How to Keep Your PHI Secure, With Ransomware on the Rise

Presented by Susan Clarke
Health Care Information Security and Privacy Practitioner

Thursday, March 26, 2020 | 11 AM – 12 PM
Zoom tips and tricks!

**VIDEO:** We want to see you! If your camera isn’t on, start your video by clicking here.

**AUDIO:** You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click “Join Audio,” this “Choose one...” box will pop up. If you dial in, just make sure you include your audio code.

**MUTE/UNMUTE:** *6 or click the mic on the bottom left of your screen.

**CHAT:** Please jump in if you have something to share, but we also have this nifty chat function.

**ATTENDANCE:** If there are multiple attendees together on the call, please list the names and your location in the chat box.
Upcoming HCCN Sessions

HIPAA Series: HHS Information Blocking Rules: Balancing Data Access with Privacy and Security
Thursday, April 16
11:00 a.m.

HIPAA Series: Breach Mitigation and Response Plans
Thursday, June 25
11:00 a.m.

Health Center Framework for Electronic Patient Engagement
Tuesday, April 7
12:00 p.m.

EHR Data Hygiene Tools: Methods for Finding and Fixing Issues that Could be Hindering Quality
Wednesday, April 22
10:00 a.m.
Susan Clarke, HCISPP

Certified Healthcare Information Security (ISC)² and Privacy Practitioner and Computer Scientist

20 years’ health care experience

10 years’ design and coding EHR software including HL7 Healthcare application development

Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic-affiliated health care system

Served as communications unit lead during health care system’s ready and complete alerts
The presenter is not an attorney and the information provided is the presenter(s)’ opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users patient needs.
Acronyms

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis
Learning Objectives

1. Proactive approaches to data security
2. Effects of ransomware on your organization, IT security and compliance
3. Proven steps to mitigate, including good backup and disaster recovery practices
4. Training is the key – exploring phishing emails and other types of social engineering techniques
5. Cyber attacks are increasing – be prepared
Relaxing of HIPAA during COVID-19

- Requirement to obtain patient’s agreement to speak with family members/friends involved in patient’s care
- Requirement to honor request to opt out of facility directory
- Requirement to distribute notice of privacy practices
- Patient’s right to request privacy restrictions
- Patient’s right to request confidential communications

Above waiver only applies if:
(1) in the emergency area identified in public health emergency declaration; (2) to hospitals that have instituted disaster protocol; and (3) for up to 72 hours from time hospital implements disaster protocol.

Relaxing of HIPAA to Promote Telehealth Visits during COVID-19

HHS Office of Civil Rights (OCR) will exercise enforcement discretion and waive penalties for HIPAA violations against health care providers who serve patients in good faith through everyday communications technologies (e.g., FaceTime, Skype).

HIPAA Standing Down for Telehealth

- Some technologies and how they are used may not fully comply with HIPAA Rules
- OCR will exercise enforcement discretion and not impose penalties for noncompliance (good faith provision)
- OCR will not impose penalties against covered health care providers for lack of BAA with vendors

“Never allow a good crisis to go to waste when it's an opportunity to do things that you had never considered, or that you didn't think were possible.” – Rahm Emanuel
The Wild, Wild West

Bank Robbers vs. Cyber Criminals

Instead of robbing a bank, why not get the bank to send you their funds without them even being aware?

Instead of stealing company data, why not put the data in a vault you have the only key to, then demand a ransom?
Health Care Data Trends

EHRs + Sharing patient records across ecosystem + Interoperability + Analytics used to enhance care + Electronic registries for population health + Personalized medicine

= DATA EXPLOSION
Health care organizations are a prime target for cyber criminals.

- Hold valuable data (e.g., PII, PHI, financial)
- Focus on patient care and safety; security can take backseat to operations
- Balance costs with risks
- Ensure functionality of networks
- Safeguard data
- Maintain operational viability
Patient Data Breaches

33% Increase in Breaches
2018: 371
2019: 494

195% Increase in Number of Breached Records
2018: 13,947,909
2019: 41,134,121

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Medical sector saw a 98% increase in threat detections.

“Net new ransomware activity against organizations remains higher than we’ve ever seen before, with families such as Ryuk, Phobos and Sodinokibi making waves against cities, schools and hospitals...

...In 2019, we detected an average of 11 threats per Mac endpoint—nearly double the average of 5.8 threats per endpoint on Windows.”
What Is Malware?

Malicious Software

Collective name for many variants, e.g., viruses, ransomware, spyware

Designed to cause extensive damage to data and systems

Delivered via link or file over email; requires user click

Threat since 1970s \( \rightarrow \) hundreds of thousands attacks
What Is Ransomware?

