PREPARE FOR THE INEVITABLE: STRATEGIES FOR SURVIVING A DATA BREACH

Cori McKeever Ashford, Weber Shandwick

Sasha Boghosian, ReviveHealth

Celeste H. Davis, Esq., HIPAA Subject Matter Expert, Former Regional Manager, U.S. Department of Health and Human Services Office for Civil Rights, Midwest Region

September, 2017
U.S. consumers trust healthcare organizations to protect their data — and they may be unforgiving of failure
90% of healthcare organizations have experienced a data breach*

1 in 4 U.S. consumers had personal medical information stolen*

50% had to pay $2,500 in out-of-pocket costs*

*Ponemon Institute Sixth Annual Benchmark Study on Privacy and Data Security of Healthcare Data (2016)

*Accenture 2017 Healthcare Cybersecurity and Digital Trust Research

*Accenture 2017 Healthcare Cybersecurity and Digital Trust Research
50% of organizations have been affected by ransomware.*

Hospitals often use outdated operating systems, leaving them particularly vulnerable.*

*SentinelOne Ransomware Research Data Summary (2016)

*Xu Zou, ZingBox Inc. (2017)
Among those who experienced a breach, 1/3 said it occurred in a hospital, 1/5 each mentioned an urgent care clinic, pharmacy, physician’s office or health insurance company.

*Accenture 2017 Healthcare Cybersecurity and Digital Trust Research*
THE FINANCIAL COSTS ARE STEEP:

HEALTHCARE ORGANIZATIONS
LOST REVENUE PER DATA BREACH
IS AS HIGH AS $113MM

Protenus Cost of a Breach (2017)
HEALTHCARE PROVIDERS THAT DO NOT MAKE CYBERSECURITY A STRATEGIC PRIORITY WILL PUT $305 BILLION OF CUMULATIVE LIFETIME PATIENT REVENUE AT RISK OVER THE NEXT FIVE YEARS*. 

*Accenture The $300 Billion Attack (2015)
IT’S NOT ALL BAD NEWS:

SIGNIFICANTLY MORE CONSUMERS STILL TRUST

88% THEIR HEALTHCARE PROVIDER  
88% AND PAYER  

TO KEEP THEIR HEALTHCARE DATA SECURE

57% THAN TRUST HEALTH TECHNOLOGY COMPANIES  
56% OR THE GOVERNMENT*

WHAT IS OCR’S HIPAA BREACH NOTIFICATION RULE?

The rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

It applies to vendors of personal health records and their third party service providers.
WHAT IS THE DEFINITION OF A BREACH?

A breach is an **impermissible use or disclosure** under the Privacy Rule **that compromises the security or privacy of the protected health information**. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; The unauthorized person who used the protected health information or to whom the disclosure was made; Whether the protected health information was actually acquired or viewed; and The extent to which the risk to the protected health information has been mitigated.
Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.
WHO MUST BE NOTIFIED?

1. INDIVIDUAL
2. MEDIA
3. SECRETARY
7 FIGURE OCR HIPAA RESOLUTION AGREEMENTS – 2017

January 18, 2017
MAPFRE Life Insurance Company of Puerto Rico (MAPFRE)
$2.2 million

February 16, 2017
Memorial Healthcare System
South Florida
$5.5 million

April 24, 2017
CardioNet
Pennsylvania based company.
First OCR settlement involving a wireless health services provider.
$2.5 million

May 10, 2017
Memorial Hermann Health System (MHHS), Houston, Tx
$2.4 million

COMMON THEME?
IT’S THE PEOPLE
Top enforcement priority is to find a “big, juicy, egregious” breach case to use as an example...

ROGER SEVERINO, Director, Office of Civil Rights

Healthcare Info Security, September 5, 2017
REPUTATION MANAGEMENT

CULTURE OF PREPAREDNESS
PANEL DISCUSSION
SASHA BOGHOSIAN
SENIOR VICE PRESIDENT, REVIVEHEALTH

Sasha Boghosian is a communication strategist with nearly two decades of experience in helping high profile clients develop and execute targeted communication programs to overcome controversy, shape their public image, and build grassroots support. He has served as senior vice president at ReviveHealth since 2014, leading the integrated marketing and communication firm’s issues and crisis practice.
CELESTE DAVIS, ESQ.

REGIONAL MANAGER, OFFICE FOR CIVIL RIGHTS; MIDWEST REGION, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

As regional manager, Celeste Davis serves as the chief civil rights enforcement official for the U.S. Department of Health and Human Services in 10 Midwestern states. The Office of Civil Rights (OCR) enforces the HIPAA Privacy and Security Rules, Breach Notification Rule and also enforces federal civil rights laws. Prior to joining OCR in 2007, Celeste was a practicing attorney in the labor and employment arena, including serving as the supervisory attorney for the U.S. Equal Employment Opportunity Commission Mediation Program.
THANK YOU