A Data Breach Lived and Learned: Tips for Responses and HHS OCR's Review

BASS BERRY + SIMS PLC

PANELISTS

John Bailey, *Global Privacy Counsel,*
St. Jude Children's Research Hospital

Lisa S. Rivera, *Member*
Bass Berry Sims

BASS BERRY + SIMS PLC

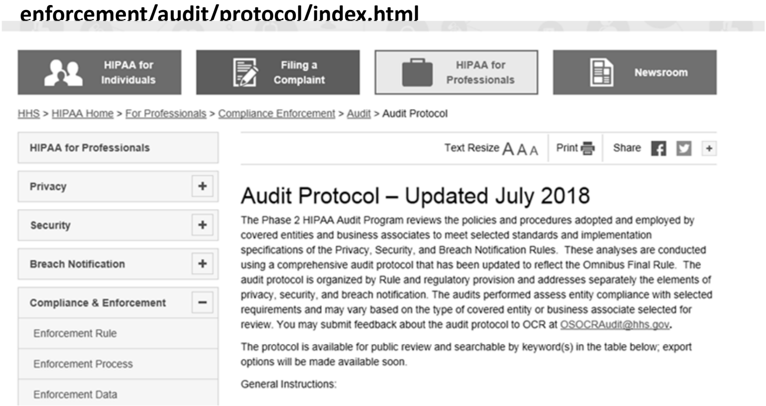
Overview

- OCR updates
- Recurring compliance issues
- Responding to data breaches
- OCR investigations
- Takeaways

OCR Update: Audit Program

OCR has tweaked its audit protocol, which is also used by investigators when evaluating compliance.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

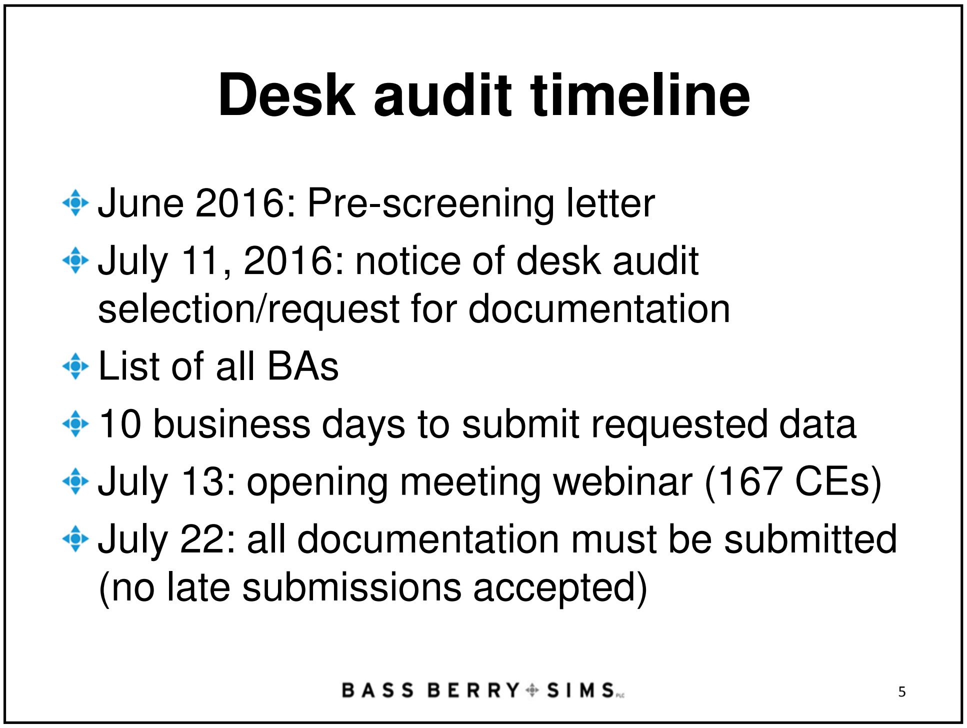


Audit Protocol – Updated July 2018

The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule. The audit protocol is organized by Rule and regulatory provision and addresses separately the elements of privacy, security, and breach notification. The audits performed assess entity compliance with selected requirements and may vary based on the type of covered entity or business associate selected for review. You may submit feedback about the audit protocol to OCR at OSOCRAudit@hhs.gov.

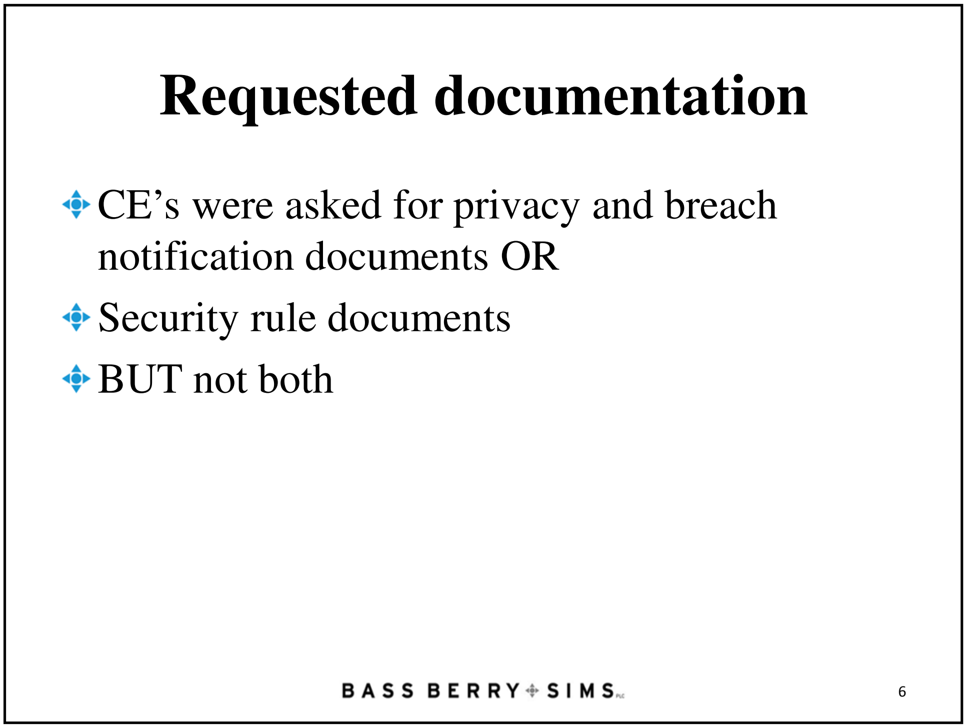
The protocol is available for public review and searchable by keyword(s) in the table below; export options will be made available soon.

