Cyber Hot Topics Webinar Series:

HIPAA Comes of Age: 21 Years of Privacy and Security

August 17, 2017
11:30AM – 12:30PM CST

Presented by: Andrew Elbon, Judd A. Harwood, Amy S. Leopard, and Jordan A. Stivers

Welcome from the Bradley Cybersecurity and Privacy Team

Breach Incident Response

- 17 attorneys in 4 offices
  - Healthcare
  - IP
  - Financial Services and Banking
  - Litigation
  - Government Contracts
  - Insurance coverage issues

Health Information and Technology (HIT)

- Compliance Training and HIPAA audits
- Operational and Regulatory Guidance
- Contracting
  - Data Sharing
  - Outsourcing/ IT Procurement
  - Vendor Management
- Due Diligence

Next Webinar:

Cyber Hot Topics: Vendor Management
September 20, 2017

Presenters

Judd A. Harwood
Birmingham

Amy S Leopard
Nashville

Andrew Elbon
Nashville

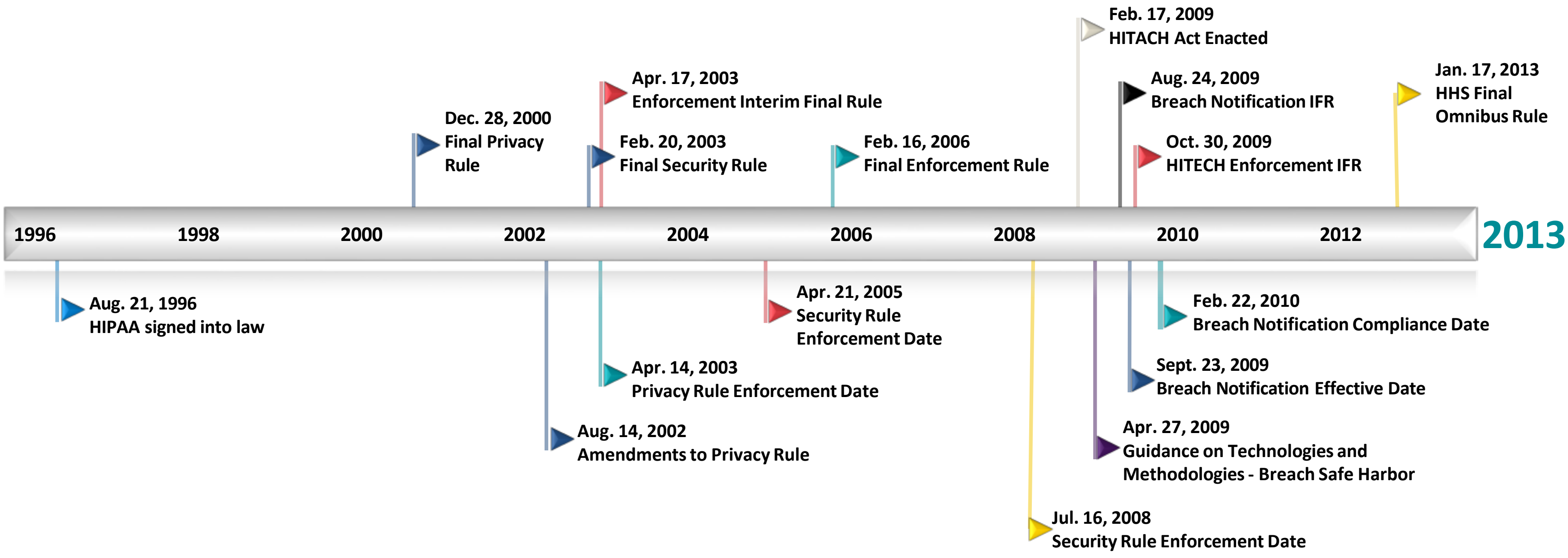
Jordan A. Stivers
Nashville

Agenda

- Important HIPAA developments over 21 years
- The Enforcement Focus
- The Cybersecurity Imperative
- Impact on Health Plans
- Digital Health

HIPAA Through the Years

HIPAA Through the Years.



