CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

Cyberattacks in Healthcare

Melissa Thompson, RN, BSN, CMSRN

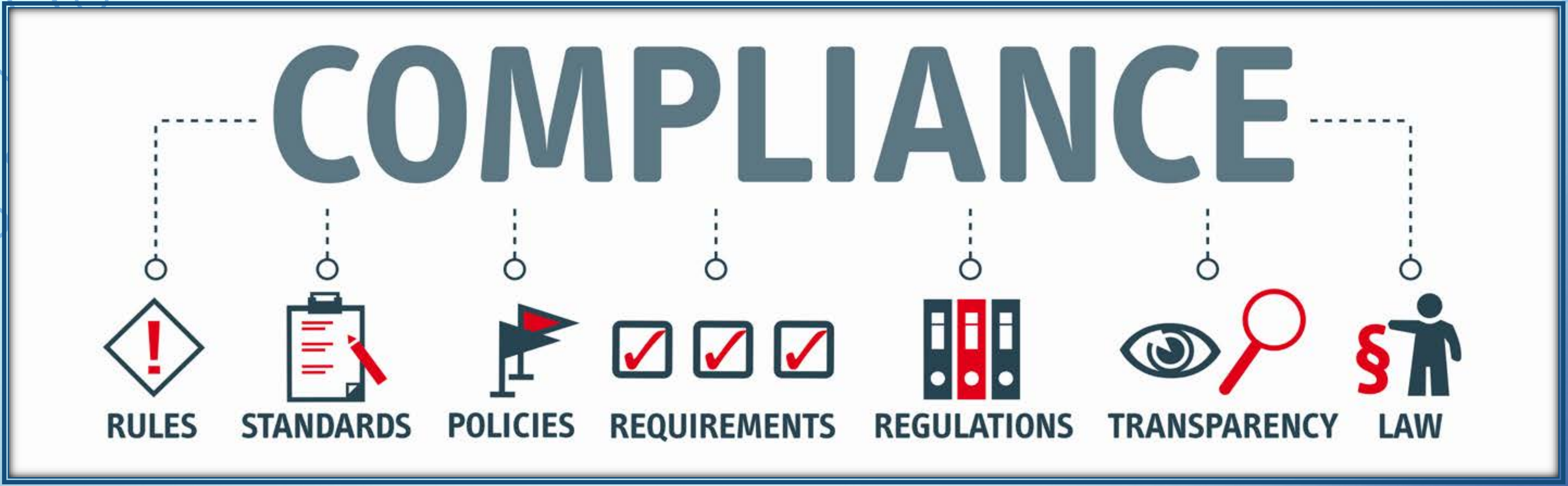
Outpatient Quality Program Systems and Stakeholder Support Team

October was National Cybersecurity Awareness Month.

Learning Objectives

Attendees will be able to:

- Describe security standards in the protection of Electronic Personal Health Information (ePHI).
- List the steps in the event of a cyberattack.
- Locate the security standards and measures found in the *Federal Register*.
- Identify at least five ways you can limit risk of cyberattack.



Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA Security Rule

- HIPAA establishes standards to protect individuals' ePHI and requires healthcare facilities to maintain reasonable safeguards.
- Additional information such as a HIPAA security rule crosswalk, resources, and links can be found on the Health and Human Services (HHS) website at hhs.gov

HIPAA Compliance

Compliance can assist in the prevention of infections of malware, including ransomware by implementing:

- Security management processes
- Procedures to guard against and detect malicious software
- Training on malicious software protections
- Controls to limit access to PHI and ePHI

Security Rule Standards

- Ensure confidentiality of all PHI
- Identify and protect against reasonably anticipated threats
- Protect against reasonable impermissible uses or disclosures
- Ensure compliance by the workforce

Breaching Your System

Phishing

Phishing is the fraudulent attempt to obtain sensitive information or data by disguising oneself as a trustworthy entity in an electronic communication. Phishing is usually carried out by:

- Email spoofing
- Instant messaging
- Text messaging

Data Breach

- A data breach is an intentional or unintentional unauthorized access of secure information.
- Basic examples are:
  - Human error
  - Theft or loss of devices
  - Employee data leak or theft
  - Cyberattacks

Breaches by the Numbers

- Many healthcare organizations have experienced a data breach in the past two years.
- Almost all web applications connected to critical health information is vulnerable to cyberattacks.
- Healthcare data breaches have an average cost of $8.6 million in the United States*.