General Instructions:



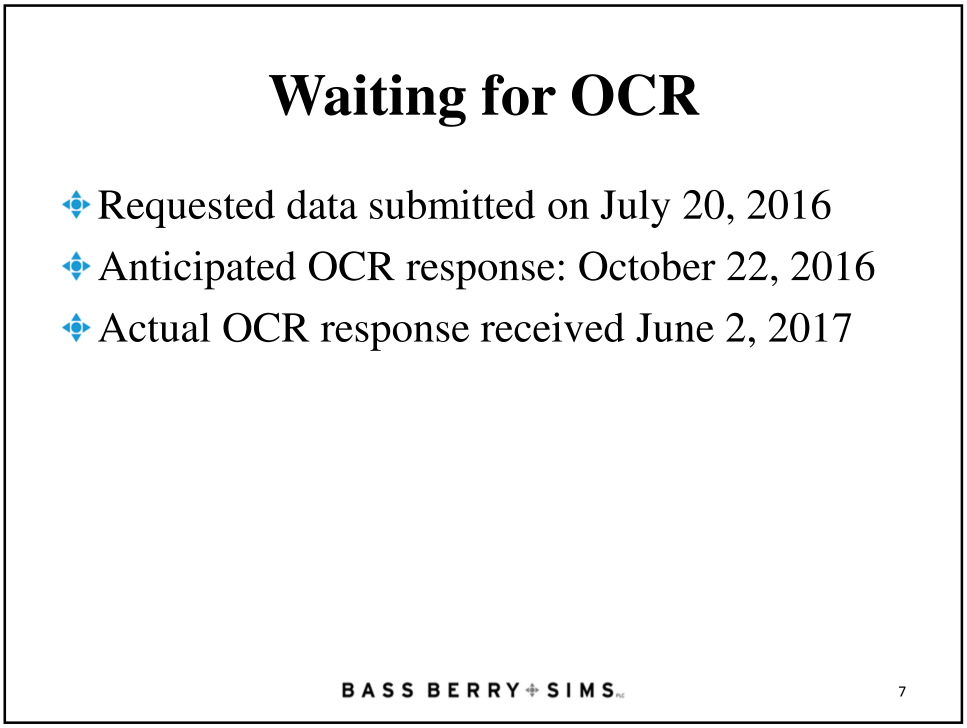
Desk audit timeline

- June 2016: Pre-screening letter
- July 11, 2016: notice of desk audit selection/request for documentation
- List of all BAs
- 10 business days to submit requested data
- July 13: opening meeting webinar (167 CEs)
- July 22: all documentation must be submitted (no late submissions accepted)



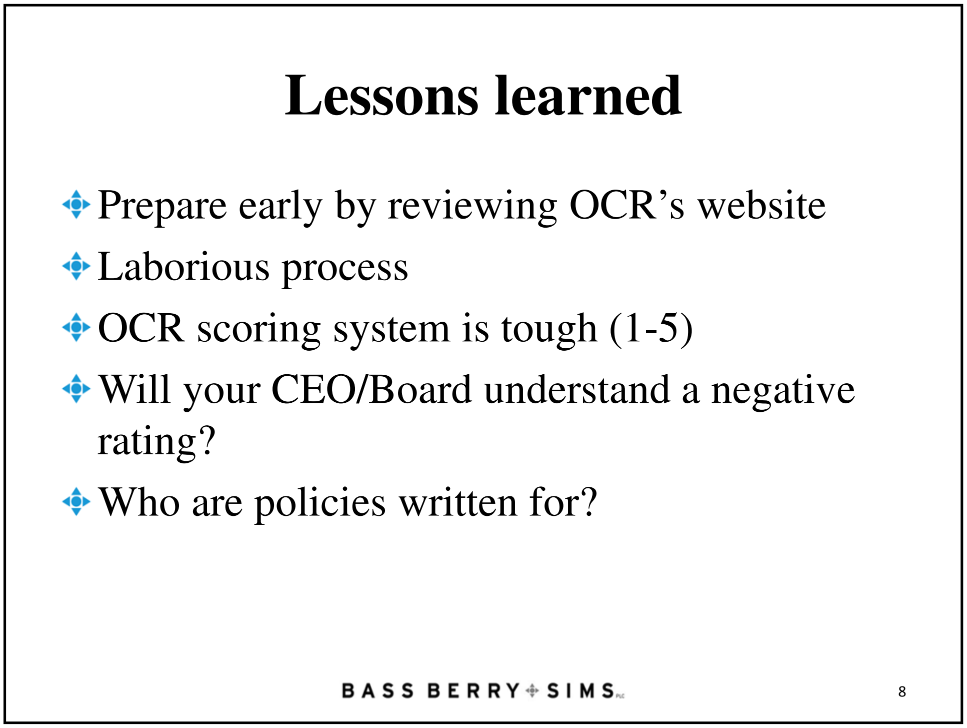
Requested documentation

- CE's were asked for privacy and breach notification documents OR
- Security rule documents
- BUT not both



Waiting for OCR

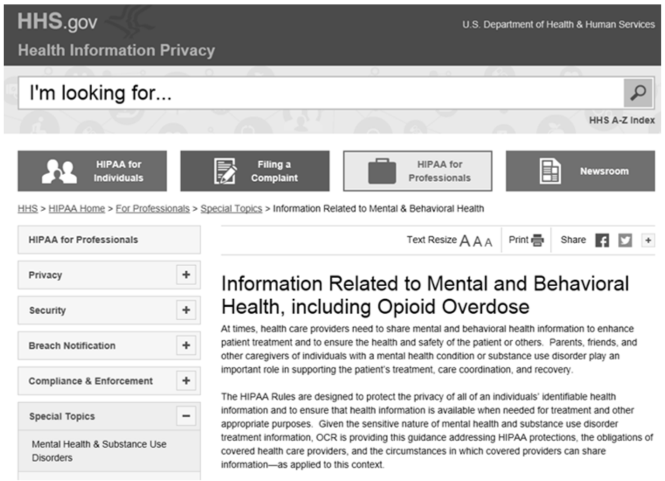
- Requested data submitted on July 20, 2016
- Anticipated OCR response: October 22, 2016
- Actual OCR response received June 2, 2017



Lessons learned

- Prepare early by reviewing OCR’s website
- Laborious process
- OCR scoring system is tough (1-5)
- Will your CEO/Board understand a negative rating?
- Who are policies written for?

