

Healthcare Data and Privacy/Protection

October 18, 2016

Patricia Stahura, RN, MSN



© 2016 ECRI Institute



Objectives

- Understand the background and history of the Health Insurance Portability and Accountability Act (HIPAA)
- Identify components of the digital landscape
- Discuss challenges to privacy and security in healthcare
- Review ways to address privacy and security gaps
- Design a privacy and security plan of action



Privacy and Security Action Plan

| Identified Issue | Proposed Action | Responsible Person(s) | Action Due Date | Progress/ Evaluation Date | Comments |
|------------------|-----------------|-----------------------|-----------------|------------------------------|----------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |



HIPAA

- **Health Insurance Portability and Accountability Act**
 - 1996 Privacy Rule
 - 2003 Security Rule
 - Enforcement Rule
 - Breach Notification Rule



2013 Omnibus Rule

- **Review and revise**
 - Security policies and procedures
 - Business associate agreements
 - Breach notification requirements
 - Penalties



2013 HIPAA “The Audits”

- Security/risk analysis
- User access, supervision, administrative rights
- Monitoring user activity
- Privacy/security officer
- Policies current
- User termination procedure
- Training
- Volume and visibility
- Contingency plan
- Business associate agreement
- Antivirus software
- Encryption
- Mobile/portable device use
- Wireless networks
- Complaint handling
- Request to amend the record
- Releasing information
- Response to an incident
- Current Notice of Privacy Practices (NPP)
- State laws



Fact or Fiction?

A safe practice is to label the outside cover of paper records with warnings and important information such as “AIDS.”



Breach

- **Act of breaking or failing to observe a law, agreement, or code of conduct**
- **Impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information (PHI)**
- **PHI breach involves three notifications:**
 - Affected individuals
 - Media in some cases
 - Secretary of Health and Human Services



Security

- The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction
- Security is a general term that can be used regardless of the form the data may take (e.g., electronic, physical)



Cybersecurity

- **Cybersecurity: insufficient protections for medical devices and systems**
- **ECRI Institute Hazard #9—Top 10 Health Technology Hazards for 2016**



[ECRI Institute. 2016 Top 10 Health Technology Hazards.](#)

Digital Landscape

- Electronic health record (EHR)
- Laboratory, pharmacy, radiology systems
- Networks and other sites
- Billing, Uniform Data System (UDS), coding
- Desktop computers
- Mobile devices
- USB (Universal Serial Bus)
- Medical applications
- Internet of Things (IoT)
- Texting
- E-mail
- Wi-Fi
- Social media
- “The cloud”
- Encryption
- Malware



Fact or Fiction?

As long as a patient consents, it's OK to take his or her picture and post it on Facebook.



Social Media

- The internet is forever
- There is no delete button
- Social networks
- Facebook, LinkedIn



Internet and E-mailing

- Reasonable, conservative guidelines for cell phone and e-mail use within the office
- “Reply all”
- Who is receiving, reading, and forwarding
- Forwarding unencrypted content that contains PHI
- Replaces face-to-face or telephone interaction
- Forward to personal account



Fact or Fiction?

I have to leave the office at 3:00 p.m. Those labs I have been waiting on aren't back yet. It is fine to have the medical assistant e-mail them to my personal e-mail at home.



Mobile Devices: mHealth

- **Handheld computers**
- **Smartphones**
- **Tablets**
- **Laptops**
- **Flash drives/USB**



To BYOD or Not BYOD?

- **Bring your own device to work (BYOD)**
 - Create a policy based on your risk appetite
 - Educate staff on how to secure personal devices
 - Passwords, encryption, remote wipe, automated data disintegration
 - Continuously monitor use and provide oversight

Fact or Fiction?

Our system is very sophisticated, so it is totally safe.



Mobile Security

- Think before connecting to a Wi-Fi hot spot
- Guard your mobile device
- Keep it locked: autolock, password
- Update your mobile software
- Only connect to internet if needed
- Think before you download apps
- Be cautious with apps



[“Stop. Think. Connect.” Campaign. U.S. Department of Homeland Security.](#)

Texting

- Encryption is a priority
- Texting policy re: when it is acceptable to text and when a call is indicated
- Assume text can be viewed by anyone in proximity
- Secure text messaging (STM) developed for healthcare: meets HIPAA security standards, integrates with EHR
- Texting medical orders





Mobile Devices: Know the **RISKS**. Take the **STEPS**.
PROTECT & SECURE Health Information.

