701: Ransomware - Don’t Be a Hostage

Frank Ruelas
Facility Compliance Professional
St. Joseph’s Hospital and Medical Center
Dignity Health
Objectives

• Understand the specifics of ransomware and how it may affect the practice’s ePHI
Objectives

• Understand the specifics of ransomware and how it may affect the practice’s ePHI
• Learn how to apply the HHS guidance on ransomware to determine if you have experienced a presumed breach using the LoProCo Model

• Compare and contrast the different strategies that are used to minimize the risks of a successful ransomware attack.
Objectives

• Understand the specifics of ransomware and how it may affect the practice’s ePHI
• Learn how to apply the HHS guidance on ransomware to determine if you have experienced a presumed breach using the LoProCo Model
• Compare and contrast the different strategies that are used to minimize the risks of a successful ransomware attack.

How is our ePHI affected?

First...let’s look at what makes up security.
Let’s start with a description. (NIST)

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.
Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.

How is our ePHI affected?

First...let’s look at what makes up security.
Now let’s look at malware...

Common Categories and Types of Malware

- Viruses
- Worms
- Spyware
- Rootkits
- Keyloggers
- Grayware
- Trojan Horses
- Ransomware
Common Categories and Types of Malware

- Viruses
- Worms
- Spyware
- Rootkits
- Keyloggers
- Grayware
- Trojan Horses
- Ransomware

Our focus today...
FACT SHEET: Ransomware and HIPAA

A recent U.S. Government Technology report indicated that, on average, there have been 4,600 daily ransomware attacks since each 2016 is 99% increase over the 2,000 daily ransomware attacks reported in 2016.1 Ransomware exploits human and technical weaknesses to gain access to an organization's critical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA-covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification procedures should be managed in response to a ransomware attack.

1. What is ransomware?
Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only by the hacker who deployed the malware, until a ransom is paid. After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker usually in a cryptocurrency, such as Bitcoin, in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or erases2 data, or ransomware in conjunction with other malware that does so.

2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?
Yes, The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of those required security measures include:

- Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- Implementing procedures to guard against and detect malicious software;

2HIPAA imposes a total of 16 security rules, and the four most relevant to HIPAA covered entities are: (1) Access Controls, (2) Audit Controls, (3) Security Management Process, and (4) smoothly processes.


3. How do I pay?
Payment is accepted in Bitcoin only. For more information, click «About bitcoin».
Please check the current price of Bitcoin and buy some bitcoins. For more information, click «How to buy bitcoins».
And send the correct amount to the address specified in this window.

After your payment, click «Check Payment». Best time to check: 9:00am - 11:00am
FACT SHEET: Ransomware and HIPAA

A recent U.S. Government Intelligence report indicates that, on average, there have been 4,600 daily ransomware attacks since early 2016 at 200% increase over the 1,000 daily ransomware attacks reported in 2015. Ransomware exploits human and technical weaknesses to infect an organization’s technical infrastructure in order to deny the organization access to its systems and data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a Healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?
Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who disabled the malware, until a ransom is paid. After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may destroy ransomware that also destroys or extorts” data, or ransomware in conjunction with other malware that does so.

2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?
Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:
• Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate these identified risks.
• Implementing procedures to guard against and detect malicious software.


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. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

This applies to each of the four “impermissibles”...
What are the four impermissibles?

- Access
- Acquisition
- Use
- Disclosure

So essentially we have a presumed breach.
What is the question that most people want to ask?

Is it a HIPAA breach if ransomware infects a covered entity’s or business associate’s computer system?
Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

Let’s do a LoProCo for a ransomware attack...
Four Factors

Four Factors
Four Factors

Four Factors
Four Factors

Four Factors
To pay or not to pay?

That IS a very good question.
Interesting Observations

- Customer service focus
- Knowledgeable

One IT supervisor mentioned good “Help Desk Etiquette”
Strategies Considerations

Safeguards

Strategies Considerations

- Administrative
- Physical
- Technical
Actual Practices

• Link detection and processing
Actual Practices

- Link detection and processing
- Attachment quarantine

Actual Practices

- Link detection and processing
- Attachment quarantine
- Drills: Practice vs “Gotcha”
Actual Practices

• Link detection and processing
• Attachment quarantine
• Drills: Practice vs “Gotcha”
• Patch Management

Actual Practices

• Link detection and processing
• Attachment quarantine
• Drills: Practice vs “Gotcha”
• Patch Management
• Security Reminders
Actual Practices

• Link detection and processing
• Attachment quarantine
• Drills: Practice vs “Gotcha”
• Patch Management
• Security Reminders
• Access privileges