HIPAA Breach Response: Breach Notification and Crisis Management

The 26th National HIPAA Summit

Washington, DC
March 29-31, 2017

Adam H. Greene, Partner
Davis Wright Tremaine LLP
adamgreene@dwt.com
202.973.4213

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

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

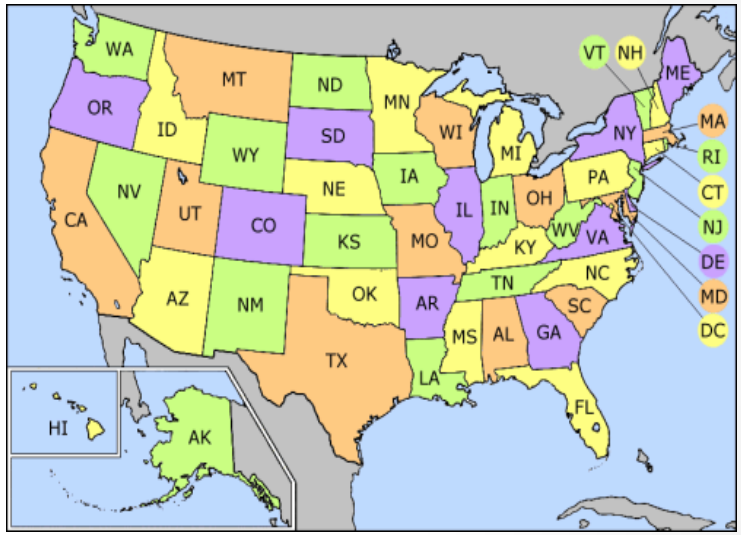
Step 5 (cont'd)

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

Questions?

6 REGIONAL RESPONSE TEAMS
READY TO HELP. ANYTIME. ANYWHERE.

24/7 BREACH RESPONSE TEAM
844-GoToDWT
(844-468-6398)

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER