Data Breach Webinar Series: Hot Topics in Healthcare

September 21, 2016

11:30 a.m. – 12:15 p.m. CST

Presented by:

Amy S. Leopard
Nashville

Travis Lloyd
Nashville

Jordan Stivers
Nashville

Agenda

- Recent OCR Ransomware Guidance
- Current OCR Enforcement Activities
- OCR Phase 2 Audit Program

Bradley

Recent OCR Ransomware Guidance

Bradley

Defining Ransomware

- Type of malware that 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 a ransom to the hacker (usually in the form of a cryptocurrency, such as Bitcoin), in order to receive a decryption key
- Infection often occurs through phishing messages
- It is estimated that there have been approximately 4,000 ransomware attacks per day since early 2016, an increase of 300% from 2015
- **88% of ransomware attacks in the second quarter of 2016 were against healthcare entities**

Bradley

OCR Ransomware Guidance

- Fact sheet released July 11, 2016, describing ransomware prevention and recovery from a health care sector perspective
- Comply with HIPAA Security Rule at a minimum, and consider the adoption of more stringent security measures that specifically take the threat of ransomware into account
- In the event of a ransomware attack, initiate the security incident and response and reporting procedures
- When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the Privacy Rule
- Must conduct a risk assessment to determine the extent of the breach, and resulting breach notification requirements

Bradley

OCR Ransomware Guidance

- Risk assessment after a ransomware attack should take into account:
  - The exact type and variant of the malware discovered
  - The algorithmic steps undertaken by the malware
  - Communications, including destruction or exfiltration attempts, between the malware and the attackers' command and control servers
  - Whether or not the malware propagated to other systems, potentially affecting additional sources of ePHI
  - The impact the ransomware had on the integrity of the ePHI (consider whether there are backups or whether the data can be restored)

To Pay or Not to Pay?

- The ransom amount is usually relatively low, likely to encourage payment
- The FBI has recommended that entities **not** pay the ransom, as doing so encourages further ransomware attacks
- There is no good data on the number of entities who have paid a ransom, but it is estimated that many have because they could otherwise not recover data essential to their business
- Consider the nature of the information at issue and the quality of your organization's data backup