OCR Update: Opioids and Behavioral Health



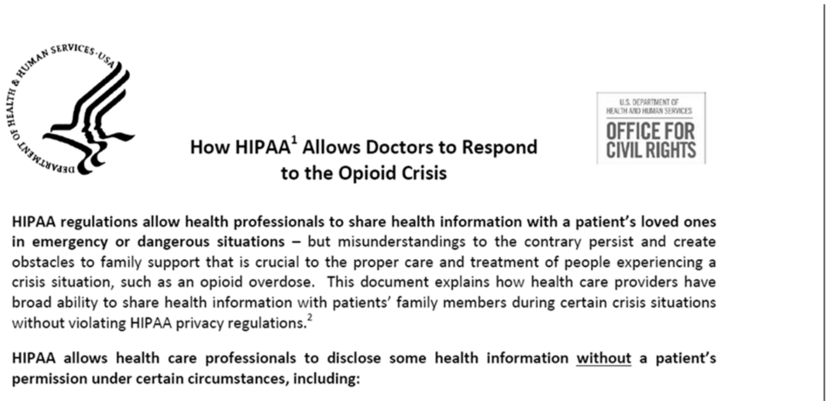
HHS > HIPAA Home > For Professionals > Special Topics > Information Related to Mental & Behavioral Health

Information Related to Mental and Behavioral Health, including Opioid Overdose

At times, health care providers need to share mental and behavioral health information to enhance patient treatment and to ensure the health and safety of the patient or others. Parents, friends, and other caregivers of individuals with a mental health condition or substance use disorder play an important role in supporting the patient's treatment, care coordination, and recovery.

The HIPAA Rules are designed to protect the privacy of all of an individuals' identifiable health information and to ensure that health information is available when needed for treatment and other appropriate purposes. Given the sensitive nature of mental health and substance use disorder treatment information, OCR is providing this guidance addressing HIPAA protections, the obligations of covered health care providers, and the circumstances in which covered providers can share information—as applied to this context.

OCR Update: Opioids and Behavioral Health



DEPARTMENT OF HEALTH & HUMAN SERVICES·USA
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

How HIPAA[1] Allows Doctors to Respond to the Opioid Crisis

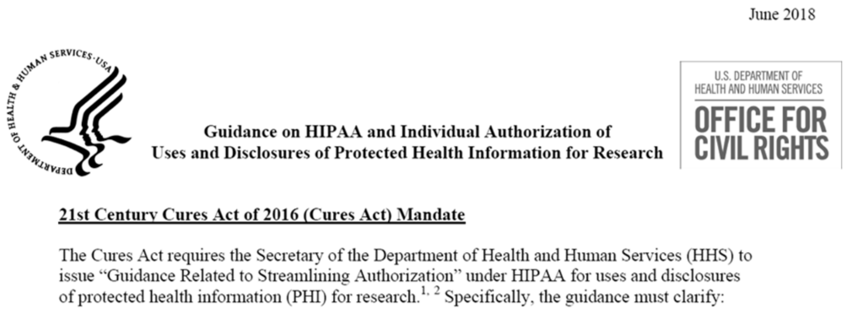
HIPAA regulations allow health professionals to share health information with a patient's loved ones in emergency or dangerous situations – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose. This document explains how health care providers have broad ability to share health information with patients' family members during certain crisis situations without violating HIPAA privacy regulations.[2]

HIPAA allows health care professionals to disclose some health information <u>without</u> a patient's permission under certain circumstances, including:

OCR Update: Opioids and Behavioral Health

- fn 5
- HIPAA still requires that a disclosure to prevent or lessen a serious and imminent threat must be consistent with other applicable laws and ethical standards. 164.512(j)(1). For example, if a state's law is more restrictive regarding the communication of health information (such as the information can only be shared with treatment personnel in connection with treatment), then HIPAA compliance hinges on the requirements of the more restrictive state law.

OCR Update: Research



June 2018

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research

21st Century Cures Act of 2016 (Cures Act) Mandate

The Cures Act requires the Secretary of the Department of Health and Human Services (HHS) to issue "Guidance Related to Streamlining Authorization" under HIPAA for uses and disclosures of protected health information (PHI) for research.[1, 2] Specifically, the guidance must clarify:

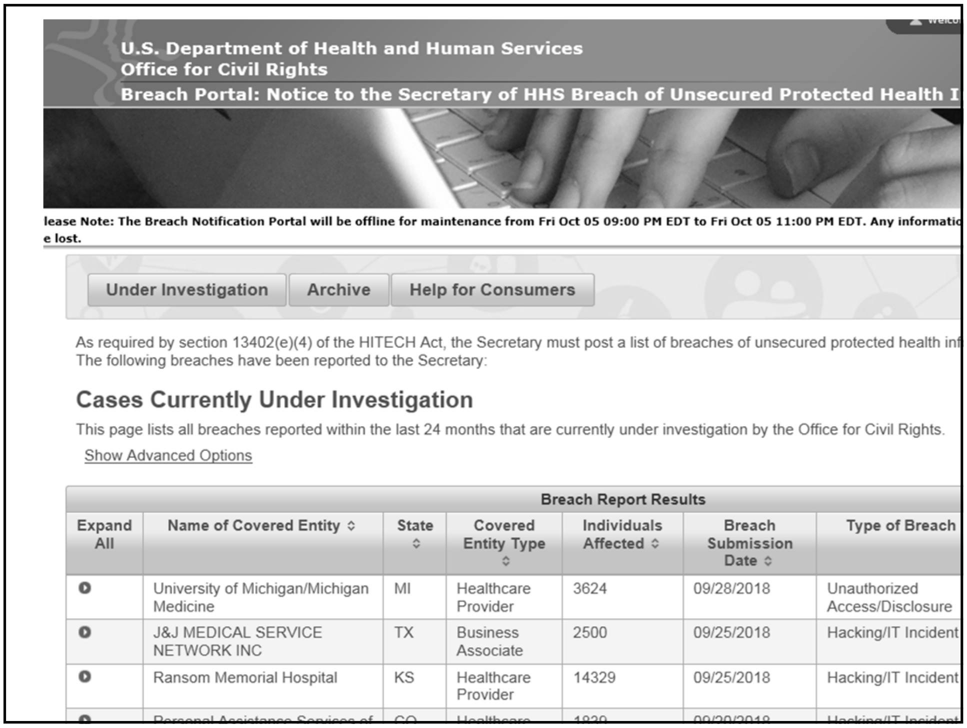
OCR Update: Resolutions and Awards

Three settlements:

- ❖ Anthem - $16 million
- ❖ Fresenius - $3.5 million
- ❖ Filefax, Inc. - $100,000
- ❖ Boston Medical Center, Brigham and Women’s Hospital, and Mass. General Hospital – total $999,000

Litigated resolution:

- ❖ UT MD Anderson Cancer Center - $4.348 million



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health I

lease Note: The Breach Notification Portal will be offline for maintenance from Fri Oct 05 09:00 PM EDT to Fri Oct 05 11:00 PM EDT. Any informatio
e lost.

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health inf
The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

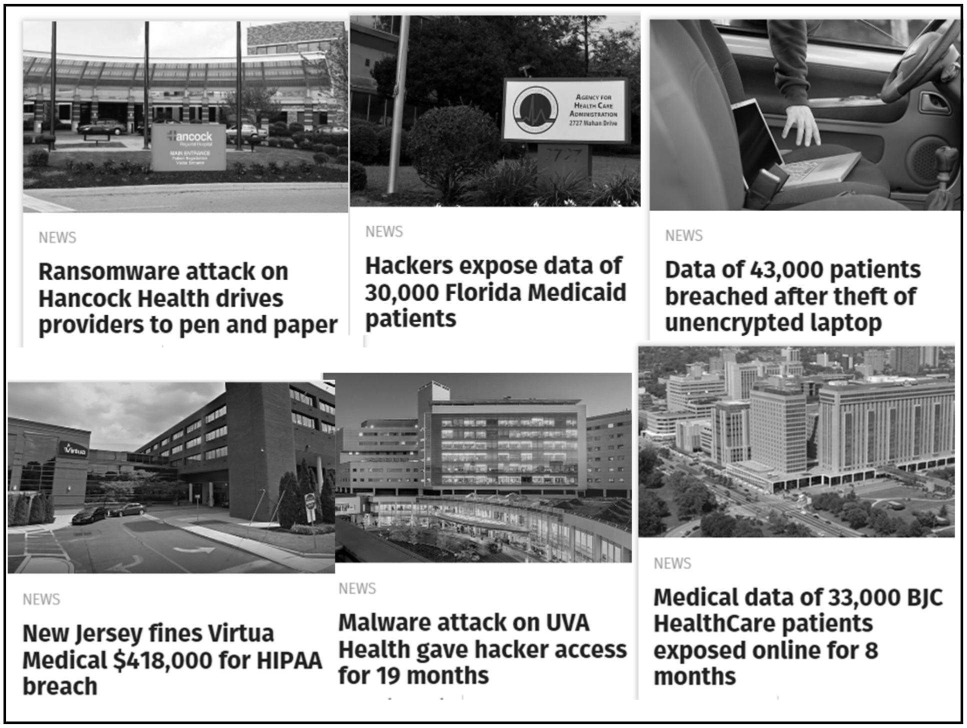
Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach
●	University of Michigan/Michigan Medicine	MI	Healthcare Provider	3624	09/28/2018	Unauthorized Access/Disclosure
●	J&J MEDICAL SERVICE NETWORK INC	TX	Business Associate	2500	09/25/2018	Hacking/IT Incident
●	Ransom Memorial Hospital	KS	Healthcare Provider	14329	09/25/2018	Hacking/IT Incident
●	Personal Assistance Services of	CO	Healthcare	1820	09/20/2018	Hacking/IT Incident

Recurring Compliance Issues

- Business Associate Agreements/ Vendor management
- Incomplete or inaccurate risk analyses
- Failure to manage identified risks
- Lack of transmission security
- Lack of appropriate auditing and testing
- Failure to patch/update software
- Insider threat (ineffective training)
- Improper disposal



NEWS

Ransomware attack on Hancock Health drives providers to pen and paper

NEWS

Hackers expose data of 30,000 Florida Medicaid patients

NEWS

Data of 43,000 patients breached after theft of unencrypted laptop

NEWS

New Jersey fines Virtua Medical $418,000 for HIPAA breach

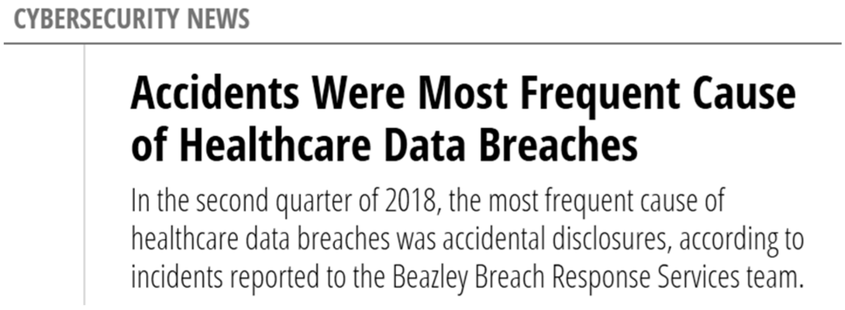
NEWS

Malware attack on UVA Health gave hacker access for 19 months

NEWS

Medical data of 33,000 BJC HealthCare patients exposed online for 8 months

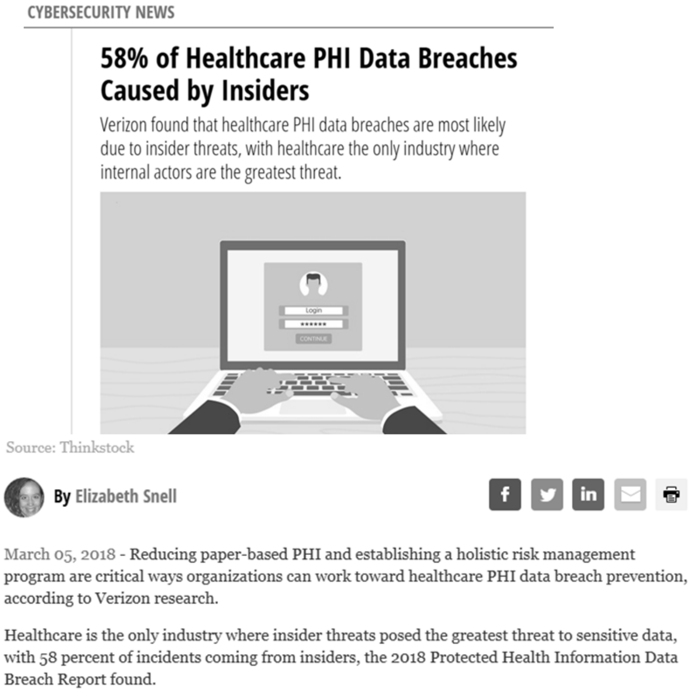
Recurring Compliance Issues



CYBERSECURITY NEWS

Accidents Were Most Frequent Cause of Healthcare Data Breaches

In the second quarter of 2018, the most frequent cause of healthcare data breaches was accidental disclosures, according to incidents reported to the Beazley Breach Response Services team.



CYBERSECURITY NEWS

58% of Healthcare PHI Data Breaches Caused by Insiders

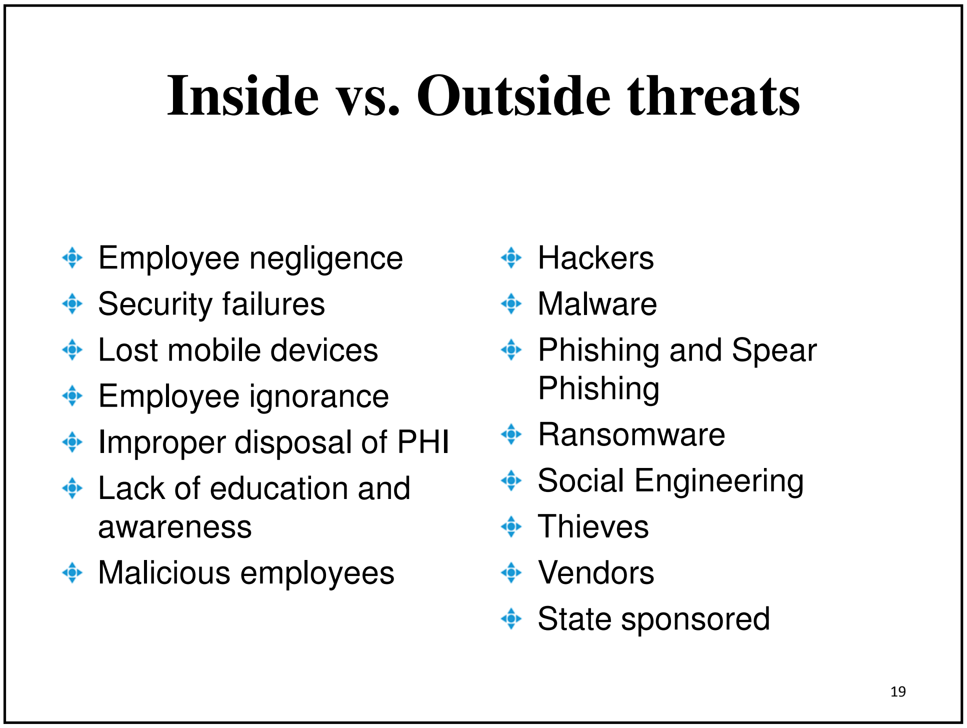
Verizon found that healthcare PHI data breaches are most likely due to insider threats, with healthcare the only industry where internal actors are the greatest threat.

Source: Thinkstock

By Elizabeth Snell

March 05, 2018 - Reducing paper-based PHI and establishing a holistic risk management program are critical ways organizations can work toward healthcare PHI data breach prevention, according to Verizon research.

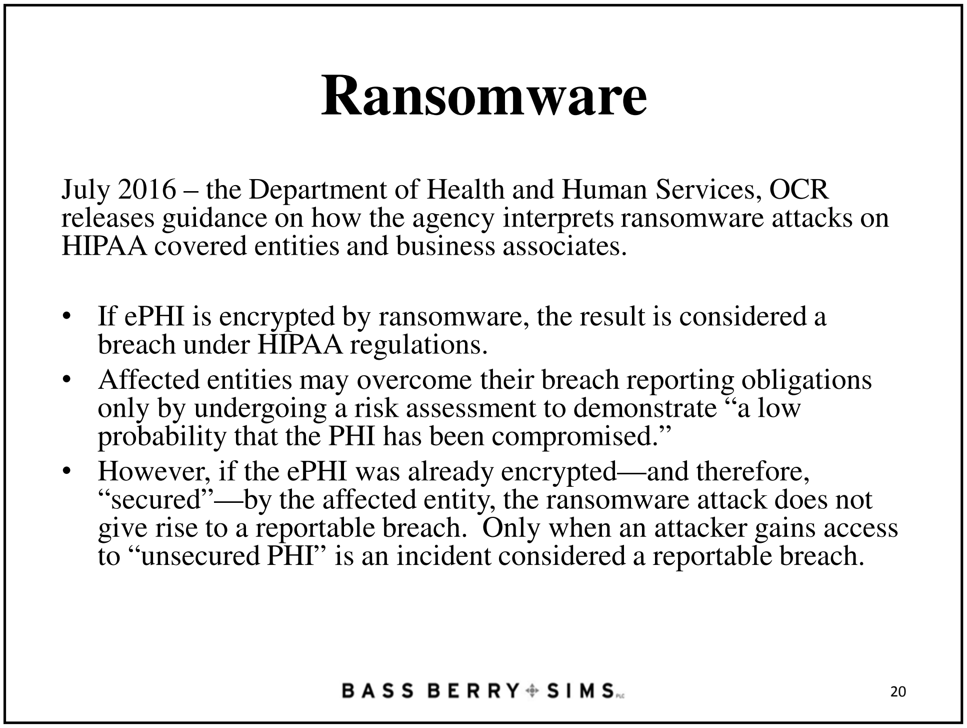
Healthcare is the only industry where insider threats posed the greatest threat to sensitive data, with 58 percent of incidents coming from insiders, the 2018 Protected Health Information Data Breach Report found.