*Source: HIPAA Journal

Breach Notification

- Notification of a breach is made to the Department of Health and Human Services, Office for Civil Rights (OCR) through the breach portal.
  - Filing of a breach can be done online.
  - The notification form is used to report the breach.

Submitting Notice of a Breach

- In breaches affecting 500 or more individuals, the covered facility must be reported without delay and in no case later than 60 calendar days from the breach.
- In breaches affecting fewer than 500 individuals, the facility must report the breach within 60 days of the end of the calendar year in which the breach was discovered.

Breaking Through Your Security

Ransomware

- Malicious software can:
    - Attempt to deny access to a user's data by encrypting the data until a ransom is paid.
        - Ransom is usually in cryptocurrency.
- Hackers may deploy ransomware that destroys data.

Threats

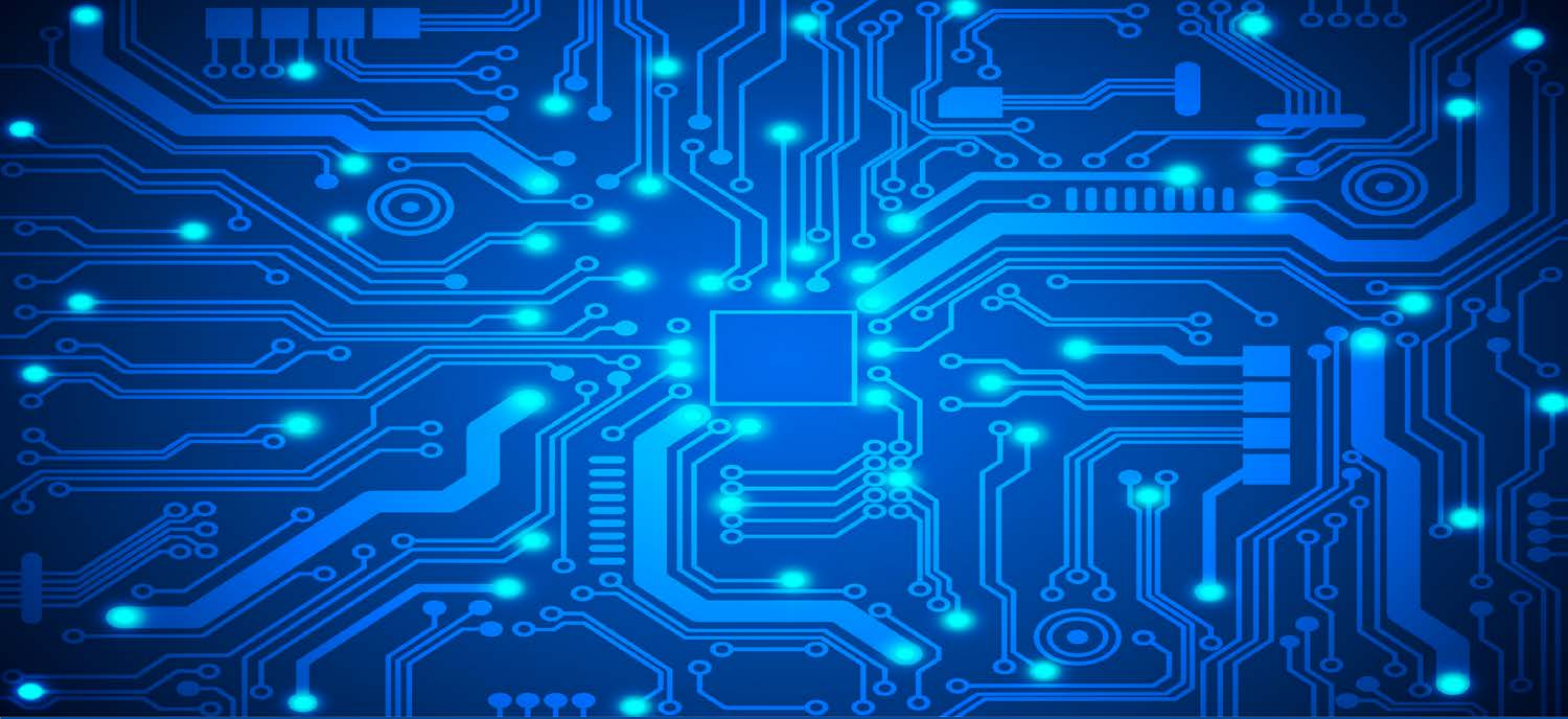
- An Advanced Persistent Threat (APT) is a long-term attack to find and exploit, steal, or disrupt operations.
- Zero Day exploits take advantage of a previously unknown hardware, firmware, or software vulnerability.
  - It is difficult to detect and contain standard hacking attacks.
  - Exploiting of vulnerabilities can be made public.