Aug. 21, 1996
HIPAA signed into law

Dec. 28, 2000
Final Privacy
Rule

Aug. 14, 2002
Amendments to Privacy Rule

Feb. 20, 2003
Final Security Rule

Apr. 14, 2003
Privacy Rule Enforcement Date

Apr. 17, 2003
Enforcement Interim Final Rule

Apr. 21, 2005
Security Rule
Enforcement Date

Feb. 16, 2006
Final Enforcement Rule

Jul. 16, 2008
Security Rule Enforcement Date

Feb. 17, 2009
HITACH Act Enacted

Apr. 27, 2009
Guidance on Technologies and
Methodologies - Breach Safe Harbor

Aug. 24, 2009
Breach Notification IFR

Sept. 23, 2009
Breach Notification Effective Date

Oct. 30, 2009
HITECH Enforcement IFR

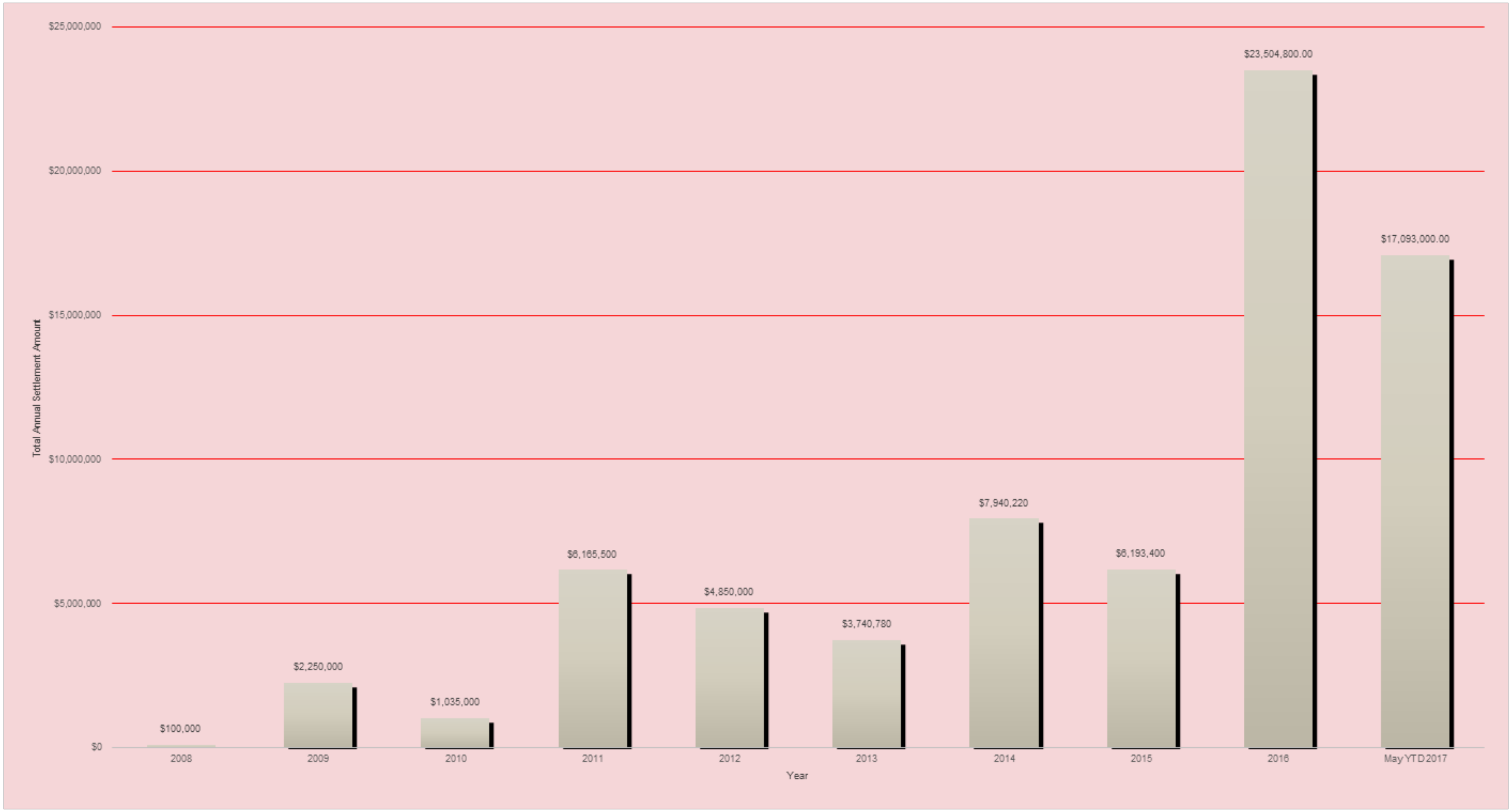
Feb. 22, 2010
Breach Notification Compliance Date

Jan. 17, 2013
HHS Final
Omnibus Rule

Enforcement

HITECH Civil Penalties for HIPAA Violations

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations of identical prohibition/requirement	$50,000 per violation, with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations of identical prohibition/requirement	$50,000 per violation, with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations of identical prohibition/requirement	$50,000 per violation, with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement	$50,000 per violation, with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement



OCR Resolution Agreements: 2008-YTD 2017 = > $73M

- Corrective Action Plans (CAPs) in most cases
- 2016: malware/SRA and covered entity BAA compliance
- May 2017 YTD: $17M (despite transition of Administration)

OCR Resolution Agreements - Types

Security	
Devices and Media Controls/encryption	$$$$
Incomplete Security Risk Analysis/Sec Mgt.	$$$
Software patches, malware	$$
BAA	$
Improper Disclosure	$

Privacy	
Improper Disclosure	$$
Lack of BAA	$$
Improper Disposal	$$
Remote PHI	$$
Patient Access to Records	$$
Breach Notification	
Late Breach Notice	$

Office for
Civil Rights

U.S. HHS OCR Compliance Review Data Request (Complaint or Breach)

