

Healthcare Data Breaches: How Ransomware Has Changed the Game

May 3, 2017

Presented by Adam Greene and Rick Kam

Learning Objectives

- Understand threats ransomware poses
- Understand how HIPAA guidance on ransomware has changed how organizations should think about breach response

Ransomware

- Malware that encrypts an organization's data
- Demand for the organization pay a ransom to regain access
- Can result in loss of data
- OCR issued guidance concerning ransomware
- Whether ransomware constitutes a breach is a facts and circumstances analysis



HIPAA breach analysis

Step 1 – Is it an impermissible use or disclosure of PHI under Privacy Rule?

- PHI?
- Use or disclosure? Guidance suggests that encryption of ePHI, could be an impermissible disclosure, subject to HIPAA risk assessment
- Impermissible under Privacy Rule

Step 2 – Is the PHI secured through appropriate destruction or encryption?

- Guidance states that encrypted PHI is not subject to notification
- Verify proper encryption



HIPAA breach analysis

- Step 3 – Does a statutory exception apply?
- Unintentional use, good faith, no further impermissible use/disclosure
- Inadvertent disclosure within organization (or OHCA), recipient had authorized access, no further impermissible use/disclosure
- Good faith belief that unauthorized recipient could not retain information

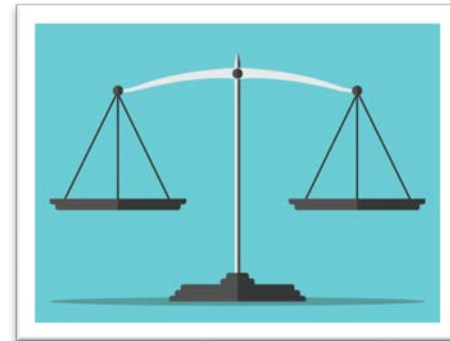


Presumption of breach

Step 4 – Presumption of breach

Step 5 – Can overcome presumption by demonstrating a *low probability of compromise* based on documented breach risk assessment of at least:

- Nature of PHI (e.g., identifiability, sensitivity)
- Unauthorized recipient (e.g., subject to confidentiality requirements?)
- Whether PHI was actually acquired or viewed
- The extent that risk has been mitigated



Presumption of breach

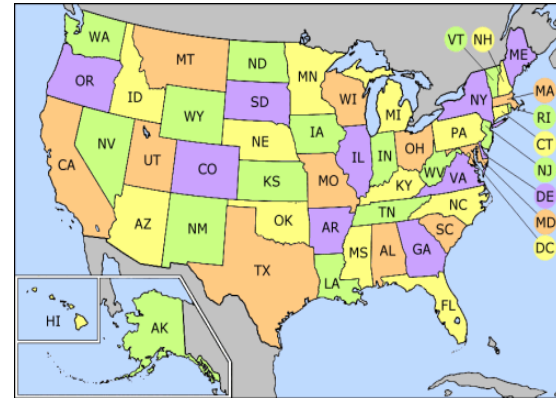
Step 5 (cont'd)

Ransomware guidance introduced new factors:

- High risk of unavailability
- High risk to the integrity of the data

Don't Forget State Law

- 47 state data breach notification statutes (plus Guam, Puerto Rico, Washington D.C., and the Virgin Islands)
- Does state law require breach notification?
 - Definition of covered information?
 - Definition of breach?
 - Risk of a harm threshold?
- Notification may include:
 - Residents of the State
 - State regulatory officials, such as Attorney General
 - Credit reporting agencies
- For information on state breach laws, visit:
<http://www.dwt.com/statedatabreachstatutes/>



Ransomware Considerations

- Risk analysis to include ransomware
- Implement security safeguards
- Information security awareness
- Routinely back up ePHI
- Test your monitoring and incident response processes
- Test your disaster recovery processes
- Consider table-top exercises, with ransomware as a potential scenario
- Cyber insurance with cyber extortion coverage



Healthcare Data Breaches Among U.S. Consumers

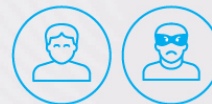
1 in 4

Consumers had their healthcare data stolen



1 in 2

Breaches resulted in identity theft



FROM THESE LOCATIONS:



Hospitals



Urgent
Clinic



Pharmacy

Highest percentage of breaches occurred

OUTCOME FOR VICTIMS:

\$2.5K



in average out-of-pocket costs
per incident

STOLEN DATA USED TO:

37%



Purchase items

35%



Fraudulently
bill for care

26%



Fraudulently
receive care

26%



Fraudulently fill
prescriptions

12%



Access/modify
health records

Source: Accenture Survey, 2017

What is New in 2017

- Ransomware attacks include data extraction
- IRS refund attacks add “W2” phishing scam
- Medical identity theft and medical fraud risk
- Impact of state sponsored hacking

Future Predictions

- IoT will provide basis for attacks on attached devices of all kinds
- Ransomware will continue to be successful in targeting healthcare
- Medical device and wearable hacks will surface soon
- Growth in cybercrime-as-a-service make attacks viable for less sophisticated actors



DATA ▾

MEDIA ▾

WCL

RESOURCES

ABOUT ADVISEN ▾

2017

CYBER RISK INSIGHTS CONFERENCE – CHICAGO

May 16, 2017

12:00 pm – 6:00 pm CT

May 17, 2017

8:00 am – 6:00 pm CT

Swissotel Chicago
323 E. Wacker Drive
Chicago, IL, 60601
USA
(312) 565-0565



Questions?

Adam H. Greene

Partner

Davis Wright Tremaine LLP

202.973.4213

adamgreene@dwt.com

Rick Kam

President and Co-Founder

ID Experts

971-242-4706

rick.kam@idexpertscorp.com