Combination Threat

An example of a combination APT and zero-day threat is the *EternalBlue* exploit.

- Targeted vulnerabilities in Microsoft's Window operating system
- Released *WannaCry* ransomware spread infecting computers around the world
- Estimated to have caused billions of dollars* in damages

* Source: Health and Human Services



Prevention, Mitigation, and Recovery

Security Measures

Security standards and measures can be found in the *Federal Register*, including the following:

- Risk analysis and risk management
- Information system activity review
- Security awareness and training
- Security incident procedures
- Contingency plan

Detection of Infected Systems

Indicators of attack could be:

- Links, files, or websites may have been malicious
- An increase in activity of the Central Processing Unit (CPU)
- The inability to access certain files
- Detection of suspicious network communications

Paying Ransom

The FBI does not recommend paying ransom*.

- Ransom does not guarantee return of data.
- Ransom may encourage further attacks.
- Corruption may occur when data is returned.

- Always report incidents to law enforcement to:
  - Prevent future attacks.
  - Enable a criminal investigation to be initiated.

* HHS

Security Incident Procedures

Procedures for responding to an attack should include processes for the following:

- Detect and conduct an initial analysis
- Contain the impact and propagation
- Eradicate and mitigate vulnerabilities
- Recover by restoring lost data
- Conduct post-incident activities