Ransomware

- Form of malware
- Denies access until ransom paid
- Takes different forms
October 2: FBI Issued Ransomware Attack Threat
Public Service Announcement (I-100219-PSA)

Encrypts computer or server files, making them unusable

User pays ransom to get key to decrypt files

Becoming more targeted, sophisticated, costly

Most often infected via email link/attachment

Techniques changing to prevent detection
Ransomware Infects Via…

- Phishing emails
- Unpatched programs
- Compromised websites
- Poisoned online
- Advertising
- Free software downloads (not REALLY free)

Also known as attack vectors
Ransomware Characteristics

- Travels across network to encrypt files
- One infected user can affect organization
- Hacker explains how to unlock files
- Missing deadline causes ransom to increase
- Must pay with e-currency (cryptocurrency), e.g., Bitcoin (BTC)
Email Most Common

1. User receives email
2. User opens attachment without verification
3. Ransomware infection
Dear Colleagues,

It’s truly a time of optimism at Mountain-Pacific Quality Health as we reflect on the great things we’ve accomplished thus far in the past years and look forward to the opportunities that lie ahead. Every day, I am motivated by our staffs who are making discoveries in ways that are collaborative, innovative, and impactful.

We are ready to accept online registration for the 2019 Employee Strategic plan for the year! It will only take 30-45 seconds. Attached is the link that contains important information you need to complete the registration:

Mountain-Pacific Quality Health Annual Strategic Plan Update

Thank you for your continuous efforts to support the success of our great Institution!

Sincerely,

Sara Medley
Chief Executive Officer
Mountain-Pacific Quality Health
3404 Cooney Drive
Helena, MT 59602
Signs of Malicious Email

- To/from/received/reply unconnected
- URLs branding slightly off
-Disconnected/bogus URLs
- Unexpected file attachments
- Internet mail extension type mismatches
- Unexpected requests for actions
- Stressor claims, sense of urgency
Business Email Compromise Attacks

Sophisticated scam targeting those who make wire transfers

Start with phishing email or social engineering to gain access to CEOs email account

Majority of fraudulent wire transfers are destined for banks in China

Vary in sophistication from simple to highly skilled
Successful attack! Money went to Utah bank, then to bank in China. …and to Procurement to pay vendor through wire transfer.

Attacker sends emails to Finance to set up wire transfer…

Successful attack! Money went to Utah bank, then to bank in China.

CEO gets phishing email and opens attachment. Attackers watch and learn internal process.

“Social Engineering”

Empower and train employees to protect your network!
Ways to Get Infected: Internet Surfing

Visiting a compromised website via...
- Old browser
- Software plug-in
- Third-party application

Using a computer with...
- Unpatched vulnerabilities

For example...
- Unpatched version of Adobe Flash or Java
- Old web browser
- Unpatched/obtated operating system (e.g., Windows 7)
Ways to Get Infected: Free Software

- Hacker offers free software
- User downloads file
- Hacker can bypass firewall/email filter

Example: Minecraft Mod
- Hacker exploited game’s popularity
- When players installed the “mod” sleeper version of ransomware also installed
- Attacked users’ machines weeks later
Ways to Get Infected: Remote Desktop

- Used to remotely log in to Windows computers to control computer as if user is sitting in front of it
- Port 3389 used to communicate
- Many organizations allow traffic from Internet through firewall for access
How to Determine You Are Infected

- Unable to open files; errors (e.g., wrong extension)
- Message sent: Files have been encrypted
- Countdown warning for time to decrypt
- Window opens to ransomware program
- All file names changed (e.g., HOW TO DECRIPT FILES.TXT, DECRYPT_INSTRUCTIONS.HTML)
Most of your files are encrypted with strong AES-128 ciphers.
To decrypt files you need to obtain the private keys, and it is the only possible way.
To obtain the keys you should pay with bitcoin.
The cost will double by the specified time.

What to do, How to do

1. Send 0.1 BTC to 1G7bggAjH8pJaUfUoC9kRAcSoev6djwFZ
   You will be able to download the private key within 12 hours.

2. How to DECRYPT your files
   1) Click "Start Decrypt".
   2) First, you should send a download request with your Bitcoin wallet address.
      (Important: You must know your actual wallet address from where your payment be sent.)
   3) Sleep.
   4) After 5–6 hours you will have the key and can decrypt your files. Go!
   5) That’s all.