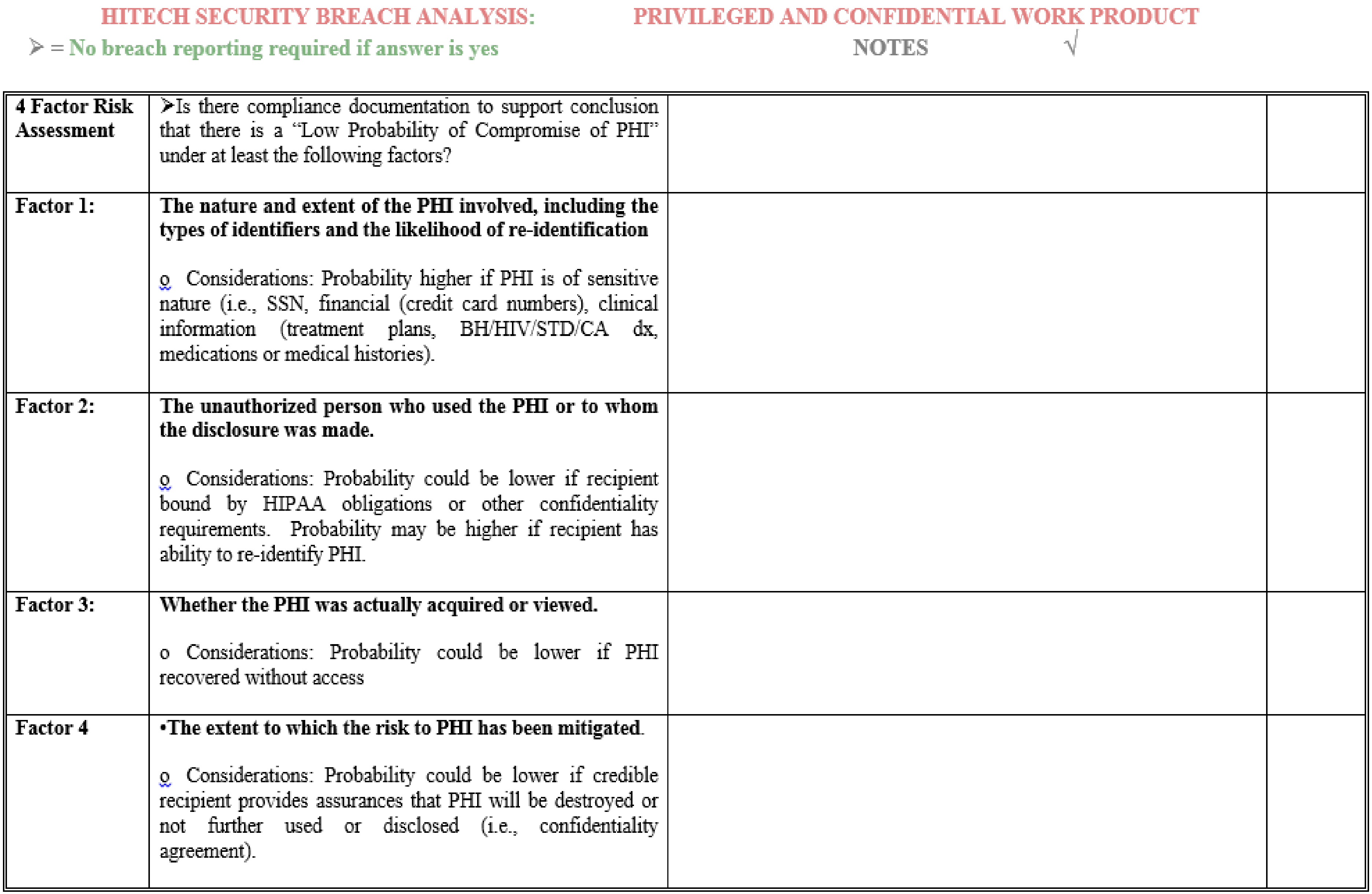
OCR REFERENCE NUMBER: 17-XXXXX

Dear Privacy Officer - The HHS Office for Civil Rights (OCR) is performing a compliance review to assess [Entity's] compliance with federal health information privacy and security requirements . . . **Please provide the following information *[within 20-30 days]:***

- Most recent accurate and thorough **enterprise-wide assessment** of **potential risks and vulnerabilities** to confidentiality, integrity, and availability of e-PHI held by Entity ("Enterprise Risk Analysis") § 160.308(a)(1)(ii)(A)
- Evidence of security measures implemented to reduce risks identified through the Risk Analysis
- Evidence of [Physical] [Technical][Administrative] Safeguards implemented to safeguard PHI
- Evidence of implementation of [virus protection] [a mechanism to encrypt PHI] maintained by Entity
- Documentation and policies re: breach notification of unsecured PHI to individuals, OCR, and media
- Documentation of **internal investigation** conducted by Entity in response, including incident report
- Documentation of corrective action to prevent type of incident from happening again, addressing:
- Evidence Entity evaluated security safeguards and assessed need for a **new evaluation based on changes to security environment** since last evaluation (e.g., new technology or responses to newly recognized risks) and repeated evaluations as necessary

What have we learned from OCR?

- OCR move to broaden inquiry toward enterprise-wide assessments
- Continued focus on basics (SRA, BAA, encryption) with more advanced guidance and tools on cyber
  - How will OCR informal guidance creep into investigations?
- Have ready documentation of remediation when HIPAA standard not met
- Mitigate harm, as required by both HIPAA Privacy and Security Rule
- Retrain and/or sanction workforce members as needed
  - Include training materials used following the breach
  - Sanction those who violate HIPAA Rules or organizational policies
- Careful consideration of internal investigation and incident report
  - Importance of recon and forensics on the nature and scope of the compromise, how to contain and mitigate
  - Preservation of evidence
  - OCR: More qualitative assessment
  - Privilege issues and consider potential class action lawsuits



