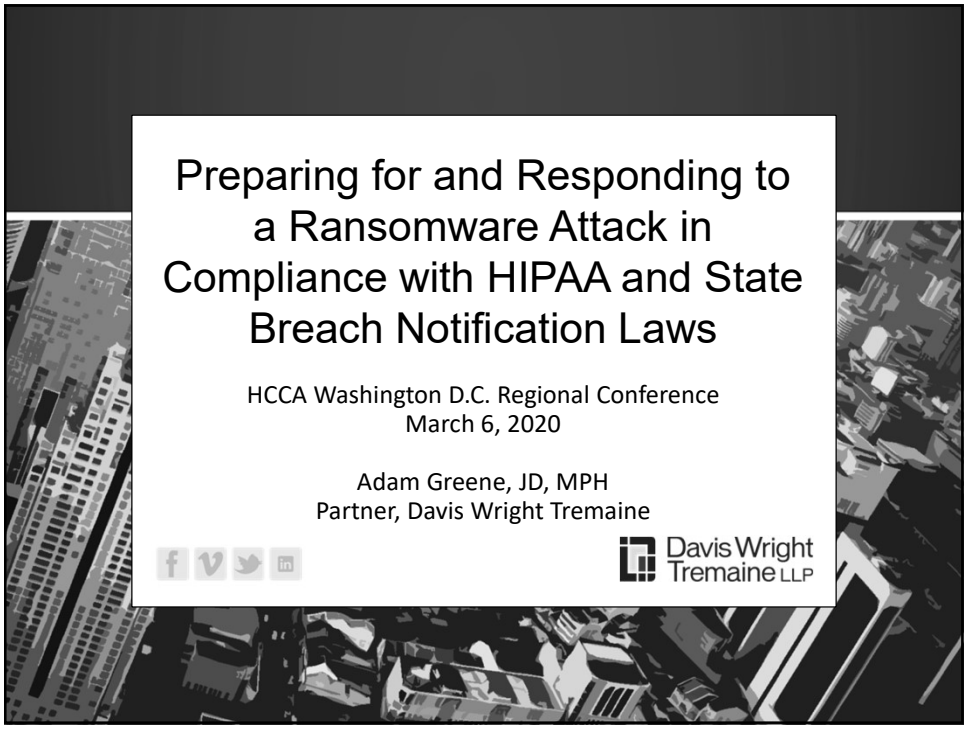

1

Agenda

- Preparing for Ransomware
- Breach Notification Analysis
- Preparing for and Responding to an OCR Investigation

2

Preparing for Ransomware

Start with risk analysis – what is the risk to confidentiality, integrity, or availability due to ransomware

- Evaluate controls:
  - Antivirus software
  - Patching
  - Training
  - Monitoring
  - Disaster recovery

3

Preparing for Ransomware

- Risk analysis (cont'd)
  - Likelihood – Based on current controls, what is the likelihood of loss of confidentiality, integrity or availability for different information systems
  - Impact – What is the impact of ransomware on different information systems if successful
  - Risk – What is the level of risk?

4

Preparing for Ransomware

- Practice defense in depth – assume that some safeguards will fail and that you will need to contain a threat.
- Consider regular vulnerability scanning and penetration testing.
- Test disaster recovery.

5

Preparing for Ransomware

- Have you addressed all systems containing ePHI with respect to the threat of ransomware?
- Do you have documentation that demonstrates implementation of controls that you can produce to OCR? How will you get credit for everything you are doing?
- Do you have documentation of testing of disaster recovery?

6

Recipe for a HIPAA Breach

- Protected Health Information (PHI)
- Unsecured PHI (e.g., not encrypted)
- A use or disclosure of PHI in violation of the Privacy Rule that compromises security or privacy
- None of the three statutory exceptions
- Cannot demonstrate low probability of compromise through a breach risk assessment

7

Key Terms

Use - sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information

Disclosure - the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

8

Privacy Rule Guidance on "Use"

"Comment: One commenter observed that the definition [of use] could encompass the processing of data by computers to execute queries."

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,629 (Dec. 28, 2000)

9

Privacy Rule Guidance on "Use"

"Response: We interpret 'use' to mean only the uses of the product of the computer processing, not the internal computer processing that generates the product."

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,629 (Dec. 28, 2000)

10

Ransomware Guidance

"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 HIPAA Privacy Rule."

Disclosure - the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

11

Ransomware Guidance

"Unless the covered entity or business associate can demonstrate that there is a '…low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred."

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

12

Ransomware Guidance

"If, for example, there is high risk of unavailability of the data, or high risk to the integrity of the data, such additional factors may indicate compromise…."