3. About BITCOIN
   1) For more information about bitcoin, please visit https://en.wikipedia.org/wiki/Bitcoin
   2) Here are our recommendations to purchase bitcoin:
STEPS TO TAKE WHEN INFECTED

Now what?
Step 1: Disconnect

Disconnect infected computer from network(s)

- Shut down wireless
- Unplug storage devices

Do NOT erase or “clean up” anything
Step 2: Find Patient Zero

1. Look for ransomware ownership or ransom note
2. From which user account is ransomware being deployed?
3. Revoke user account’s access to shares
4. OR
   Physically isolate computer(s) from network
Open file properties of any encrypted file.
Step 3: Assess the Damage

Did first infected machine have access to any of the following:

- Shared or unshared drives or folders
- Network storage
- External hard drives
- USB memory with files
- Cloud-based storage
Step 3: Assess the Damage

If it is new, the situation is more complex.
Discovery

Main Methods

Visual Inspection  Forensic Analysis
Research  Tools

• Can be time-consuming!
• May require isolated system (LAB)
Today’s Ransomware

Can spread without being shared

Connects to drives/network folders

“Installs” itself
Step 4: Evaluate Your Options

Four options, from best to worst:

1. Restore from recent backup
2. Decrypt your files using third party decryptor
3. Do nothing (lose your data)
4. Negotiate/pay ransom
Backups

Good
Working
Cold-store
Tested
Version
Control

Make sure you have functional backups!
Restoring from Backup

THEN
Costly, required regular checkups and maintenance

NOW
Cloud storage and backup software = absolute necessity
Decrypt Yourself

Make sure decryptor/unlocker is reliably vetted

Review reputable antivirus or malware support forums

Consult security professionals
Do Nothing

Choosing to not recover encrypted files

- Take a hit
- May want to back up encrypted files
- Often not viable in health care
- Restore computer
Pay the Ransom

Controversial opinion!

• Most IT security experts/law enforcement recommend avoid paying
• Nothing encourages MORE ransomware attacks than successfully paid ransom

However…
Sometimes there will be no choice
Prevention Steps

1. Install/maintain high-quality antivirus software
2. Configure professional backup/restore software and test
3. Implement effective security awareness training
Technical Controls

- Avoid mapping drives; hide network shares
- Work from principle of least permission
- Be vigilant blocking dangerous file extensions (.exe, .vbs, .wsf, .cpl, .cmd, .scr, .js)
- Install old CryptoLocker software restriction policies
- Run whitelist approach (vs. blacklist)
Ransomware infections typically start in certain directories. Using Microsoft’s Software Restriction Policies can cut down on susceptibility.

In addition to antivirus, use specialized software that scans for these infections.

Microsoft’s “Controlled Folder Access” prevents files in specified folders from being modified by unauthorized applications.
Patch Management

Important, but not enough

- Patch development
- Vulnerability not publicly disclosed
- User allows malware
- Unauthorized devices
- Insider threat
Defense in Depth

To protect from attacks, secure main layers of defense.

Computer network = series of layers

Malware/virus must infiltrate these layers.
Defense in Depth Includes...

- Antivirus
- Firewalls
- Email filters
- Web content filtering
- Network segmentation
- Network and host-based intrusion detection/protection systems
- Logging
- Access control
- Regular backups
- Continuity of operations plan
- Incident response plan
In addition to technical controls…

Keep employees up-to-date on the basics of IT, email security and the ever-changing attack types and threat vectors.
IT Security and CIA Triad

Confidentiality

What if my health record isn’t kept private?

Information Assets

Integrity

What if my health record isn’t accurate?

Availability

What if my health record isn’t there when needed?
Healthcare’s Changing Risk Priorities

Confidentiality
- PHI (HIPAA)
- But also PII & PCI
- Account Information
- Billing & Payment Data
- Intellectual Property
  - Clinical Trials
  - Research
  - Designs & Formularies
- Legal & HR Documents
- Identities & Credentials

Availability
- Clinical Systems
  - EHR & Specialty
  - Ancillary (PACS, Lab, Pharma)
  - ePrescription / EPCS
- Medical Devices
  - Availability of clinical services and diagnostic results
- Business Systems
  - Email
  - Billing, Scheduling

Integrity
- Critical Patient Data
  - Prescriptions, Medications, Dosages
  - Allergies and History
  - Diagnosis and Therapy Data
  - Alarms
- Critical Technical Data
  - Calibration
  - Safety Limits
  - Functionality & reliability
  - Risk of patient harm

Patient Experience: “Trust Zone”
Harm Risk: “Patient Safety Zone”

Source=HIMSS Cybersecurity Forum
Justice Can Be Difficult

Finding, punishing or prosecuting hackers, or getting back money, can be done, but it is very hard:

- **Jurisdiction**: Hackers are often in a different country; law enforcement can’t get involved
- **Elusive Damage**: No real damage or hard to prove
- **Elusive Evidence**: Evidence is hard to get and is expensive
US natural gas operator shuts down for 2 days after being infected by ransomware

Infection spread to site's OT network that monitors and controls physical processes.

DAN GOODIN - 2/18/2020, 8:00 PM

Please let me know how I can help.

For assistance please contact:
Susan Clarke
sclarke@mpqhf.org | (307) 248-8179

THANKS FOR YOUR VALUABLE TIME TODAY!
https://www.knowbe4.com/
Questions