Inside vs. Outside threats

- Employee negligence
- Security failures
- Lost mobile devices
- Employee ignorance
- Improper disposal of PHI
- Lack of education and awareness
- Malicious employees

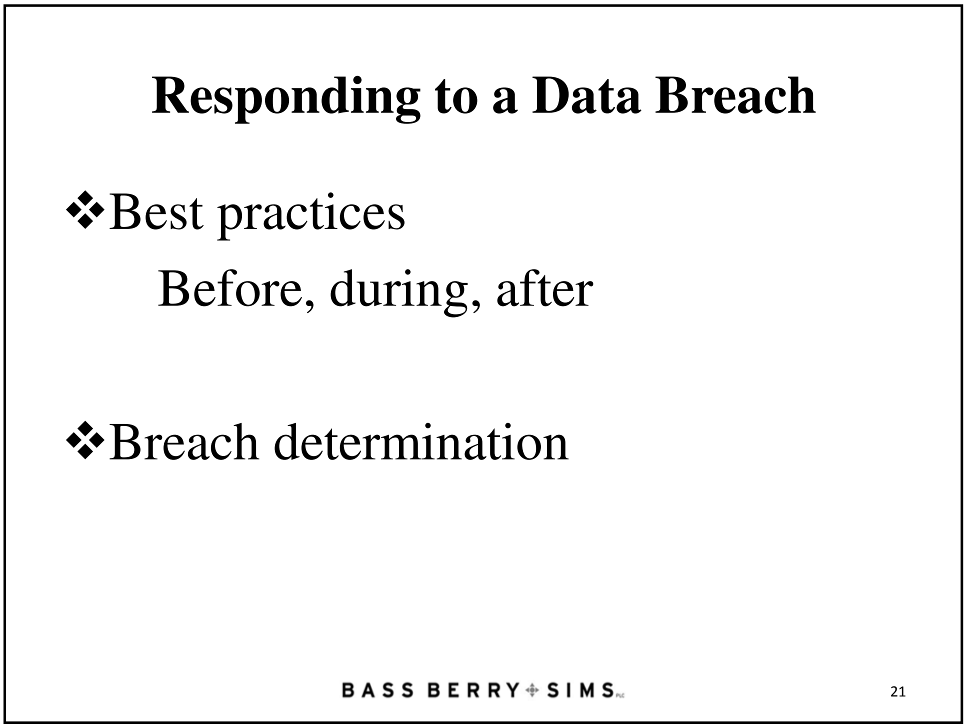
- Hackers
- Malware
- Phishing and Spear Phishing
- Ransomware
- Social Engineering
- Thieves
- Vendors
- State sponsored



Ransomware

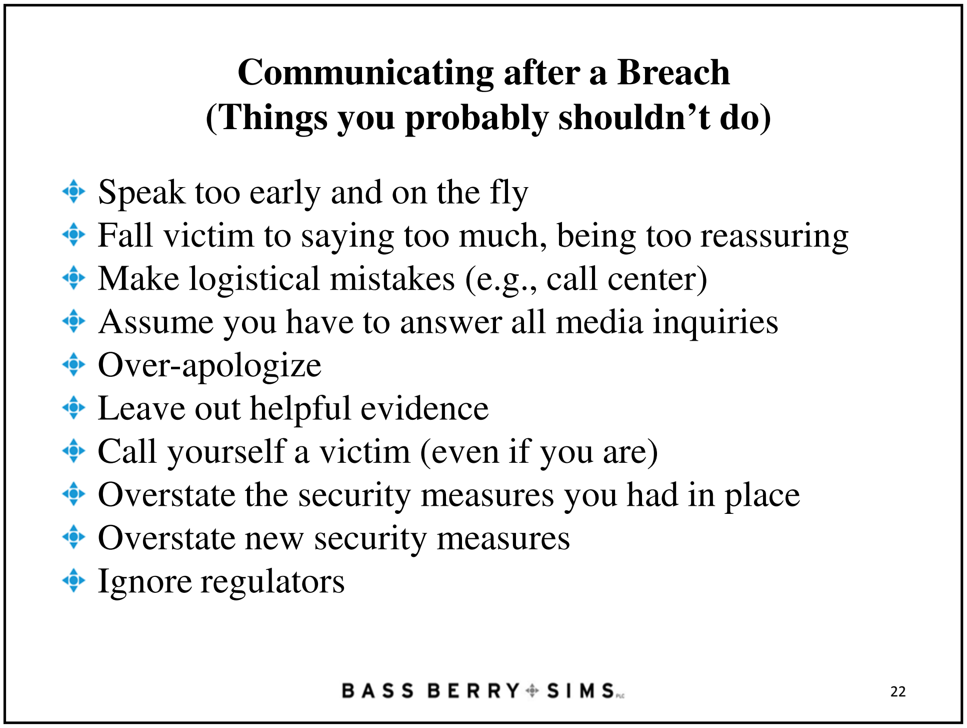
July 2016 – the Department of Health and Human Services, OCR releases guidance on how the agency interprets ransomware attacks on HIPAA covered entities and business associates.

- If ePHI is encrypted by ransomware, the result is considered a breach under HIPAA regulations.
- Affected entities may overcome their breach reporting obligations only by undergoing a risk assessment to demonstrate "a low probability that the PHI has been compromised."
- However, if the ePHI was already encrypted—and therefore, "secured"—by the affected entity, the ransomware attack does not give rise to a reportable breach. Only when an attacker gains access to "unsecured PHI" is an incident considered a reportable breach.