HITECH SECURITY BREACH ANALYSIS: PRIVILEGED AND CONFIDENTIAL WORK PRODUCT

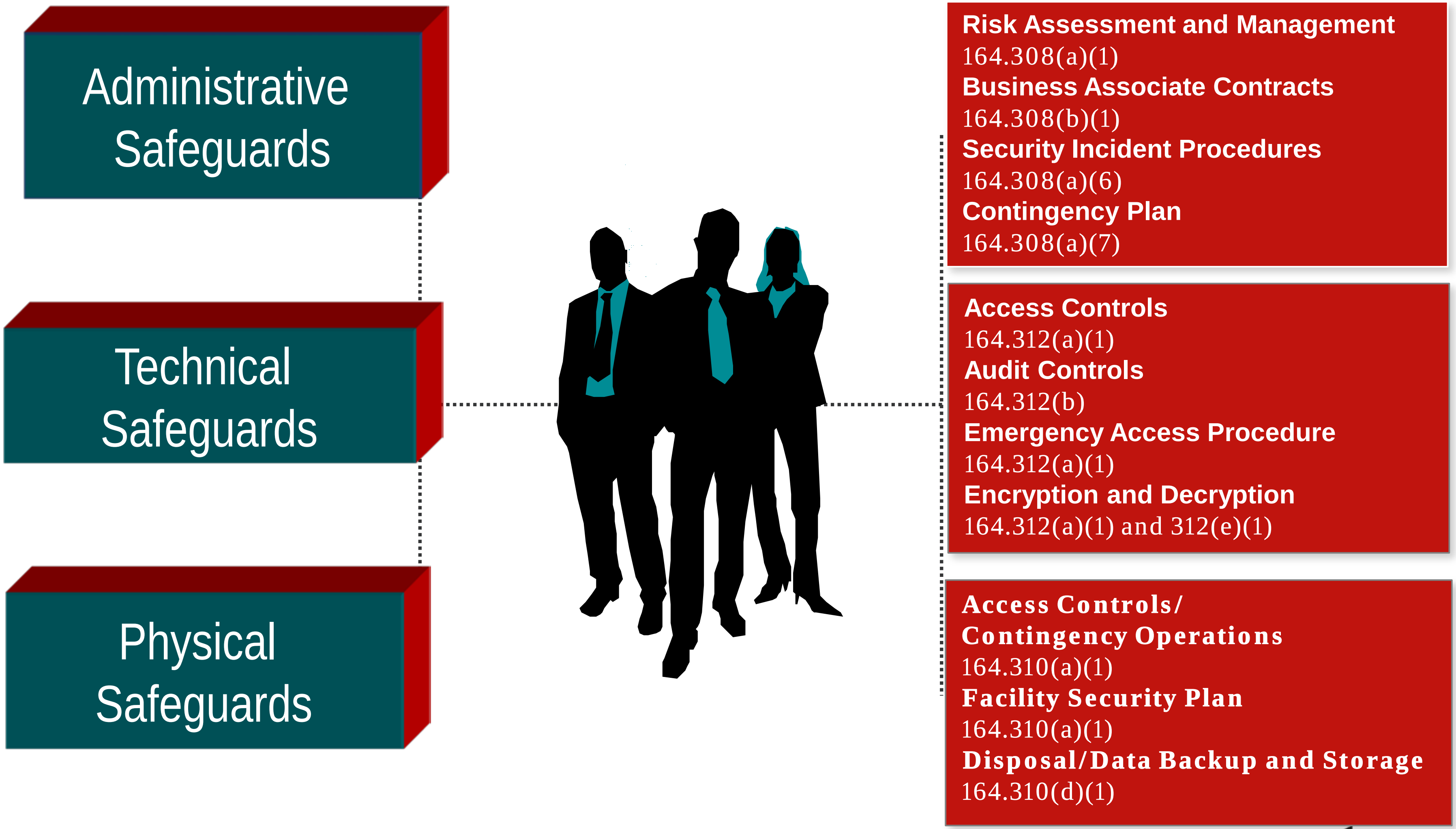
➢ = No breach reporting required if answer is yes NOTES √

4 Factor Risk Assessment	➢Is there compliance documentation to support conclusion that there is a "Low Probability of Compromise of PHI" under at least the following factors?		
Factor 1:	**The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification** o Considerations: Probability higher if PHI is of sensitive nature (i.e., SSN, financial (credit card numbers), clinical information (treatment plans, BH/HIV/STD/CA dx, medications or medical histories).		
Factor 2:	**The unauthorized person who used the PHI or to whom the disclosure was made.** o Considerations: Probability could be lower if recipient bound by HIPAA obligations or other confidentiality requirements. Probability may be higher if recipient has ability to re-identify PHI.		
Factor 3:	**Whether the PHI was actually acquired or viewed.** o Considerations: Probability could be lower if PHI recovered without access		
Factor 4	•**The extent to which the risk to PHI has been mitigated**. o Considerations: Probability could be lower if credible recipient provides assurances that PHI will be destroyed or not further used or disclosed (i.e., confidentiality agreement).		

HIPAA: Breach Risk Assessment = > Low Probability of Compromise factors

The Cybersecurity Imperative

The Cybersecurity Imperative



Administrative Safeguards

Technical Safeguards

Physical Safeguards

Risk Assessment and Management
164.308(a)(1)
Business Associate Contracts
164.308(b)(1)
Security Incident Procedures
164.308(a)(6)
Contingency Plan
164.308(a)(7)

Access Controls
164.312(a)(1)
Audit Controls
164.312(b)
Emergency Access Procedure
164.312(a)(1)
Encryption and Decryption
164.312(a)(1) and 312(e)(1)

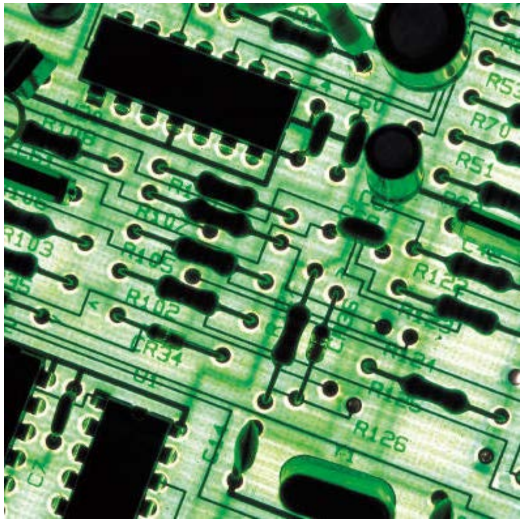
Access Controls/ Contingency Operations
164.310(a)(1)
Facility Security Plan
164.310(a)(1)
Disposal/Data Backup and Storage
164.310(d)(1)