Bradley

Current OCR Enforcement

Bradley

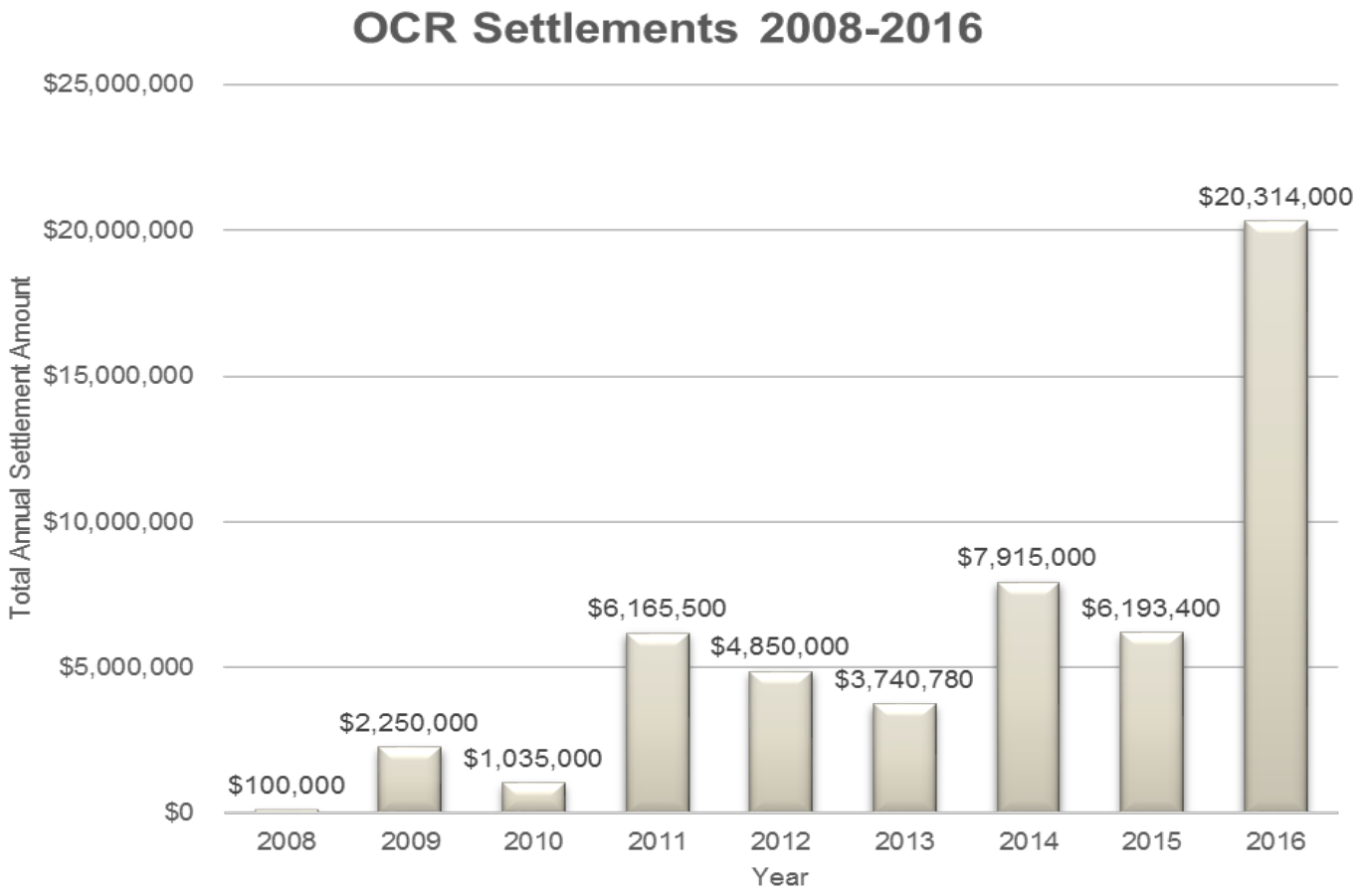
HHS OCR Enforcement

Violation Category	Penalty Range for Each Violation	Maximum Penalty for All Violations of Identical Provision in Calendar Year
Violation due to "willful neglect" but not corrected within the 30-day period.	At least $50,000	$1,500,000
Violation due to willful neglect and corrected during 30-day period beginning on first date the entity knew, or by exercising reasonable due diligence, would have known that the violation occurred.	$10,000 to $50,000	$1,500,000
Violation is due to "reasonable cause" and not to willful neglect.	$1,000 to $50,000	$1,500,000
Entity did not know (and, by exercising reasonable diligence, would not have known) that it violated the applicable provision	$100 to $50,000	$1,500,000

Willful neglect: includes reckless indifference to a compliance duty
OCR MUST investigate Big Breaches

Bradley

2016 – Record Year



2016 OCR Resolution Agreements: Cause of Breach

What caused the breach?	$239K Lincare	$25K Complete PT	$1.55M NMHC MN	$3.9M Feinstein	$750K Raleigh Ortho	$2.2M NYP	$650K CHCS	$2.7M OHSU	$2.75M UMMC	$5.55M Advocate
Internet Risks/Technical Safeguards										
Improper Disposal/Handling of PHI	X	X				X				
Stolen Laptop - Device/Media Controls			X	X			X	X	X	X
Failure to Obtain/Manage BAA					X					