Recovering From Infection

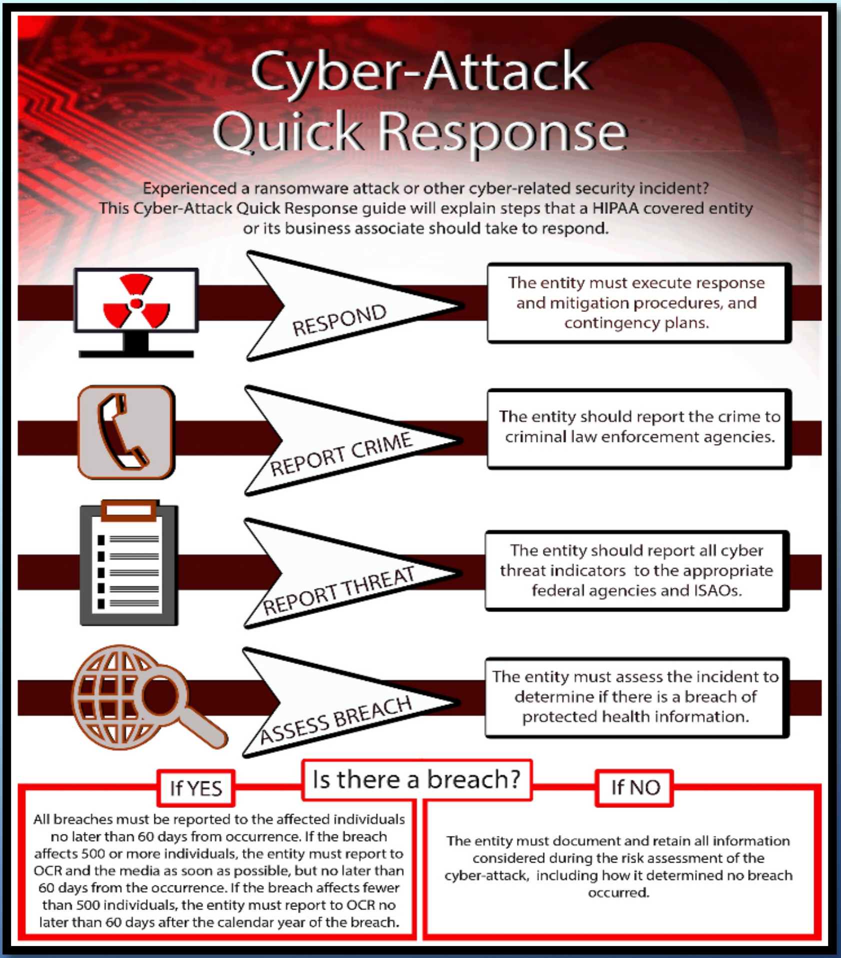
- Maintaining frequent backups
  - Conduct test restorations
- Disaster recovery planning
- Operations planning
- Analyzing the criticality of applications
- Contingency plans

Quick-Response Checklist

In the event of a cyberattack, a facility should:

- Execute its response, mitigation procedures, and contingency plans.
- Report the crime to other law enforcement agencies.
- Report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs).