Bradley

OCR Cyber Awareness Initiative

Updated Security Guidance - Cybersecurity Newsletters

Ransomware (2 2016)
Malware and Medical Devices (3 2016)
Cyberthreats and Attacks in Healthcare (3 2016)
BA Preparedness for Security Incidents (5 2016)
Third Party App Vulnerabilities (6 2016)
Cybersecurity Incident Response (7 2016)
Insider Threats (8 2016)
Cyberthreat Information Sharing (9 2016)
FTP Service Threats (10 2016)
Authentication (10 2016)
DoS and DDos Attacks (11 2016)
Audit Controls (1 2017)
Reporting and Monitoring Cyberthreats (2 2017)
Man-in-the-Middle Attacks and HTTPs (4 2017)
Cybersecurity Incident Response (5 2017)
File Sharing and Cloud Computing (6 2017)
Petya Attack (6 2017)
Phishing Attacks … and Training (7 2017)



OCR Quick Response Checklist and Graphic

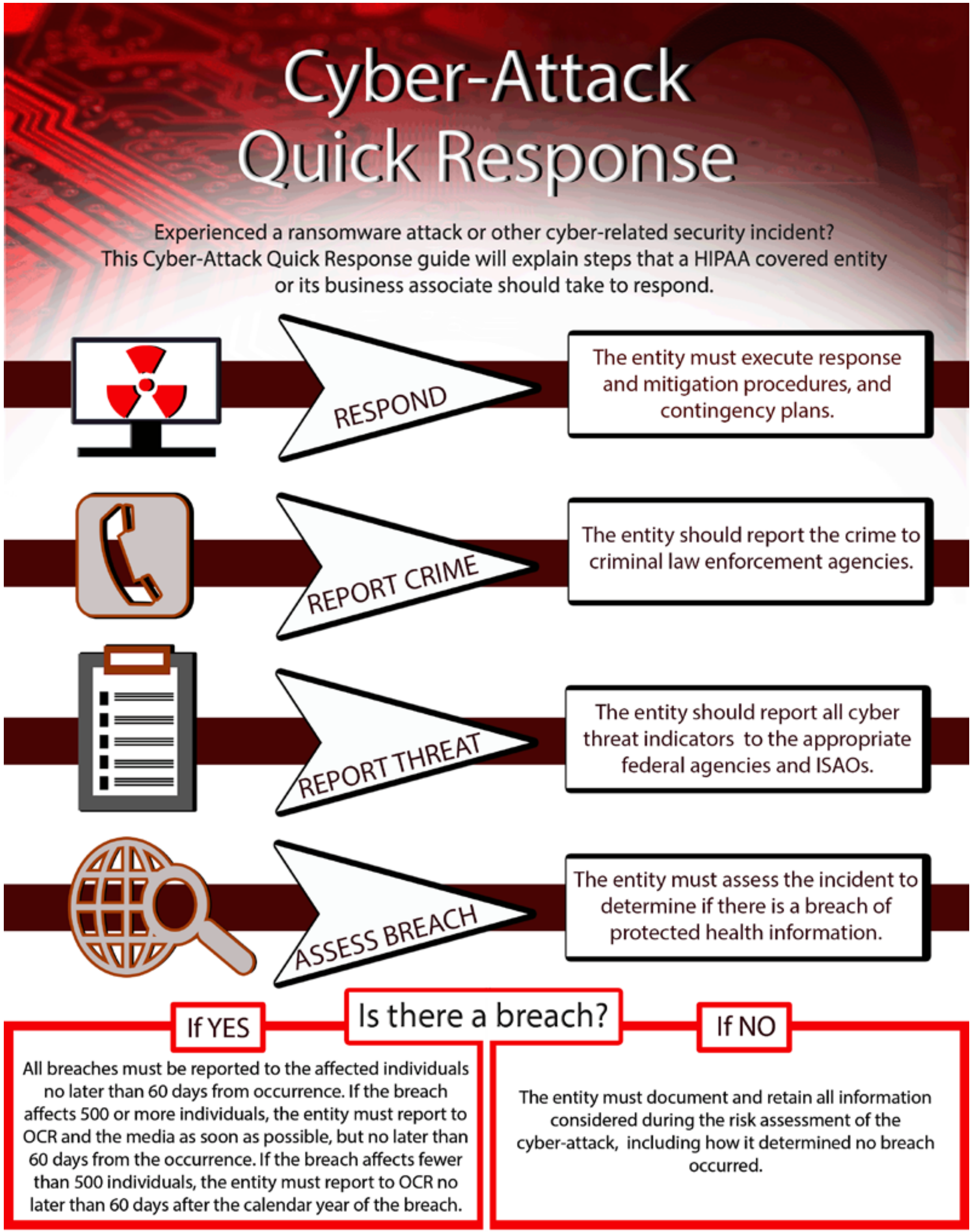
In the event of a cyber-attack or similar emergency an entity:

□ **Must execute its response and mitigation procedures and contingency plans.** For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of PHI, which may be done by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate, if it has access to PHI for that purpose).

□ **Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the FBI, and/or the Secret Service.** Any such reports should not include PHI, unless otherwise permitted by the HIPAA Privacy Rule. If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.

□ **Should report all cyber threat indicators to the appropriate federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs.** Any such reports should not include PHI. OCR does not receive such reports from its federal or HHS partners.

□ **Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting.** OCR presumes all cyber-related security incidents where PHI was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify: individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.



Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident?
This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND — The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME — The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT — The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

ASSESS BREACH — The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

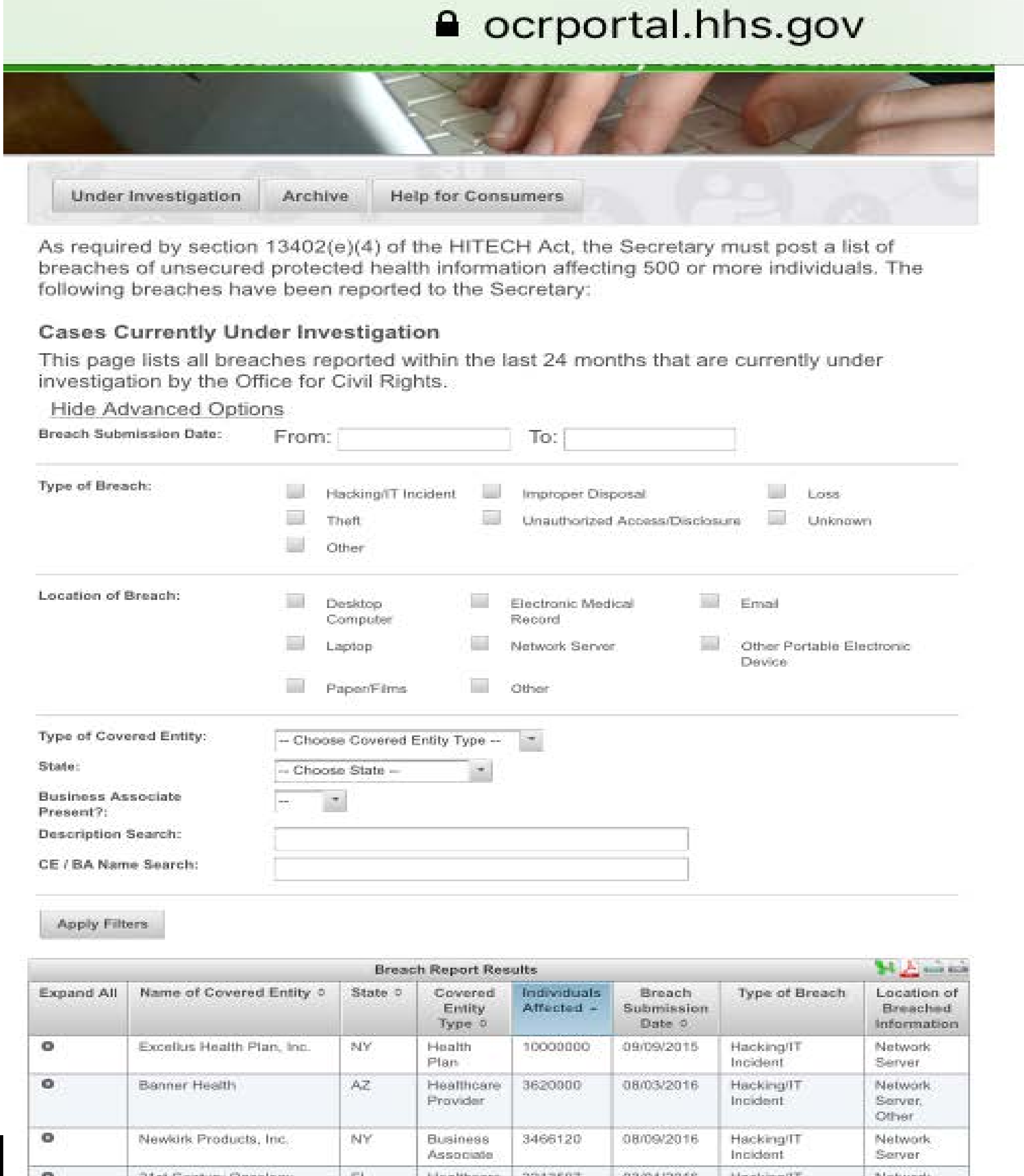
If YES — All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

If NO — The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

New OCR Portal Tool

Case review by type of breach, entity, location, whether closed

Archive with breach resolution shows how resolved



🔒 ocrportal.hhs.gov

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. 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.

Breach Submission Date: From: To:

Type of Breach: ☐ Hacking/IT Incident ☐ Improper Disposal ☐ Loss ☐ Theft ☐ Unauthorized Access/Disclosure ☐ Unknown ☐ Other

Location of Breach: ☐ Desktop Computer ☐ Electronic Medical Record ☐ Email ☐ Laptop ☐ Network Server ☐ Other Portable Electronic Device ☐ Paper/Films ☐ Other

Type of Covered Entity: -- Choose Covered Entity Type --

State: -- Choose State --

Business Associate Present?: --

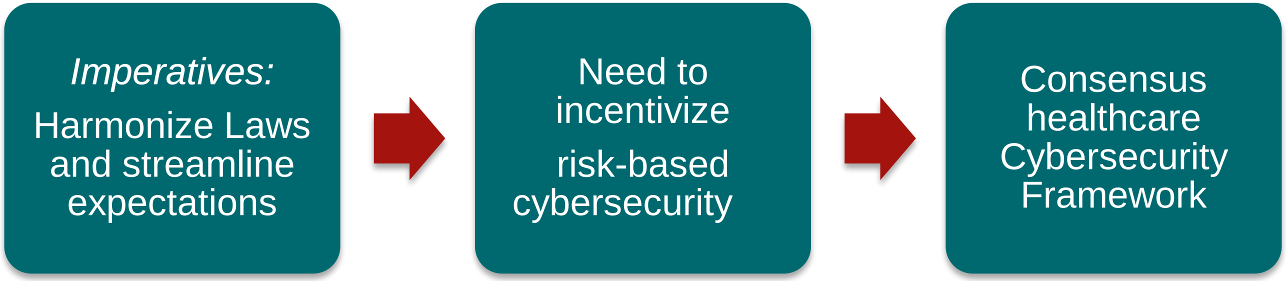
Description Search:

CE / BA Name Search:

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	Excellus Health Plan, Inc.	NY	Health Plan	10000000	09/09/2015	Hacking/IT Incident	Network Server
●	Banner Health	AZ	Healthcare Provider	3620000	08/03/2016	Hacking/IT Incident	Network Server, Other
●	Newkirk Products, Inc.	NY	Business Associate	3466120	08/09/2016	Hacking/IT Incident	Network Server

Where Is Healthcare Cybersecurity Headed?