Responding to a Data Breach

- ❖Best practices
  - Before, during, after
- ❖Breach determination



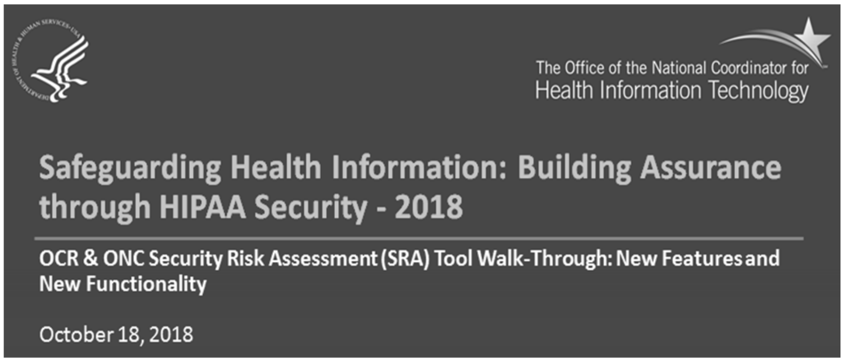
Communicating after a Breach (Things you probably shouldn't do)

- Speak too early and on the fly
- Fall victim to saying too much, being too reassuring
- Make logistical mistakes (e.g., call center)
- Assume you have to answer all media inquiries
- Over-apologize
- Leave out helpful evidence
- Call yourself a victim (even if you are)
- Overstate the security measures you had in place
- Overstate new security measures
- Ignore regulators

What do Regulators expect?

- Transparency
- Prompt and thorough investigation
- Good attitude & cooperation
- Appropriate and prompt notification
- Corrective action (know the root cause and address it; staff training; awareness program; technical safeguards; new policies/procedures/physical safeguards)
- Remediation and mitigation

Recent Myths Addressed by OCR

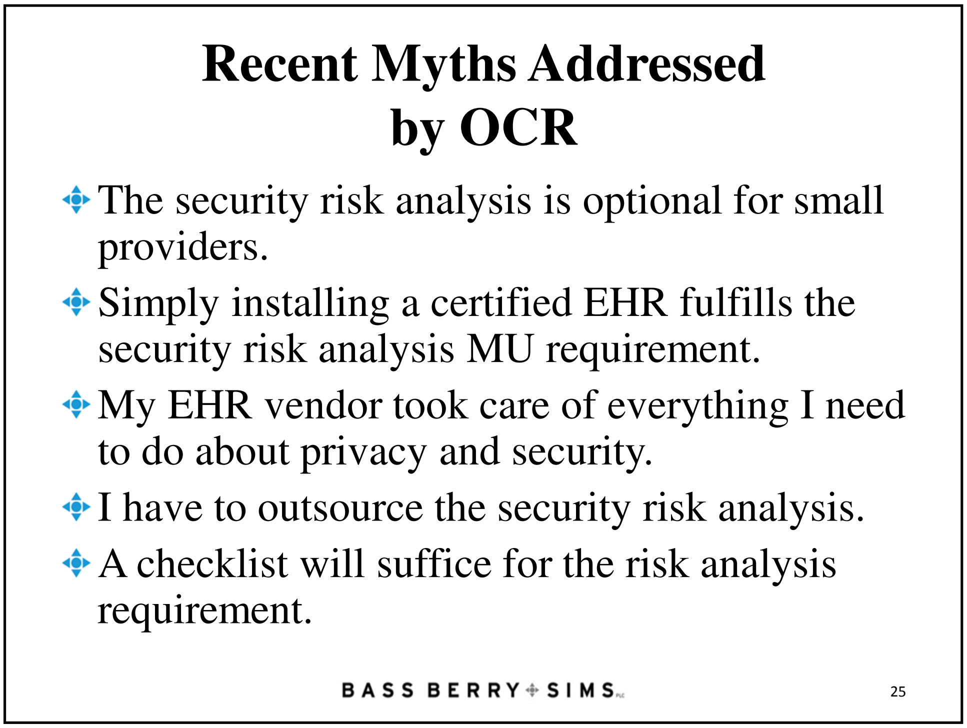


The Office of the National Coordinator for
Health Information Technology

Safeguarding Health Information: Building Assurance through HIPAA Security - 2018

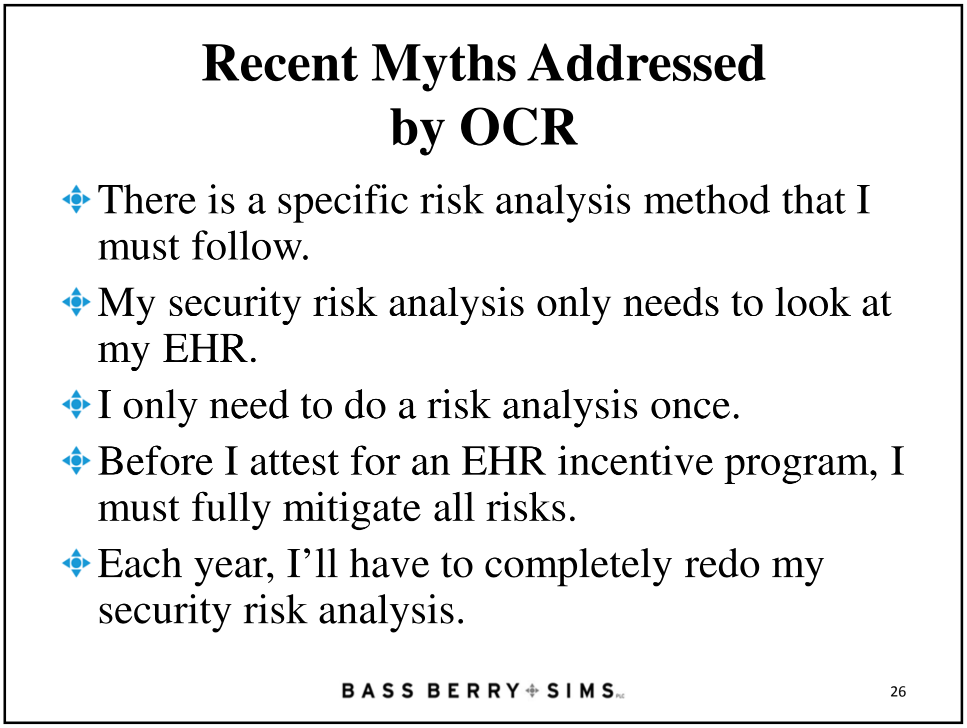
OCR & ONC Security Risk Assessment (SRA) Tool Walk-Through: New Features and New Functionality