- Report the breach to Office for Civil Rights (OCR) no later than 60 days after the breach affecting 500 or more individuals.

Quick Response



Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND: The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME: The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT: The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

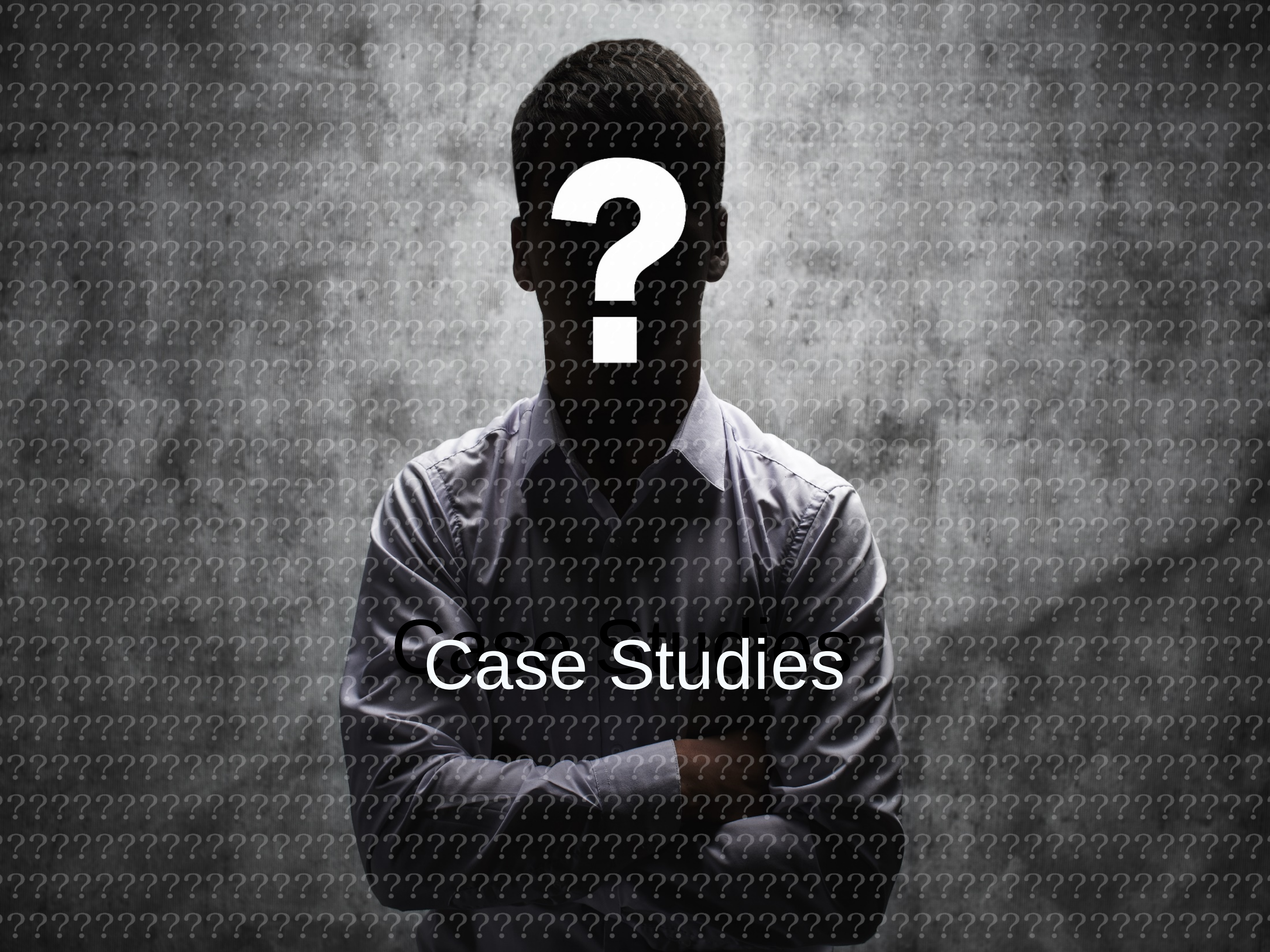
ASSESS BREACH: The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