Find out more at HealthIT.gov/mobiledevices



Wi-Fi

- Think before you connect
- Wi-Fi hot spots in coffee shops, libraries, airports, hotels, and public places are convenient but often not secure
- Send information only to sites that are fully encrypted
- Encrypted website: look for “https” in the web address (the “s” is for secure)
- Some websites use encryption on the sign-in page only

Virtual Private Network (VPN)

- VPN encrypts data between your computer and the internet, even on unsecured networks
- VPN provides security even on a public unsecured network
- VPN encryption is available for mobile devices



Encryption

- **Renders unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals**
- **Encryption converts data into an unreadable format**



The Cloud

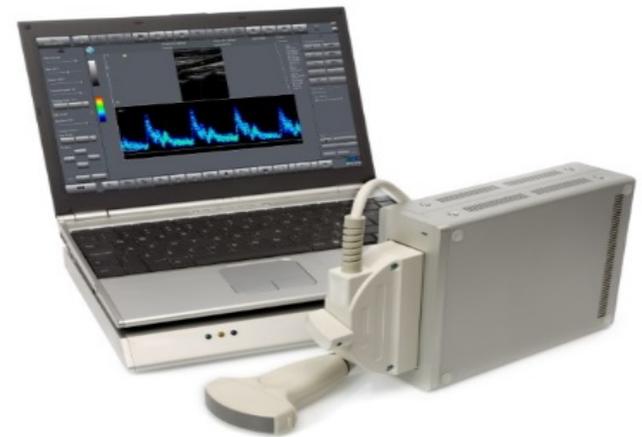
- **Cloud storage is a network of remote servers with online access**
- **Check out vendor reputation and security policies**
- **Ensure data are encrypted when uploaded and downloaded and stored in the cloud**
- **Business associate agreement**

“There’s an App for That”

- Medical applications for patients and staff
- Downloads or by prescription
- Alert physician before problem becomes a bigger issue
- Patient education to better inform and engage
- Self-monitor activity, track weight loss, improve medication adherence, blood pressure, or blood sugar
- Staff downloading apps

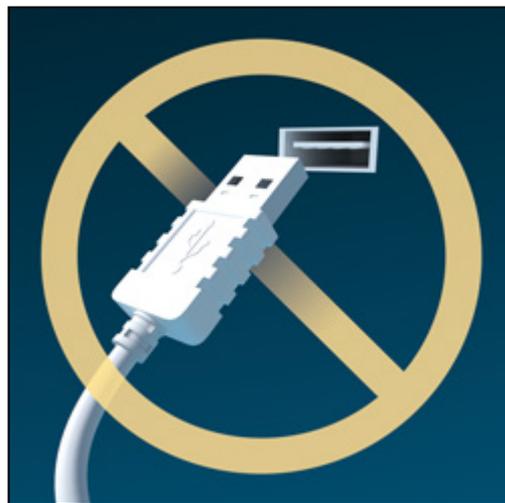
Medical Devices

- Food and Drug Administration oversight of digital platforms that either directly control wireless medical devices or store and forward data from these devices
- Inventory your devices—they need protection



Fact or Fiction?

When you run out of USB ports, it is acceptable to connect to the port on the electrocardiograph machine.



Internet of Things (IoT)

- **Wearable, connected devices**
- **Smart watches**
- **Fitness trackers**
- **Lighting**
- **Climate control**
- **Barcode scanners**
- **Security systems and cameras**
- **Remote patient monitoring—wireless heart monitors or insulin pumps**

Fact or Fiction?

It is likely your personal information has been breached.



Cybercrime

- Theft of unencrypted devices and electronic records
- Sources difficult to trace
- Attacks generated remotely
- Even after your device has been decrypted, ransomware may remain
- Back-up may be infected
- Cost of entry low, with high reward
- Easy access to “kits”—about \$1,000



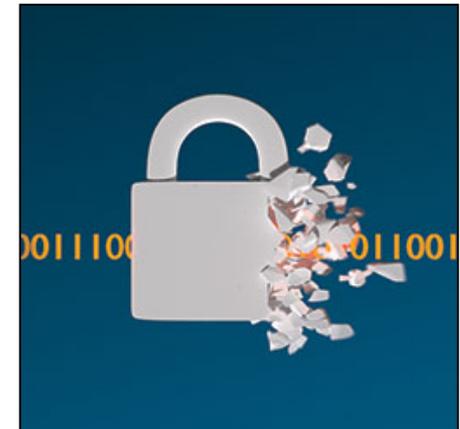
Fact or Fiction?

Cybercriminals are only interested in PHI, such as Social Security numbers and birth dates.



“Cybercrime: Why Healthcare?”