October 18, 2018



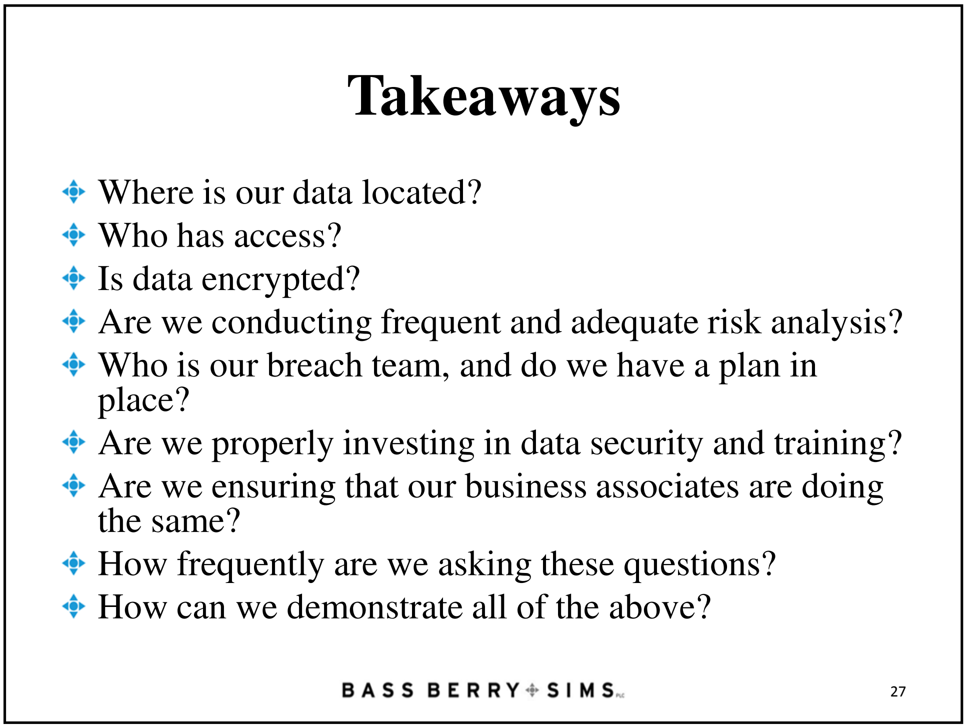
Recent Myths Addressed by OCR

- The security risk analysis is optional for small providers.
- Simply installing a certified EHR fulfills the security risk analysis MU requirement.
- My EHR vendor took care of everything I need to do about privacy and security.
- I have to outsource the security risk analysis.
- A checklist will suffice for the risk analysis requirement.



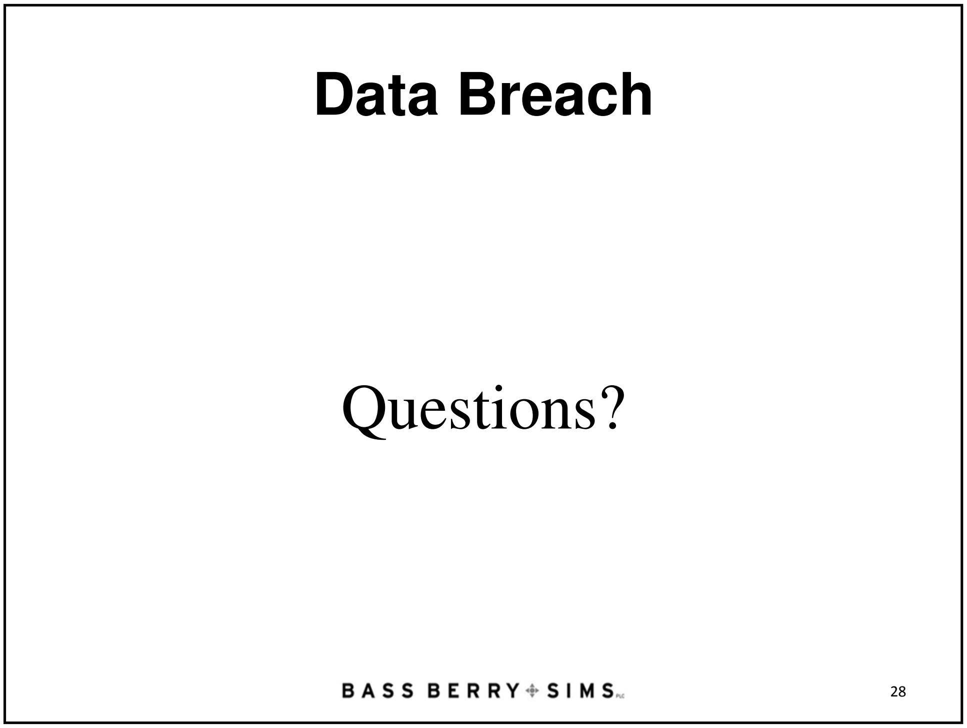
Recent Myths Addressed by OCR

- There is a specific risk analysis method that I must follow.
- My security risk analysis only needs to look at my EHR.
- I only need to do a risk analysis once.
- Before I attest for an EHR incentive program, I must fully mitigate all risks.
- Each year, I'll have to completely redo my security risk analysis.



Takeaways

- Where is our data located?
- Who has access?
- Is data encrypted?
- Are we conducting frequent and adequate risk analysis?
- Who is our breach team, and do we have a plan in place?
- Are we properly investing in data security and training?
- Are we ensuring that our business associates are doing the same?
- How frequently are we asking these questions?
- How can we demonstrate all of the above?



Data Breach

Questions?