ABA Webinar

Beware of Ransomware: Is Your Organization Ready?

Winston Krone, Kivu Consulting, Inc.
Heather Deixler, Latham & Watkins LLP
Overview of Today’s Webinar

• What is Ransomware?
• Is it a HIPAA Breach?
• How to Prepare Your Organization
• How to Respond to a Ransomware Attack
• 7 Practical Tips for Preparing for and Dealing with a Ransomware Attack
What is Ransomware?

- Distinct type of *malware*

1. **Locked Out**: Malware attempts to *deny access* to user’s data – usually by *encrypting* the data with key known only to hacker
   - *Hackers may also destroy or exfiltrate data*

2. **Demand for Ransom**: Ransomware directs user to pay ransom to hacker (usually via cryptocurrency such as bitcoin) to receive decryption key
What is Ransomware?

- **Most common vectors of attack**
  - **Phishing email**: Carries a malicious attachment or instructs recipients to click on a URL that downloads malware to their computer
  - **Malvertising**: Visit a web site that contains compromised ads
  - **Network penetration**: Common vulnerabilities exploited by ransomware hackers
Why Should We Care?

- Since early 2016, 4,000 ransomware attacks EACH day
  - 300% increase over the 1,000 daily ransomware attacks reported in 2015

Are healthcare organizations targeted?
- High profile victims
- Many healthcare organizations maintain a variety of personal and financial information (e.g., health information, social security numbers, credit card information)
- Need access to patient records - many healthcare organizations provide critical care and rely on access to up-to-date patient records
Is this a Security Incident under HIPAA?

- Yes, per HHS guidance issued in July of this year (the “HHS Ransomware Guidance”), the presence of ransomware (or any malware) is a security incident under the HIPAA Security Rule.

- Covered entities and their business associates must initiate security incident response activities in response to ransomware to determine what happened and whether this rises to the level of a HIPAA Breach.
  - BAAs typically require business associates to report security incidents to covered entities.
Is this a HIPAA Breach? Definition of Breach

- **Fact-specific** determination

- **Definition of a Breach under HIPAA:** Acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI
**Is this a HIPAA Breach? HHS Ransomware Guidance**

- **Per HHS Ransomware Guidance**, when ransomware attacks and encrypts ePHI – presumed to be a [breach](#) because the ePHI encrypted by ransomware was acquired (i.e., [unauthorized individuals have taken possession or control of the information](#))

  **UNLESS**

- The entity can demonstrate a “[low probability](#)” that the PHI has been compromised
Is this a HIPAA Breach? Determining “Low Probability”

**Risk Assessment considering at least the following 4 factors:**

1. What type of PHI was involved (incl. types of identifiers and likelihood of re-identification)?
2. Who used the PHI? To whom was the disclosure made?
3. Was the PHI actually acquired or viewed? Or did just the opportunity to view the data exist?
4. What steps were taken to mitigate the risk to the PHI?
Is this a HIPAA Breach? Questions to Ask

1. Was the PHI involved sufficiently encrypted or de-identified?
   - HIPAA breach notification provisions apply to “unsecured PHI” – if encrypted ePHI has been rendered unusable, unreadable or indecipherable in accordance with HHS Guidance, not a reportable HIPAA Breach

2. Has ransomware variant been identified? Was data exfiltrated?
   - Identify the exact type and variant of malware
   - Determine capabilities of that variant (can it exfiltrate?)
   - Did attackers access network to install the malware?
   - Was malware isolated? Propagated to other systems?
3. *Has the ePHI been successfully restored from backups?*
   - Implementation of robust contingency plans incl. disaster recovery and data backup plans
   - Ensuring ability to recover data from backups – ensuring integrity of PHI affected by ransomware

4. *Is there a high risk of unavailability or integrity of the data?*
   - Would delay in availability or integrity of data impact healthcare service and patient safety? If data is critical to providing healthcare to individuals, may indicate compromise
Is this a HIPAA Breach? Steps to Take

1. **Fact-specific determination**: Gather facts, isolate systems
2. **Implement Cybersecurity Incident Response Plan**: Internal reporting, work with internal/external counsel
3. **Document Risk Assessment**: Must be “completed in good faith” and reach “conclusions that are reasonable given the circumstances”
   - Consider all mitigation steps
4. **Reporting Obligations**: If ePHI is not encrypted and not possible to reasonably demonstrate “low probability” that ePHI has been compromised, perform **external reporting obligations**
Is this a HIPAA Breach? Steps to Take

• **External Reporting Obligations**
  
  • **Covered entity:**
    
    • **Individuals:** Must notify affected individuals without unreasonable delay and no more than **60** days after discovery
    
    • **Media:** > 500 residents of a State or jurisdiction, provide notice to prominent media outlets (e.g., press release) without unreasonable delay and no more than **60** days after discovery
    
    • **Secretary of HHS:** Must electronically submit breach report form
      
      • **500 or more individuals:** Must notify Secretary without unreasonable delay and no more than **60** days after discovery
      
      • **Less than 500 individuals:** May include in annual notice to the Secretary (due no later than **60** days after end of calendar year when breaches are discovered)
  
  • **Business Associates:** Must notify covered entities
    
    • Without unreasonable delay and no more than **60** days after discovery
    
    • *Look to BAA terms for tighter contractual timelines!*
Prepare, Prepare, Prepare

- **Train your workforce:**
  - Understand the warning signs
  - Appreciate limitations of training (won’t stop new ransomware attacks)
- **Technical safeguards:**
  - Block phishing emails
  - Prevent malware from executing/spreading
- **Data Backup:** Secure off-line backups
- **Cybersecurity Incident Response Plan**
  - Internal and external reporting systems
  - Plan in place to deal with cybersecurity incidents
- **Cybersecurity Insurance**
You’ve Been Attacked… Now What?

- Confirm no available backups
- Responding to the attacker
- What to expect if you pay a ransom
- Preserving evidence and preparing the forensic analysis of PHI compromise
Top 7 Practical Tips for Ransomware Attacks

1. Enterprise-wide Risk Analysis – know where your data is and understand your risks and vulnerabilities
2. Implement Technical Safeguards
3. Perform regular monitoring – be vigilant!
4. Train your workforce
5. Update your Cybersecurity Incident Response Plan
6. Encrypt your data!
7. Rethink your backup strategy
Questions?

Heather Deixler, Esq.
Latham & Watkins LLP
Heather.Deixler@lw.com
T: +1.415.395.8110

Winston Krone
Kivu Consulting, Inc.
wkrone@kivuconsulting.com
T: +1.415.524.7322