healthcare industry upwards of $6.2 billion per year
- A breach of medical information costs healthcare organizations an average of $2.2 million per breach
- Interestingly, the value of medical information on the black market has recently plummeted, one reason hackers are resorting to ransomware

HIPAA and Breach Prevention

- **Privacy Rule - 45 CFR Part 160 and Subparts A and E of Part 164**
  - Sets national standards for the protection of certain health information
  - Requires appropriate safeguards to protect the privacy of PHI
  - Sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization
  - Gives patients rights over their health information, including rights to examine and obtain a copy of the ir health records, and to request corrections
- **Security Rule - 45 CFR Part 160 and Subparts A and C of Part 164**
  - Establishes a national set of security standards for health information that is held or transferred in electronic form
  - Operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that CEs must put in place to secure individuals' "electronic PHI" (e-PHI)
    - Administrative Safeguards
    - Technical Safeguards
    - Physical Safeguards
- **Breach Notification Rule - 45 CFR §§ 164.400-414**
  - If an impermissible use of disclosure of PHI is determined to be a Breach, CEs must provide notification of the Breach to affected individuals, the Secretary of HHS (The Secretary), state entities (under applicable state law) and, in certain circumstances, to the media

Breaches under HIPAA – 45 CFR §§ 164.400-414

- An impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the PHI
- An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity (CE) or Business Associate (BA) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
  - The 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
  - The extent to which the risk to the PHI has been mitigated

Breaches under HIPAA – 45 CFR §§ 164.400-414

- CEs and BAs must only provide the required notifications if the breach involved "Unsecured PHI"
  - "Unsecured PHI" is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS' Guidance on Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- The Guidance specifies encryption and destruction as the technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals

MRO

2018 OCR Activities

- OCR stated that 2018 was a "***record year***" for enforcing HIPAA.

- Ten cases were settled by OCR and an Administrative Law Judge granted summary judgment on a case as well. These 2018 enforcement actions resulted in **$28.7 million in fines**, a 22 percent increase from the earlier record year of $23.5 million in 2016.
  - Included in this settlement figure was an American health insurance company settlement, which resulted in a $16 million fine, the largest fine yet.

MRO

Recent Resolution Agreements and Civil Money Penalties involving Breaches

ANTHEM, INC
A record HIPAA settlement following largest health data breach in history - October 15, 2018 Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules ***after a series of cyberattacks led to the largest health data breach in history and exposed the electronic protected health information of almost 79 million people.***
settlement, a **$16 million fine**, the largest fine yet. http:anthem/index.html://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/a

The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016

- This breach affected electronic protected health information (ePHI) that Anthem, Inc. maintained for its affiliated health plans and any other covered entity health plans.
- On March 13, 2015, Anthem filed a breach report with the HHS Office for Civil Rights detailing that, on January 29, 2015, they discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data, otherwise known as an advanced persistent threat attack.
- After filing their breach report, Anthem discovered cyber-attackers had infiltrated their system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks.

The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016

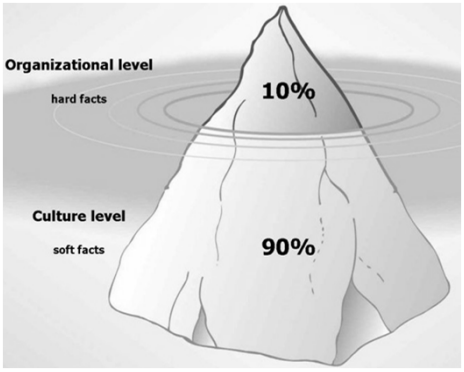
- OCR's investigation revealed that between December 2, 2014 and January 27, 2015, the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.
- OCR's investigation revealed:
  - that Anthem failed to conduct an enterprise-wide risk analysis,
  - had insufficient procedures to regularly review information system activity,
  - failed to identify and respond to suspected or known security incidents, and
  - failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2014.

