Clinical Practice Compliance Conference

October 15-17, 2017
Phoenix, AZ

701: Ransomware - Don’t Be a Hostage
Frank Ruelas
Facility Compliance Professional
St. Joseph’s Hospital and Medical Center
Dignity Health

Objectives
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.

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

Our focus today...
Ransomware Can be Stopped - Try the Free Security Scan Now
www.ransomware.com/ransomware
(605) 267-7465
Our multi-layer protection safeguards your network and data from cyberattacks.
Ransomware Protection - State of the Art backup solutions.
Free Email Test
Baracuda SSL VPN Web Generation Firewall
Ransomware Protection Guide - Steps to Follow After Attack - cirtuva.com
Access now Key Steps to Follow After Being Infected With a Ransomware
Address Detection - Critical Recovery - Full Responsibility
Recovery Process - Follow-up - Monitor
16
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
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
Actual Practices

- Link detection and processing
- Attachment quarantine

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
• Security Reminders

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

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

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