If YES: All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

If NO: The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

Source: HHS.gov



Case Studies

Case Studies

Cyberattack: Hospital

Background:

- General medical and surgical hospital with 424 beds
- More than 500 physicians seeing over 16,000 patients

Ransom Request:

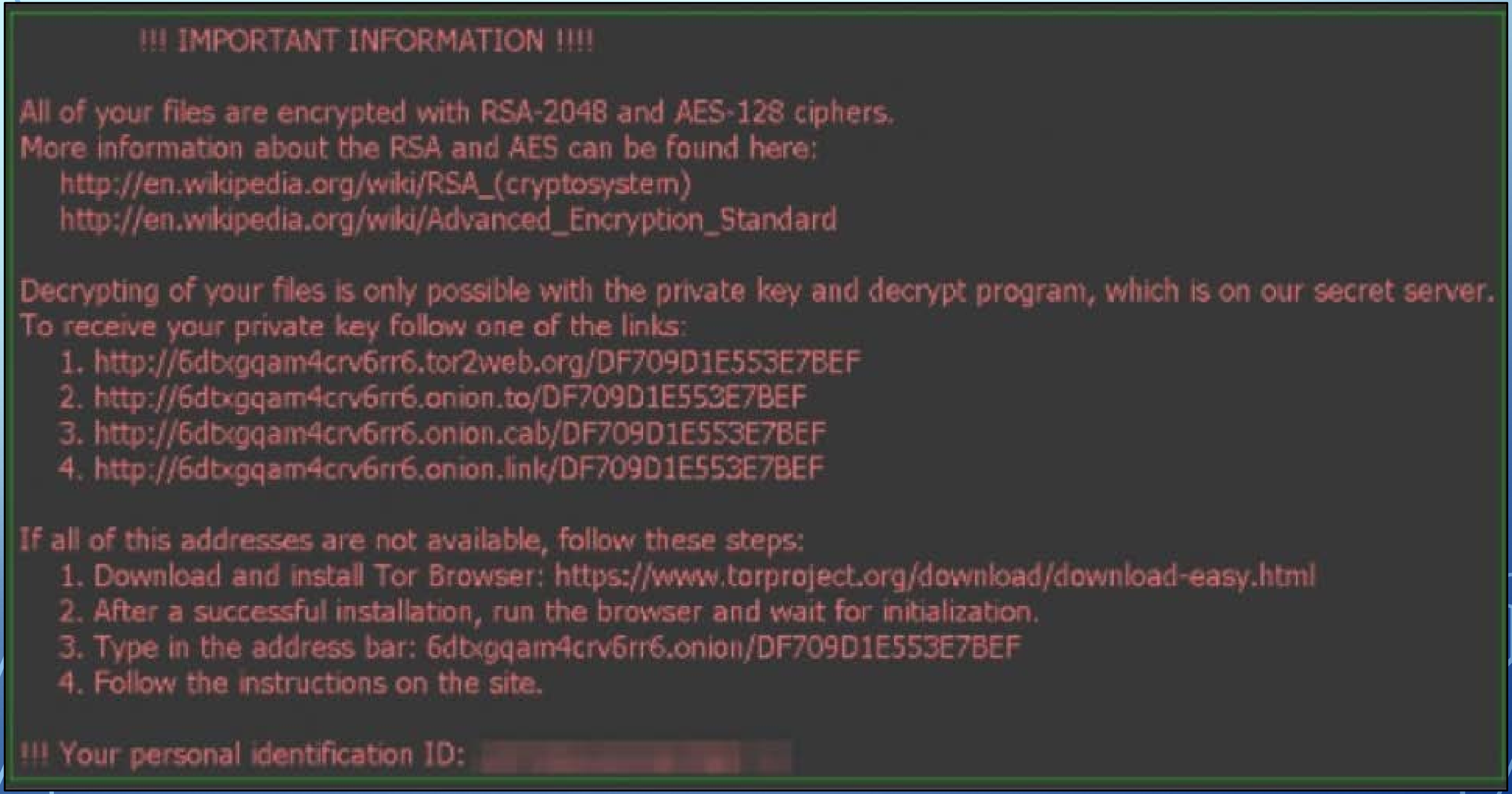
- 40 Bitcoin (approximately $17,000)

The Details

Here’s what happened:

- The computer system was hit by a ransomware virus called *Locky*.
- The CEO stated the attack was random. Symantec says *Locky* is spread usually by malicious Word documents disguised as an invoice. He felt the attack likely occurred when an employee mistakenly clicked on an email attachment that was phishing.
- Staff reported to their supervisors that they were unable to access the network.

Ransom Notice



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org/DF709D1E553E7BEF
    2. http://6dtxgqam4crv6rr6.onion.to/DF709D1E553E7BEF
    3. http://6dtxgqam4crv6rr6.onion.cab/DF709D1E553E7BEF
    4. http://6dtxgqam4crv6rr6.onion.link/DF709D1E553E7BEF

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/DF709D1E553E7BEF
    4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]

Effects of the Attack

- Internal emergency was declared, and the computer system taken offline.
- Departments were told not to turn their computers on.
- Physicians were unable to access patient medical records.
- Some patients were diverted to nearby hospitals.
- Staff resorted to record-keeping on paper.

After the Attack

The hospital did not notify law enforcement until after the ransom had been paid. All systems were cleared of the malware before law enforcement involvement.

Cyberattack: ASC

Background:

- Specialty ASC with associated physician network
- Compromised PHI of up to 400,000 patients

Ransom Request:

- $14,649.09 to be paid in only in cryptocurrency

The Details

- Employees were not able to access patient files or data.
- Hackers deployed ransomware to encrypt files on all servers.
- Encrypted files contained patient Personal Identifiable Information (PII).
- The ASC launched an investigation into the breach and contacted an IT security provider.