Recent Resolution Agreements and Civil Money Penalties involving Breaches

A health system in California (the "System") **The System operates several hospitals, including a rehabilitation hospital**
• The System reported to OCR two breaches of unsecured electronic protected health information ("ePHI") that affected over 60,000 individuals. One breach occurred in December 2013 and impacted approximately 50,197 individuals, and the other occurred in December of 2015 and impacted about 11,608 individuals. • The removal of server protections by a System contractor led to the first breach, where protected health information ("PHI") was available to anyone who could access the System's server who could also download files – even if they did not have a username and password. • PHI was accessible on the internet again due to an employee activating the incorrect website on a SQL server. This led to the second breach.
Resolution Payment: **$3 million fine** and adopt an extensive corrective action plan

Potential financial impact of HIPAA noncompliance on covered entities and business associates

- Is not limited to fines from OCR. These record figures do not include the costs covered entities and business associates incur when required to respond to an OCR investigation that does not result in direct fines and penalties.
  - **Hard costs**
  - **Soft costs**



Potential financial impact of HIPAA noncompliance on covered entities and business associates

- The increasing demands on technology infrastructure and capabilities as well as the accompanying demands on information technology staff have created a complex environment to manage for entities that must comply with HIPAA. Entities subject to HIPAA should:
  - Recognize the importance of a robust HIPAA compliance plan that is regularly reviewed and updated by all relevant internal parties;
  - Ensure that sufficient resources are allocated to implement adequate security measures to address identified risks and vulnerabilities;
  - Establish processes to regularly conduct system reviews for all systems and applications that maintain ePHI to reduce the chance that human error results in such a significant breach of ePHI; and
  - Ensure that those responsible for contracting and procurement are fully apprised of the nature and scope of services a particular vendor is providing and that they work with information technology staff and business partners to properly address regulatory obligations, like business associate agreements
    - » *Taken from* Hall Render Killian Heath & Lyman PC

State Breach Notification Laws

- Not only do CEs and BAs have to follow the HIPAA Breach Notification Rule, they also have to comply with state laws regarding health data breaches
  - The law of the state in which the CE and BA are located AND
  - The state in which the impacted residents reside
- 50 states have data breach notification laws
- 14 states have notification requirements for breaches involving PHI
- The definition of breach under some of these state laws is *broader* than HIPAA

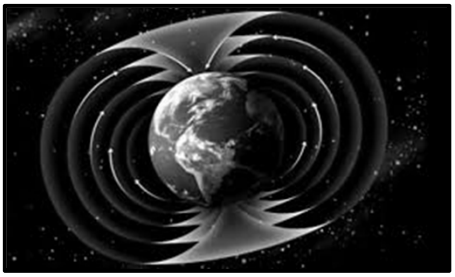
HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Management Process - 45 CFR § 164.308(a)(1)
- Risk Analysis (Required)
  1. The scope of the Risk Analysis is key
  2. Document *where* ePHI is stored, received, maintained or transmitted
  3. Identify and document potential threats and vulnerabilities
  4. Document how well your current security measures address the potential threats and vulnerabilities
  5. Determine the likelihood of threat occurrence, the threat's level of risk, and the potential impact of such an occurrence
  6. Identify next steps that need to be taken to mitigate risk
- Risk Management (Required)

The actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its ePHI and to meet the general security standards

Cyber breaches rocked the healthcare universe in 2018, and the lesson to learn is clear:

Heed caution in 2019 — you must perform an annual risk analysis and follow through on your HIPAA compliance problems.



HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Management Process - 45 CFR § 164.308(a)(1)
- Helpful Tools:
  - HHS - Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework: http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/
  - HHS Guidance on Risk Analysis: http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html
  - ONC's Security Risk Assessment Tools: https://www.healthit.gov/providers-professionals/security-risk-assessment
    - *Updated tools due out any day now!*
  - HHS Security Rule Guidance Material: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Management Process - 45 CFR § 164.308(a)(1)
- Sanction Policy (Required)
  - "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE"
    - Require workforce members to sign a Statement of Adherence to your organization's HIPAA Security Policies & Procedures
    - Statement of Adherence should state that the workforce member acknowledges that violations of HIPAA Security P&Ps may lead to disciplinary action, for example, up to and including termination
    - Sanction Policy should include examples of potential violations of HIPAA Security P&Ps
    - Sanction Policy should adjust the disciplinary action based on the severity of the violation
- Information System Activity Review (Required)
  - "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports"
  - The information system activity review enables CEs to determine if any e-PHI is used or disclosed in an inappropriate manner
    - Information system activity review procedures may be different for each CE and BA
    - The procedure should be customized to meet your organization's risk management strategy and take into account the capabilities of all information systems with e-PHI

MRO

Sanctions Policy – Use & Access of PHI

MRO

MRO applies appropriate sanctions against *Workforce* members who fail to comply with MRO's HIPAA Privacy and Security Policies and Procedures, as required under 45 CFR § 164.530(e)(1), regarding the proper use and access of Protected Health Information (PHI).