Imperatives:

Harmonize Laws and streamline expectations

Need to incentivize

risk-based cybersecurity

Consensus healthcare Cybersecurity Framework

- Need Federal Agency harmony (OCR, ONC, CMS, FDA, FTC)
- State Law Patchwork includes Healthcare Regulations in addition to Cyberlaws
  - Unauthorized access, malware viruses – most states
  - DOS attacks – 25 states
  - Some states regulate Ransomware, Spyware, Phishing
- Medical Device/EHR Security
- Need Cybersecurity expertise, awareness and education
- **Industry calling for Cybersecurity Framework built on HIPAA Security Rule and NIST**

Health Care Industry Cybersecurity Task Force
Report on Improving Cybersecurity in the Health Care Industry (June 2017)

Impact on Health Plans

HIPAA Compliance and Group Health Plans

- Fully-insured vs. self-funded plans
  - *Remember health flexible spending accounts*
- Policies and procedures
  - *Identify and train workforce members authorized to use and disclose PHI in the course of performing plan administrative functions*
- Plan amendments
  - *Required content to be included in any covered plan document*
- Business associate agreements
  - *Agreement between the plan and covered service providers*
  - *Must describe the rights and obligations of the parties*

Recent Major HIPAA Security Breaches Involving Group Health Plans

- Real risk: major breaches in 2015
- Premier, Anthem and Excellus
- Group health plan third party administrator response
- Health plan documentation of actions taken on behalf of plan

Business Associate Agreements for Health Plans

- Critical component of HIPAA compliance for group health plans
- Required content for health plans
- Discretionary provisions
  - *Insurance*
  - *Indemnification*
  - *Security Incident/Breach Response*
  - *Destruction of PHI on Termination*

BA Compliance Obligations - Basics

BA Regulatory Obligations

- Security Standards
  - Importance of risk analysis
- Privacy Rule
  - Limits on uses and disclosures
  - Report all impermissible uses and disclosures
  - BAAs with subcontractors
  - Provide electronic access to electronic designated record set
  - Accounting of disclosures
  - Internal records available to HHS
- Breach Notification Rule
  - Reporting to Covered Entity

Contractual Obligation Only

- Safeguards for hard copy, verbal PHI
- Pt. access to hard copy designated record set, amend designated record set
- Comply with Privacy Rule when carrying out CE's Privacy Obligations
- Return or destroy PHI at termination if feasible

Discretionary Provisions – risk allocation

Emerging Uses in Digital Health

Mobile Health Apps

Overview:

- Apps that allow individuals to maintain and monitor their health information, and to transfer health information to their healthcare provider
- Apps that health plans and providers provide to patients to use as a communication tool and to track health indicators

How HIPAA Applies:

- Key distinction is whether the use of the app is initiated by the provider or the individual – has the provider contracted with the app developer?
- HIPAA applies to apps that create, receive, maintain, or transmit PHI *on behalf of covered entities or their business associates*
- HIPAA does not regulate apps designed for use solely by individuals
- Privacy, security, and consent issues

Cloud Services

Cloud Services:

- A service made available to users on demand via the internet from the cloud services provider's (CSP's) servers as opposed to the service being provided from a company's on-premises servers:
  - Data storage
  - Complete software solutions (Ex. Electronic medical records system)
  - Platforms that allow app developers to create new products

How HIPAA applies:

- OCR published guidance on HIPAA and cloud computing in October 2016
- When a covered entity engages a CSP to create, receive, maintain, or transmit ePHI (such as to process or store ePHI) on its behalf, the CSP is a business associate
- Still a business associate *even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data*
- The type of cloud configuration to be used may affect the specific risks to be addressed
- May use service level agreements to address some HIPAA concerns