The Effects of the Attack

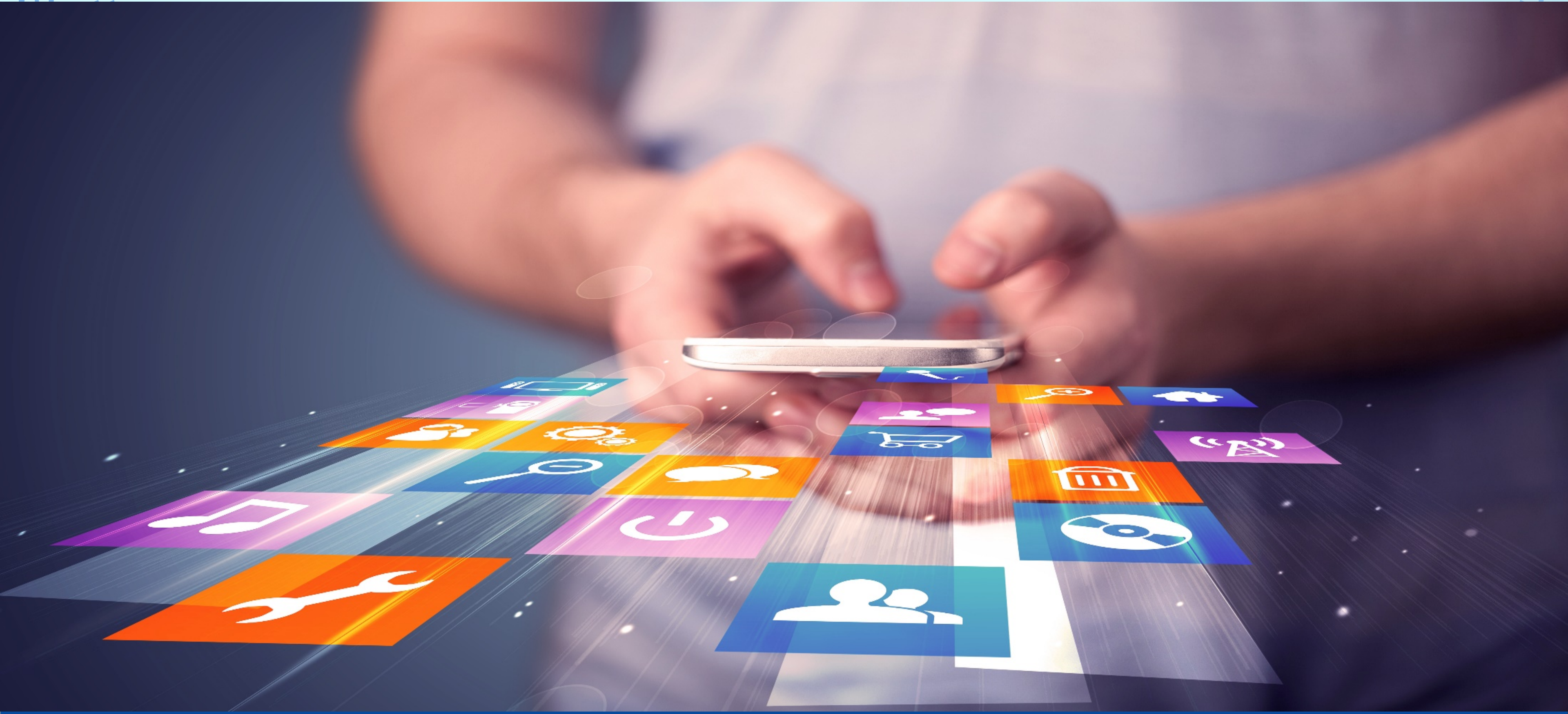
- The security company addressed the vulnerability that the hackers exploited to gain access to the network server.
- Breach notification letters were sent to the patients involved.
- Internal protocols and procedures were reviewed and updated to mitigate the risks of future ransomware attacks.

After the Attack

- The ASC did not contact law enforcement.
- The ASC paid the ransom in cryptocurrency to recover the patient files.
  - The hackers notified the ASC hours before patients were scheduled for surgeries and stated the ASC would not have access to patient information until the ransom was paid.