MRO recognizes three categories defining the significance and impact of the privacy or security incident to help guide its corrective action and remediation steps:

Category 1: *Accidental or inadvertent violation of MRO's HIPAA Privacy & Security P&Ps that may be caused by lack of knowledge and lack of training*	**Category 2:** *An unintentional violation of MRO's HIPAA Privacy & Security P&Ps due to poor job performance, carelessness, or lack of performance improvement.*	**Category 3:** *Deliberate, purposeful, willful, or malicious violation of MRO's HIPAA Privacy & Security P&Ps* due to curiosity or desire to gain information, for personal use or to cause the patient or MRO harm.
☐ Release of PHI without proper patient authorization	☐ Release of PHI without proper patient authorization	☐ Accessing the information of high-profile people or celebrities
☐ Failure to properly sign off from or lock computer when leaving a work station	☐ Failure to properly sign off from or lock computer when leaving a work station	☐ Accessing or using PHI without a legitimate need to do so
☐ Failure to report privacy and security violations	☐ Failure to report privacy and security violations	☐ Posting PHI to social media websites
☐ Improper disposal of PHI	☐ Improper disposal of PHI	☐ Disclosing PHI to an unauthorized individual or entity for illegal purposes (i.e., identity theft)

Category 1: ***Suggested Corrective Actions***	Category 2: ***Suggested Corrective Actions***	Category 3: ***Suggested Corrective Actions***
☐ Counseling	☐ Counseling	☐ Counseling
☐ Retraining on applicable policies and procedures	☐ Retraining on applicable policies and procedures	☐ Retraining on applicable policies and procedures
☐ Disciplinary action as appropriate	☐ Disciplinary action up to and including termination	☐ Disciplinary action up to and including termination
☐ Other:	☐ Other: ☐	☐ Referral to law enforcement, if necessary
☐	☐	☐ Other:
Contact Human Resources prior to taking corrective action	**Contact Human Resources prior to taking corrective action**	**Contact Human Resources prior to taking corrective action**

Mitigating factors

Sanctions may be modified based on mitigating factors. These factors may reflect greater damage caused by the violation and thus work against the violator, ultimately increasing the penalty.

Examples include:

- Violation of sensitive information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the organization
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation, lack of truthfulness
- Negative influence on others
- History of performance issues and/or violations

MRO

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Management Process - 45 CFR § 164.308(a)(1)

- Assigned Security Responsibility (Required)
  - "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity"

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards

Security Awareness and Training - 45 CFR § 164.308(a)(5)

— "Implement a security awareness and training program for all members of its workforce (including management)"

- Security Reminders (Addressable)

— Notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, as well as formal retraining on your organization's HIPAA Security P&Ps

— It is recommended that your organization review how it currently reminds the workforce of current P&Ps, and then decide whether these practices are reasonable and appropriate, or if other forms of security reminders are needed

NOTE: At the Spring 2017 HIPAA Summit, the OCR stated, "Addressable does <u>not</u> mean optional!!!"

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards - Security Awareness and Training - 45 CFR § 164.308(a)(5)

- Initial, then Annual Training
  - Documentation
  - Have a System
- Ongoing Privacy & Security Tips
  - Employee Newsletters
  - Use Technology Applications
- OCR You Tube videos: https://www.youtube.com/user/USGovHHSOCR
- Competency Testing
  - AHIOS CRIS Test
  - HITNOTS.com Quizzes
- Retrain & apply sanctions for all privacy & security incidents