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

13

Ransomware Guidance

"In those cases, entities must provide notification to individuals without unreasonable delay, particularly given that any delay may impact healthcare service and patient safety."

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

14

Case Study – Ransomware

- A health care provider discovers ransomware on its network. It encrypts electronic systems containing protected health information of 34,000 patients.
- After 25 hours, the health care provider is able to restore its systems from a backup.
- The interim backups were corrupted by the ransomware. Backup was based on a preceding full backup, but three days of information was lost, affecting 712 patients.
- Forensic review of the ransomware indicates that there was no exfiltration of data with high degree of certainty.

15

Case Study – Ransomware

Is this a reportable breach under HIPAA?

- Yes, for 34,000 patients.
- Yes, for 712 patients.
- No.

16

Case Study – Ransomware

Potential Analysis:

- Type of information – Fully identifiable and high sensitivity. [High risk]
- Recipient(s) – Bad actor took control of the information, but did not see the information [Low risk? High risk?]
- Accessed/viewed PHI – Affirmative evidence that it was accessed but not viewed. [Low risk? High risk?]
- Mitigation – No confidentiality breach. Successful restoration of availability for 33,288 patients, partial or no recovery for 712 patients [Low risk? High risk?]
- New factor – High risk of unavailability or loss of integrity for 712 patients
- Conclusion – Reportable breach for 712 patients [?]

17

State Breach Notification Analysis

- What is scope of "personal information"?
  - Does it include health information?
- How is "breach of security" defined?
  - Acquisition?
  - Access?
  - Release?

18

State Breach Notification Analysis

- Can forensics demonstrate no “acquisition”?
- What constitutes “access”? Does the malware’s access qualify?
- Most state breach notification laws arguably will not apply, but check that state law does not apply only to unauthorized “access.”
- Some states have considered changes to laws to incorporate ransomware.

19

What OCR Is Focused On?

- Corrective Action
- Risk Analysis
- Risk Management
- Policies and Procedures
- Training
- Sanctions

20

What OCR Is Focused On?

- What corrective action was taken to contain the ransomware and reduce risk of another infection?
- Did the risk analysis address the risk of ransomware? Was the risk level accurate? If not, was the risk analysis amended?
- To the extent that addressing ransomware was in a risk management plan, was it being followed? Is there evidence of implementation of corrective measures?

21

What OCR Is Focused On?

- Were policies and procedures regarding ransomware controls adequate? Do you have documentation that you reviewed them in response to the incident?
- Was training with respect to ransomware adequate?
  - How to identify a phishing attempt
  - How to spot a potential ransomware infection
  - How to respond to signs of a ransomware infection
- Was any individual who violated policy (e.g., clicked on a link) sanctioned? This could be training, a warning, suspension, etc.

22

Security Incident Report

- Does it address:
  - When incident occurred
  - When incident was discovered
  - Who reported
  - How incident was contained
  - How ransomware was eradicated
  - What corrective action was taken

23

Security Incident Report

- Does it address:
  - Whether notifications (to individuals, HHS, state regulators, media, credit reporting agencies) were made
  - Whether risk analysis sufficiently addressed the risk
  - Whether policies and procedures were reviewed and revised/determined sufficient
  - Whether training was sufficient
  - Whether anyone was sanctioned

24

Security Incident Report

- Is it strictly factual, avoiding conclusions of law (e.g., there was a violation of HIPAA).
- Does it have time entries that demonstrate that a security incident report was quickly started, and was supplemented as additional facts became available?

25

Security Incident Report

- Consider maintaining separate privileged report for purposes of assisting counsel, and then separate, non-privileged report that can be shared with OCR.
- Does report that will go to OCR maintain privilege? For example, if forensics were engaged under direction of counsel, security incident report should reflect organization's factual conclusions, but should not reflect forensics expert's privileged conclusions.

26

Security Incident Report

- Good: On 1/5/18, ABC Co. engaged XYZ forensics under direction of counsel. On 1/27/18, ABC Co. concluded that evidence did not indicate that the ransomware exfiltrated data.
- Bad: On 1/5/18, ABC Co. engaged XYZ forensics. On 1/26/18, XYZ forensics determined that it was more probable than not that the ransomware exfiltrated data, but XYZ forensics could not be certain due to limited audit logs.

27

How to Respond to OCR

- Collaborative rather than adversarial
- Transparent rather than obscuring
- Recognize gaps and explain future corrective action

28

Drafting a Response

- Don't merely respond to specific requests; provide a complete picture
- Highlight a culture of compliance
- Professional and gracious tone
- Include relevant supporting documentation as attachments
- Consider Bates stamping attachments

29

For questions …

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213

30