Bradley

2016 OCR Resolution Agreements: CAP Requirements

What corrective action was required?	$239K Lincare	$25K Complete PT	$1.55M NMHC MN	$3.9M Feinstein	$750K Raleigh Ortho	$2.2M NYP	$650K CHCS	$2.7M OHSU	$2.75M UMMC	$5.55M Advocate
Security Risk Analysis			X	X			X	X	X	X
Security Risk Management Plan			X	X			X	X	X	X
Review/Revise Policies & Procedures		X	X	X	X	X	X	X	X	X
Implement/Update Training		X	X	X	X	X	X	X	X	X

Bradley

Advocate Settlement - $5.55 Million

- Announced August 4, 2016
- Largest HIPAA settlement to date
- OCR began investigation after receiving 3 breach notification reports within 4 months in 2013
  - 4 unencrypted laptops stolen (approx. 4 million patient records)
  - Breach to BA's network (approx. 2,000 patients affected)
  - Breach to Advocate's ePHI system (approx. 2,000 patients affected)
- OCR said the record-breaking settlement amount was due to the extent and duration of Advocate's noncompliance with data security laws, as well as the number of patients affected by the security violations involving PHI

OCR Phase 2 Audits

Bradley

OCR Phase 2 Audits - Overview

Purpose:

- Identify industry best practices
- Discover risks and vulnerabilities not surfaced through enforcement activities

Procedures:

- 167 covered entities selected at random, representing a wide range of types of providers, health plans, and clearinghouses
- Desk audits of selected covered entities are currently underway, and will continue through the end of 2016
- Desk audits of business associates will begin in October, and the selection pool will be largely comprised of the BAs identified by the CEs in their document responses to OCR in the course of their audits

OCR Phase 2 Audit Focus Areas

- **Privacy Rule**
  - Notice of Privacy Practices & Content Requirements
  - Provision of Notice: Electronic Notice
  - Individuals' right to access their Protected Health Information ("PHI")

- **Security Rule**
  - Risk Analysis
  - Risk Management Process

- **Breach Notification Rule**
  - Timeliness of Notification
  - Content of Notification

Coming Up in 2017 - Onsite Audits

- Comprehensive onsite audits of both covered entities and business associates will begin in early 2017
- Onsite audits will evaluate auditees against a thorough set of HIPAA compliance controls, not limited to the 7 focus areas of desk audits
- A desk auditee may be subject to an onsite audit as well

Bradley

Bradley

HIPAA Audit Protocol: OCR Phase 2 Audit Program

See HHS Office for Civil Rights Official Audit Protocol at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

KEY ACTIVITY	ESTABLISHED PERFORMANCE CRITERIA	IMPLEMENTED	IN PROCESS	NOT IMPLEMENTED	AUDIT INQUIRY	NOTES: RESPONSE, DOCUMENT SOURCES, AND NEXT STEPS
Security Management Process - Risk Analysis	§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the CE or BA.				*Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI (ePHI) it creates, receives, maintains, or transmits?* *Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?* *Determine how the entity has implemented the requirements:* •Obtain and **review** risk analysis policies and procedures. •**Evaluate** and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated. •Obtain and **review** the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. **Evaluate** and determine whether the risk analysis or other documentation contains: • Defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating	

Bradley

How Bradley Can Help

Health IT

- Operational and Regulatory Guidance
- Contracting
  - Data Sharing
  - Procurement
  - Vendor Management
- Compliance Training and HIPAA Audits
- Due Diligence

Breach Incident Response

- Bradley Cybersecurity & Privacy Team
- 15 Attorneys in 4 Offices
- Specialties
  - Healthcare
  - IP
  - Financial
  - Litigation
- Cybercoverage Issues

Bradley

Questions?

aleopard@bradley.com

tlloyd@bradley.com

jstivers@bradley.com

Bradley

Save the Date

OCR-NIST 2016 Conference *Safeguarding Health Information: Building Assurance through HIPAA Security, 10.19-20.16, Washington DC*

Amy Leopard will be on the Provider panel

Bradley Webinar *Hot Topics Roundtable Discussion on Breach Response* : 12.07.07

Our Cybersecurity Team will Walk through a Breach Response Scenario

Bradley