- Focus on Breach Prevention!
- Your New Rights Under HIPAA (2:47) https://www.youtube.com/watch?v=3-wV23_E4eQ
- The Right to Access and Correct Health Information (1:04) https://www.youtube.com/watch?v=JY1l5s8ED5c
- Your Mobile Device & Health Information Privacy & Security (4:43) http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Incident Procedures (Required) – 45 CFR § 164.308(a)(6)
    - Requires CEs and BAs to address security incidents within their environment
    - Security Incident - "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system"
  - Procedures must address how to identify security incidents and require incident be reported to the appropriate person or persons
  - Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved
  - An entity should be able to rely upon the information gathered in complying with the other HIPAA Security Rule standards to determine what constitutes a security incident in the context of its business operations

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards
  - Security Incident Procedures (Required) – 45 CFR § 164.308(a)(6)
    - Train all workforce members on how to identify potential security incidents and who to report them to
    - When a report of a potential security incident is received …
      - Determine and document what happened
      - Identify and classify the severity of the Security Incident
      - Determine the actual risk to Individually Identifiable Health Information, and the subject(s) thereof
      - Repair, patch, or otherwise correct the condition or error that created the Security Incident
      - Retrieve or limit the dissemination of Individually Identifiable Health Information, if possible
      - Determine if the Security Incident rises to the level of a Breach under the HIPAA and HITECH regulations
      - Mitigate any harmful effects of the Security Incident
      - Fully document the causes of and responses to Security Incidents
      - Expand knowledge of Security Incident prevention through research, analyses of Security Incidents, and improved training and awareness programs for Workforce members

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Administrative Safeguards- Evaluation (Required) – 45 CFR § 164.308(a)(8)
  - "Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic PHI (e-PHI), that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]"
    - It is crucial to know if the security plans and procedures implemented continue to adequately protect e-PHI
    - Organizations must periodically evaluate their strategy and systems to ensure that the security requirements continue to meet their organizations' operating environments

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Physical Safeguards – Encryption – 45 CFR § 164.312(e)(2)(ii)
  - Where encryption is a reasonable and appropriate safeguard for organizations, they must:
    - "Implement a mechanism to encrypt ePHI whenever deemed appropriate"
  - Encryption is a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text
  - There are various types of encryption technology available
  - The Security Rule allows CEs the flexibility to determine when, with whom, and what method of encryption to use

NOTE: At the Spring 2017 HIPAA Summit, the OCR stated, "Addressable does <u>not</u> mean optional!!!"

HIPAA Security Rule Safeguards that Address Incident Response Plans

- HIPAA Physical Safeguards - Device and Media Controls (Addressable) – 45 CFR § § 164.310(d)(1)
  - *"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility"*
    - Disposal (Required)
    - Media Re-Use (Required)
    - Accountability (Addressable)

Ochsner Health System: Who We Are

Largest Health System in the Gulf South

- 29 Hospitals (Owned, Managed & Affiliated)
- Over 60 Health Centers
- Over 2,500 Affiliated Physicians, including over 1,100 Employed in more than 90 Specialties and Subspecialties
- 600 Clinical Trials – 7,000 Patients
- 417 Medical Students – Ochsner Clinical School/University of Queensland
- 375 Residents in 27 Programs
- Largest Private Employer in Louisiana

Ochsner Health System pursues partnerships and affiliations to align with our **DESTINATION CENTER OF EXCELLENCE STRATEGY**

OHS – Best Practices for Incident Prevention

Audit Controls – User Activity Monitoring

- Fair Warning - *Managed Privacy Services*
  - Proactive monitoring by Fair Warning; alerts provided to OHS
  - OHS Privacy team of three dedicated resources manage the internal investigation and follow-up
  - Monitoring rules for VIP and co-worker hierarchy

OHS – Best Practices for Incident Prevention

Access Controls – EMR/PHI

- **Break the Glass (BTG)**

-Offers a higher level of protection for a patient's private information
-Attempted access will prompt for a reason and password to gain entry
-Closely monitored to ensure that only authorized individuals are accessing

Triggers for BTG Security

a) Patient Level
   - When the patient is marked with BTG – Celebrity or BTG – all other
   - When a patient is associated with one service area and access is attempted by a user associated with another service area via the user's default log in settings in the EMP record

b) Encounter Level
   - When a patient currently or has ever had an encounter within a psych department

OHS – Best Practices for Incident Prevention

Access Controls – EMR/PHI

- **Patient Opt Out**

  -Private encounter flag

- **Sensitive Notes**

  -Default setting vs. end user initiated

  -Access to view controlled by security

- **Social Security Number Masking**

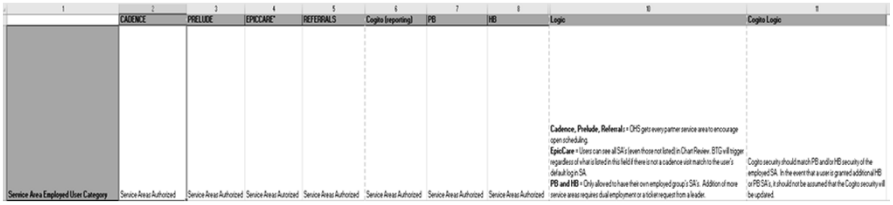
  -Limited display of SS# - controlled through security

OHS – Best Practices for Incident Prevention

Access Controls – EMR/PHI

- **Shared EMR – Service Area Build**

  - SA matrix defines the access



	CADENCE	PRELUDE	EPICCARE*	REFERRALS	Cogito (reporting)	PB	HB	Logic	Cogito Logic
Service Area Employed User Category	Service Area1 Authorized	Service Area1 Authorized	Service Area1 Authorized	Service Area1 Authorized	Service Area1 Authorized	Service Area1 Authorized	Service Area1 Authorized	**Cadence, Prelude, Referrals** = OHS gets every partner service area to encourage open scheduling **EpicCare** = Users can see all SA's (even those not listed) in Chart Review. BTG will trigger regardless of what is listed in this field if there is not a cadence visit match to the user's default login SA. **PB and HB** = Only allowed to have their own employed group's SA's. Addition of more service areas requires dual employment or a ticket request from a leader.	Cogito security should match PB and/or HB security of the employed SA. In the event that a user is granted additional HB or PB SA's, it should not be assumed that the Cogito security will be updated.

OHS – Best Practices for Incident Prevention

Access Controls – EMR/PHI

- **Security Provisioning – Role-Based Access**
  - OHS Policy: *EMR User Access Provisioning*
    - Access granted based upon job role and contingent upon proper training/application template assigned
    - Residents and students completing clinical rotations are granted time-limited access based upon start/end dates of rotation
  - OHS Policy: *DGProc.023 – Access to PHI Non-OHS Individuals*
    - Community and Referral providers, office staff, outside reviewers granted limited "view only" EMR
    - User Access Agreement – "SWAAG"
    - Limited access based upon needs (First Access, Managed access, insurance restricted)
  - OHS Policy: *Workforce Access to PHI*

OHS – Best Practices for Incident Prevention

Access Controls – EMR/PHI

- **Access Audits**
  - Audits of Role-Based EMR Access and Bypass Break the Glass
    - Conducted annually
    - One over leader validates continued access – role and template
  - Audits of Non-OHS Individuals' EMR Access
    - Conducted every 6 months
    - Ochsner sponsor validates continued access with external individual
    - SWAAG outlines responsibility for notice of access termination
  - Epic Logging

Best Practices for Incident Response Plans

1. Create a Patient Data Protection Committee

- All stakeholders in a healthcare organization involved in protecting patient information must communicate with each other on a regular basis
  - Health Information Management
  - Privacy
  - Compliance / Risk Management
  - Legal
  - Information Technology
  - Physicians and Nurses

Best Practices for Incident Response Plans

2. Create a Patient Data Protection Committee

- The Committee should be charged with conducting some patient privacy functions for the healthcare organization:
  - Overseeing the organization's patient privacy compliance program
  - Conducting the organization's quarterly risk analyses and assessments
  - Reviewing policies and procedures annually
  - Serving as the organization's incident response team
  - Doing mock audits using the new Phase II protocols from OCR

Best Practices for Incident Response Plans

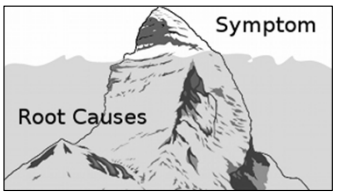
3. Provide On-Going Education and Training for Workforce Members