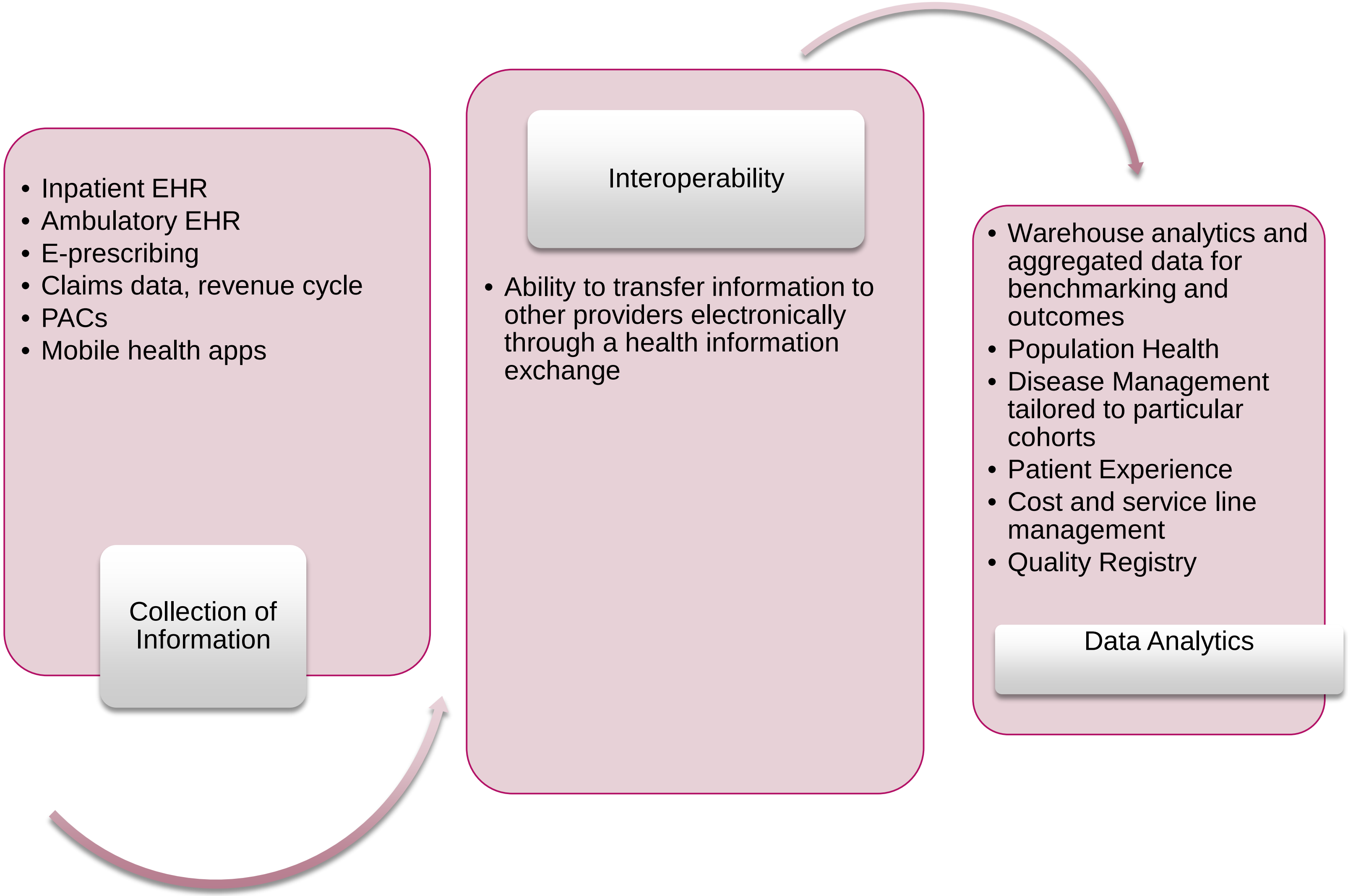
Data Analytics or "Big Data"

Overview:

- The big idea: assess individual cases within the context of an entire population to more easily identify, treat, and prevent illness
- Apply machine learning and artificial intelligence to large stores of health information to identify patterns and similarities – healthcare information no longer siloed to the individual entity that created it
- Big data is used in many industries, most of which are less regulated than healthcare

How HIPAA Applies:

- Many health IT vendors that perform data analytics also provide other health IT products and services (EHR systems, cloud-based software, etc.) and are business associates under HIPAA
- Generally prohibited from using PHI for purposes other than providing services to covered entities in accordance with services agreement, except:
  - Management and administration of BA
  - Data aggregation
  - De-identification
- Does data analytics fall under these?



Collection of Information

- Inpatient EHR
- Ambulatory EHR
- E-prescribing
- Claims data, revenue cycle
- PACs
- Mobile health apps

Interoperability

- Ability to transfer information to other providers electronically through a health information exchange

Data Analytics

- Warehouse analytics and aggregated data for benchmarking and outcomes
- Population Health
- Disease Management tailored to particular cohorts
- Patient Experience
- Cost and service line management
- Quality Registry

21st Century Cures: Prohibits “Information Blocking”

- Applies to HIT Developers, HIEs and Networks, and Healthcare providers
  - ONC to implement standardized process for public to submit claims of HIT products or developers not being interoperable or resulting in information blocking
- HHS OIG to investigate and penalize information-blocking practices
  - CMPs up to $1M per violation for HIT Developers, HIEs and Networks
  - Healthcare Providers referred to appropriate agency
- Information Blocking Practices defined
  - Unreasonable and Likely to interfere with, prevent, materially discourage access, exchange, or use of electronic health information
  - Provider: Knows the Practice is Unreasonable and Likely to Interfere
  - HIT Developers, HIEs or Networks: Knows or should know practice likely to interfere
- HHS to identify reasonable and necessary activities through rulemaking. Examples:
  - Restrict authorized access, exchange, or use under applicable state or federal law
  - Implementing HIT in non-standard ways or likely to restrict ability to export complete information sets
  - Impede innovations, advancements in health information access, exchange and use

21st Century Cures **§ 4003 and § 4004**

Questions?

Judd A. Harwood
Birmingham

Amy S Leopard
Nashville

Andrew Elbon
Nashville

Jordan A. Stivers
Nashville

HHS OCR References and Resources

- OCR Protocol for the HIPAA Audit Program
  - www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol2.html
- HHS Data Blocking FAQ
  - www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html
- HIPAA Access Guidance
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs
- Health App Developer Portal
  - https://hipaaqsportal.hhs.gov/a/index
- OCR Breach Portal
  - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS OCR References and Resources - Security

- *OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule*
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- *ONC/OCR Security Risk Assessment Tool*
  - www.healthit.gov/providers-professionals/security-risk-assessment
  - See also NIST Guide for Conducting Risk Assessment September 2012
- HHS Cloud Guidance:
  - www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- HHS Ransomware Guidance
  - www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- *OCR Security Rule Guidance Material*
  - *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html*
  - *See also NIST Special Publication 800-88 Guidelines for Media Sanitization*