- Failure to upgrade cybersecurity
- Fast adoption of technology
- Struggling to stay ahead of the curve
- Mobile devices
- Rapid growth
- Connected devices
- Unpatched vulnerabilities
- Particularly valuable personal information



Malware

- Viruses
- Worms
- Spyware
- Adware
- Trojan horses
- Key loggers
- Scareware
- Ransomware



Ransomware

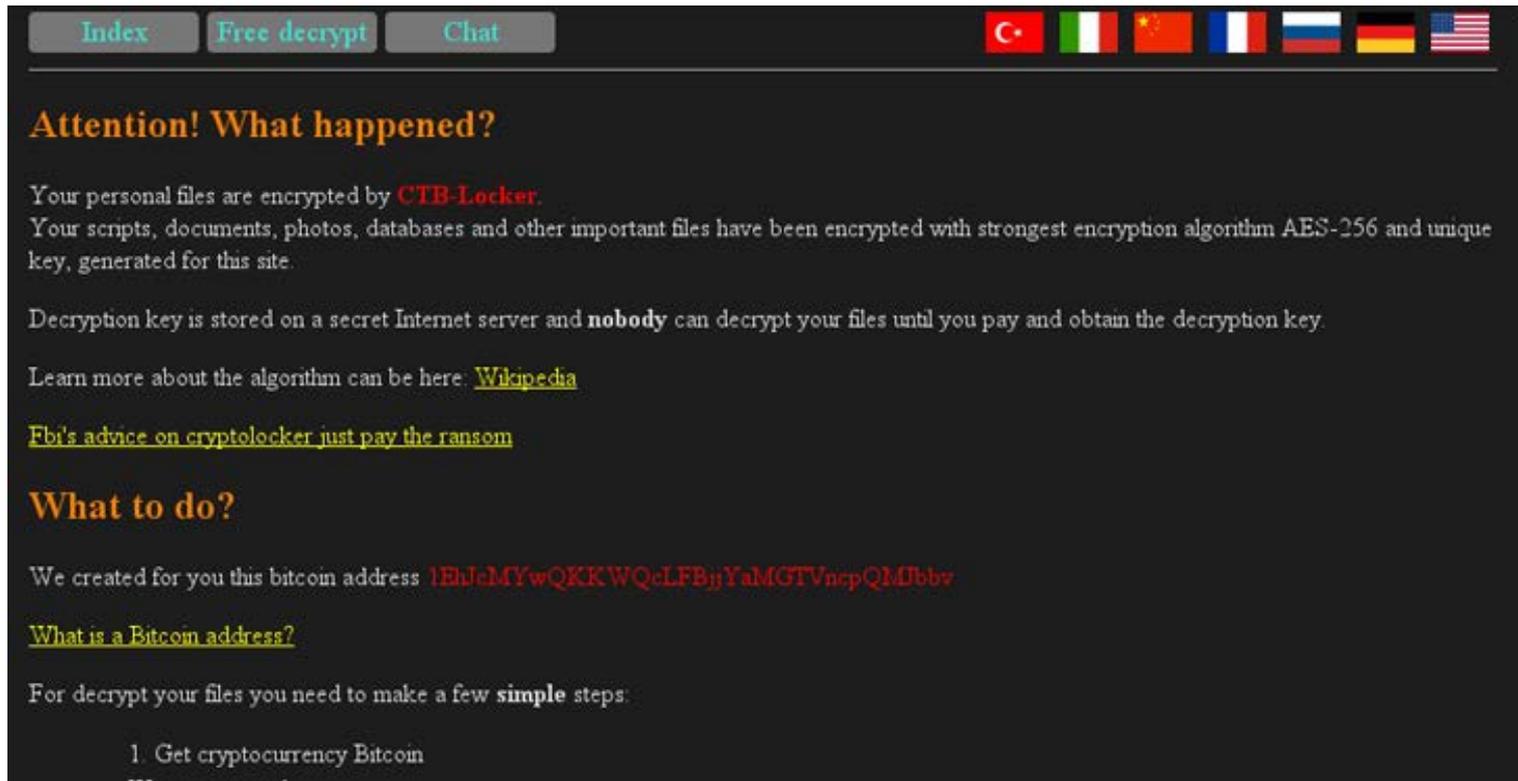
- Virus software does not protect against
- Attacks involve a virus infecting files
- Locks users out of information technology (IT) system until they pay a ransom
- Obtain a decryption key to release the files
- Sophisticated software encrypts the hard drive and/or server
- Bitcoins, nonstandard currency
- Best defense is awareness
- According to HHS, ransomware attacks are a HIPAA security incident



Signs and Signals of Malware

- Subtle signs of infection
- Message conveys fear and urgency
- Screen messages: “Your files are encrypted and you need to pay us this amount in this amount of time”
- Implies they are associated with the Federal Bureau of Investigation (FBI) cybercrimes unit—looks official

From *The Hacker News*



The screenshot shows a dark-themed ransomware message. At the top, there are three buttons: "Index", "Free decrypt", and "Chat". To the right of these buttons is a row of national flags including Turkey, Italy, China, France, Russia, Germany, and the United States. The main text of the message is as follows:

Attention! What happened?