- Many breaches are caused by unintentional actions taken by workforce members who are not familiar with the proper policies and procedures for the use and disclosure of health information

Best Practices for Incident Response Plans

4. Provide On-Going Education and Training for Workforce Members

- Creating ***a culture of compliance is key***
- Workforce members should undergo formal training at least once a year to ensure compliance with applicable federal and state law
- Provide regular reminders of P&Ps
  - Emails, posters, and patient privacy awareness events and activities
- Investigations into "Close Calls"
  - Root Cause Analysis



Best Practices for Incident Response Plans

5. Provide On-Going Education and Training for Workforce Members

- Helpful Tools
  - Your cyber-liability insurance carrier may have free tools for training and education
  - OCR's YouTube Channel: https://www.youtube.com/user/USGovHHSOCR

Best Practices for Incident Response Plans

6. Encrypt!!!

- Utilize technologies that strengthen your compliance program
  - Encryption
    - Secured PHI Safe Harbor
- Access monitoring Software
- HHS Guidance on Technical Safeguards: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

DON'T FORGET SNAIL MAIL PROCESSES --- take precautions.

For example, recent incident at Rush exposes names of 908 patients

Best Practices for Incident Response Plans

7. Test the Effectiveness of your Compliance Program

- Social Engineering
  - Fake phishing emails
  - Fake phone calls
  - Check desks for exposed passwords
- Mock Breach Exercise
- Auditing
  - Internal audits
    - OCR Phase 2 Audit Protocol
  - External audits
  - Penetration testing

Best Practices for Incident Response Plans

8. Assess your BA's Compliance

- Due Diligence
- Business Associate Agreements
- Periodic Vendor Assessments

	Authentication, Authorization & Access Management	
9	Are there integration requirements for authentication and/or authorization? If so please describe?	
10	What user access control mechanisms does the system/application provide (e.g., role-based access)? Please describe including all internal application access controls if any.	
11	What accounts are required to manage the system and/or application? Please provide a separate list of all required application accounts along with who is responsible for each account.	
12	Who is responsible for provisioning user access to the system and application (i.e., adding, modifying, and removing access)?	
13	How does your organization manage accountability of generic accounts and functional IDs?	
14	What security controls do you have to ensure that other customers or third parties could not gain unauthorized access to corporation data in this system/application? Please list and describe the controls.	
15	What method of authentication is used to authenticate users to the system application?	

The First 24 Hours Following a Breach

1. Privacy Officer should document the incident in a report and conduct and draft a risk assessment
   - What happened?
   - When did it happen?
   - What data was involved?
   - How many individuals were impacted?
   - Corrective action taken
   - Identify what state laws must be complied with in addition to the HIPAA Breach Notification Rule

2. Assemble your Patient Data Protection Committee/ Incident Response Team to review the report and risk assessment
3. If the breach involves a significant number of individuals or you anticipate the breach to be costly, notify your cyber liability insurance carrier immediately
   - If breach is caused by a BA and they indemnify you, have the BA notify their cyber liability insurance carrier
4. Draft notice to affected patient(s) in accordance with HIPAA and applicable state laws (the law of the state in which the facility is located and the law(s) of the state(s) in which the affected individual(s) reside)
5. Provide notice to applicable government entities under HIPAA and relevant state laws
6. Notify the media, if required under applicable law
7. Document the incident in the patient's accounting of disclosures

Following a Breach – Notification Requirements

- Notification under HIPAA – 45 CFR §§ 164.400-414
  - Individual Notice
    - Written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically
    - If the CE has insufficient or out-of-date contact information for 10 or more individuals, the CE must provide substitute individual notice (see Breach Notification Rule for more information on substitute notice)
    - If the CE has insufficient or out-of-date contact information for fewer than 10 individuals, the CE may provide substitute notice by an alternative form of written notice, by telephone, or other means
    - These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible
      - a brief description of the breach
      - a description of the types of information involved in the breach
      - the steps affected individuals should take to protect themselves from potential harm
      - a brief description of what the CE is doing to investigate the breach
      - mitigate the harm
      - prevent further breaches, as well as contact information for the CE (or BA, as applicable)
    - While the CE is ultimately responsible for ensuring individuals are notified, even with respect to breaches at or by a BA, the CE may delegate the responsibility of providing individual notices to the BA
      - CEs and BAs should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the BA performs on behalf of the CE and which entity has the relationship with the individual
  - Media Notice
    - CEs that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction
    - CEs will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay, and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice

Following a Breach – Notification Requirements

- Notification under HIPAA – 45 CFR §§ 164.400-414
  - Notice to the Secretary
    - In addition to notifying affected individuals and the media (where appropriate), CEs must notify the Secretary of breaches of unsecured PHI. CEs will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, CEs must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the CE may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Class Action Lawsuits becoming more common

- Community Health System, one of the largest health systems in the United States, has agreed to pay $4,500,000 to settle claims made against it arising from a 2014 data breach. The data breach, believed to be caused by malware installed by Chinese hackers on CHS's computer system, exposed the names, dates of birth, addresses, telephone numbers, and Social Security numbers of approximately 4.5 million patients.

- Following the breach, numerous lawsuits were filed by patients seeking compensation for the theft of their personal information. The lawsuits were consolidated into a single lawsuit. The settlement, which still must be approved by the Judge overseeing the case, provides for two different payments to patients affected by the breach. Individuals who can prove they incurred out-of-pocket expenses as a result of the breach and/or can show evidence in time lost securing their accounts, can claim up to $250. Individuals who have suffered identity theft or fraud can recover up to $5,000.

Putting it into Practice:

- This case is a reminder for entities to review their data protection mechanisms.

- Class action lawsuits by individuals affected by breaches are becoming more common, and could significantly increase the financial penalties and exposure applicable to companies that store patient information

Environmental Scanning is an Essential Element for your program; *Becker's Health IT & CIO Report*

editorial@beckershealthcare.com top news 2/21/2019

Seattle-based UW Medicine sent letters to 974,000 patients notifying them of a Dec. 4, 2018, data error that allowed patient information to come up in internet searches.

UW Medicine became aware of the incident Dec. 26, 2018, and took immediate action to remove the patient files from the internet.

An internal human error made the patient files accessible.

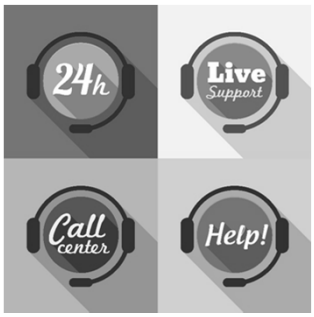
Google saved some of the files before UW Medicine discovered the breach, so the hospital worked with the tech giant to remove the saved versions. As of Jan. 10, all patient files were removed from Google's servers.

MRO

Post-Incident Actions

UW Medicine

- Reviewing its internal protocols and procedures to prevent further data errors.
- Set up a call center and website to field patient questions.



MRO

The 10 Elements of an Effective Compliance Program

1) Risk Assessments
2) Training and Education
3) Developing Workplans
4) Policies and Procedures
5) Incident Monitoring
6) Program Audits
7) Sanction Checking
8) Governance and Oversight
9) Contract Management
10) Executive Reporting

Helpful Tools

- OCR FAQs on Patient Access
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/
- Phase 2 of HIPAA Audits
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when
- Administrative Safeguards
  - HHS - Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework: http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/
  - HHS Guidance on Risk Analysis: http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html
  - ONC's Security Risk Assessment Tools: https://www.healthit.gov/providers-professionals/security-risk-assessment
  - HHS Security Rule Guidance Material: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- "Minimum Necessary" Rule
  - HHS Guidance on the Minimum Necessary Requirement: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html
- Technical and Administrative Safeguards
  - HHS Guidance on Technical Safeguards: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
  - HHS Guidance on Physical Safeguards: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Questions?

Contact Info

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB

Vice President of Privacy, Compliance and HIM Policy
MRO
rbowen@mrocorp.com
610-994,7500, Ext. 526

MRO

Melissa Landry, RHIA

Assistant Vice President of Health Information Management
Ochsner Health System
melandry@ochsner.org

Ochsner Health System

The views and opinions expressed in this presentation are those of the presenters and do not necessarily reflect or represent the views, opinions, or policies of MRO Corporation.