COPPERSMITH BROCKELMAN

LAWYERS

HIPAA Breach Reporting

Kristen Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com

The World's Biggest Data Breaches

- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

COPPERSMITH
BROCKELMAN
LAWYERS

2

Today's Topics

- Determining whether there is a reportable breach under HIPAA
- Deciding the tough calls: real-life case studies
  - Ransomware incidents
  - Hacking where no demonstrated exfiltration of data
- Handling business associate breaches

COPPERSMITH
BROCKELMAN
LAWYERS

3

Determining HIPAA Reporting Obligations

HIPAA Breach Notification - 45 CFR Part 164, Subpart D

"Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the <u>Privacy Rule</u> which compromises the security or privacy of the PHI, except:

- Unintentional acquisition, access or use of PHI by a workforce member in the scope of duties – no further access or disclosure
- Inadvertent disclosure from one authorized person to another within a CE/BA – no further access or disclosure
- Disclosure of PHI where CE/BA has good faith belief that the recipient cannot retain the information

COPPERSMITH
BROCKELMAN
LAWYERS

4

Encryption is Key

- Encryption Safe Harbor
  - Is the PHI "secured" in accordance with the NIST standard for encryption or destruction?
    - If yes, the Safe Harbor applies and notification is not required
    - If no, Risk Assessment should be conducted to determine the probability of compromise to the PHI

COPPERSMITH
BROCKELMAN

5

Presumption of Reporting

- Any unauthorized use or disclosure of PHI/ePHI that does not meet one of the exceptions is *presumed* to be a "Breach" UNLESS the CE/BA can demonstrate (through a written risk assessment) that there is a "low probability that the PHI has been compromised"

  Note: The term "compromise" is no longer defined

COPPERSMITH
BROCKELMAN

6

Title search: HIPAA Breach Reporting

Also available as part of the eCourse
2016 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"HIPAA Breach Reporting"