Your personal files are encrypted by **CTB-Locker**.
Your scripts, documents, photos, databases and other important files have been encrypted with strongest encryption algorithm AES-256 and unique key, generated for this site.

Decryption key is stored on a secret Internet server and **nobody** can decrypt your files until you pay and obtain the decryption key.

Learn more about the algorithm can be here: [Wikipedia](#)

[Fbi's advice on cryptolocker just pay the ransom](#)

What to do?

We created for you this bitcoin address **1EhJcMYwQKKWQcLFBjjYaMGTVncpQMJbbv**

[What is a Bitcoin address?](#)

For decrypt your files you need to make a few **simple** steps:

1. Get cryptocurrency Bitcoin



How Could This Happen?

- Inadvertent opening of an e-mail attachment
- Online scam artist
- Social engineering attacks
- Hackers
- Malicious insider
- Workforce snooping
- Health information exchange (HIE)
- Fake updates of real software
- Word docs with macros
- Spoofed e-mails
- “Spear phishing”
- Aging computer systems
- Human error



What's Next?

Actions that health centers can take to improve security and privacy.



Detection

- Conduct risk assessment annually or more often
- Identify threats and vulnerabilities to security and privacy
- Audit staff behaviors and unsafe practices
- Audit the effectiveness of policies and procedures
- Monitor, log, analyze, and report system intrusions
- Conduct a risk analysis
- Identify human, natural, or environmental gaps
- Partner with cyber expert—IT vendor support
- Monitor and enforce policies



Prevention: Safeguards

- Firewalls and antivirus software
- Secure wireless
- Encryption
- Use STM on smartphones
- VPN
- Back up data
- Strong passwords and biometrics
- Remote wipe or disable
- Updates and patches



Prevention: Safe Practices

- Limit access to least level of privileges needed
- Physically lock up devices
- Download only trusted apps
- Create a list of approved apps or restrict downloading
- Limit use of flash drives or use encryption
- Report suspicious e-mails and links
- Implement security measures
- Delete information before disposal



Safe Practices

Online Resource Center:
Tips to Protect and Secure Health Information

HealthIT.gov

| | | | |
|---|--|---|--|
|  | Use a password or other user authentication. |  | Keep security software up to date. |
|  | Install and enable encryption. |  | Research mobile applications (apps) before downloading. |
|  | Install and activate wiping and/or remote disabling. |  | Maintain physical control of your mobile device. |
|  | Disable and do not install file-sharing applications. |  | Use adequate security to send or receive health information over public Wi-Fi networks. |
|  | Install and enable a firewall. |  | Delete all stored health information before discarding or reusing the mobile device. |
|  | Install and enable security software. | | |

How can you protect and secure health information when using a mobile device? [Office of the National Coordinator for Health Information Technology.](#)



Training and Awareness

- Privacy and security behaviors
- Identify who is the security officer
- How to recognize suspicious e-mails
- Do not open attachments in unsolicited e-mails or click on links—what steps to take
- Use of internet and cell phones at work
- Safeguards and safe practices
- Policies and procedures



Response

- **Security plan: how will you respond to breach?**
- **Contingency or back-up plan—test it**
- **Breach: discovery, containment, reporting**
- **Breach event assessment following the breach**
- **Recovery: repair reputation, lessons learned**
- **Cyber insurance**
- **Legal counsel**
- **Vendor services: forensics, credit monitors, call centers, mailing**



Data Privacy and Security Aim

- **Protect PHI while keeping data available for patient care and services**
- **Balance between control and access**
- **Comply with regulations**
- **Keep from being the next headline**
- **Detect, prevent, train, and respond**



Privacy and Security Action Plan

| Identified Issue | Proposed Action | Responsible Person(s) | Action Due Date | Progress/ Evaluation Date | Comments |
|------------------|-----------------|-----------------------|-----------------|------------------------------|----------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Thank You

Additional Questions?

clinical_RM_program@ecri.org

610-825-6000, ext. 5200



© 2016 ECRI Institute