Storing Your Data

- Routinely backup your data and your organizations systems and configurations.
- Cloud storage
  - An off-premise system.
  - The provider should have appropriate and up-to-date procedures for handling PHI.
  - Data should be encrypted during upload, download, and while being stored.



Everyday Precautions

Passwords

Simple tips:

- Use a long passphrase.
- Don’t make passwords easy to guess.
- Avoid using common words.
- Do not share your passwords.
- Have different passwords.
- Double your login protection.
  - Use multi-factor authentication (MFA).

Social Media

Simple tips:

- There is no Delete button.
- Update your privacy settings.
- Connect with people you trust.
- Never click and tell.
- Report suspicious activity.

Applications

Simple tips:

- Treat business information as personal information.
- Technology has its limits.
- Be up-to-date.
- Social media is part of the fraud toolset.
- It only takes one time.

Remember These Quick Tips

- Don’t click without thinking.
- Use MFA when possible.
- Be aware of phishing scams.
- Keep track of your digital footprint.
- Keep up with updates.
- Connect securely.
- Back-up your data.
- Know that you are not immune.

Thank You!

Acronyms

APT	Advanced Persistent Threat	**EPHI**	Electronic Personal Health Information
ASC	Ambulatory Surgery Center	**HIPAA**	Health Insurance Portability and Accountability Act of 1996
CE	Continuing Education	**ISAO**	Information-Sharing and Analysis
CEO	Chief Executive Officer	**MFA**	Multi-factor authentication
CMS	Centers for Medicare & Medicaid Services	**OCR**	Office of Civil Rights
CPU	Central Processing Unit	**PII**	Personal Identifiable Information

Continuing Education (CE) Approval

This program has been approved for one CE credit for the following boards:

- **National credit**
  - Board of Registered Nursing (Provider #16578)
- **Florida-only credit**
  - Board of Clinical Social Work, Marriage & Family Therapy and Mental Health Counseling
  - Board of Registered Nursing
  - Board of Nursing Home Administrators
  - Board of Dietetics and Nutrition Practice Council
  - Board of Pharmacy

Note: To verify CE approval for any other state, license, or certification, please check with your licensing or certification board.

References

- https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- https://www.hhs.gov/sites/default/files/spring-2019-ocr-cybersecurity-newsletter.pdf
- https://www.ecfr.gov/cgi-bin/text-idx?SID=0ed84c7423abdfca1fa81d772667435a&mc=true&node=sp45.1.164.d&rgn=div6

References accessed on September 3, 2020.

References (cont.)

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es
- https://www.dhs.gov/science-and-technology/blog/2019/10/01/national-cybersecurity-awareness-month
- https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- https://www.hipaajournal.com/ibm-security-2020-cost-of-data-breach-report-shows-10-annual-increase-in-healthcare-data-breach-costs/
- https://www.ecfr.gov/cgi-bin/text-idx?SID=0ed84c7423abdfca1fa81d772667435a&mc=true&node=sp45.1.164.d&rgn=div6#se45.2.164_1404
- Wall Street Journal, *Online Classes Raise Stakes in New Ransomware Attacks*, September 29, 2020.

Disclaimer

This presentation was current at the time of publication and/or upload to the Quality Reporting Center or *QualityNet* websites. If Medicare policy, requirements, or guidance changes following the date of posting, this presentation will not necessarily reflect those changes; given that it will remain as an archived copy, it will not be updated.

This presentation was prepared as a service to the public and is not intended to grant rights or impose obligations. Any references or links to statutes, regulations, and/or other policy materials are provided as summary information. No material contained herein is intended to replace either written laws or regulations. In the event of any discrepancy between the information provided by the presentation and any information included in any Medicare rules and/or regulations, the rules or regulations shall govern. The specific statutes, regulations, and other interpretive materials should be reviewed independently for a full and accurate statement of their contents.