Hospital Outpatient Quality Reporting Program

Outpatient Quality Program Systems and Stakeholder Support Team

Cyber-Attacks in Healthcare

Presentation Transcript

Moderator

Karen VanBourgondien, RN, BSN
Outpatient Quality Program Systems and Stakeholder Support Team

Speaker

Melissa Thompson, RN, BSN, CMSRN
Outpatient Quality Program Systems and Stakeholder Support Team

November 18, 2020

Karen VanBourgondien Hello, everyone. Welcome and thank you for joining us today. My name is Karen VanBourgondien. Our speaker today is Melissa Thompson. We will be covering cyber-attacks in healthcare in general terms. There is a lot of information available, and we do have a variety of resources listed at the end of this presentation for your convenience.

In case you are not aware, October was National Cyber-Security Awareness month. So, in honor of that, we are presenting some basic information on cyber-security. Again, this is intended to be a general overview of data breaches, cyber-attacks, and security, and, as we all know, there has been a recent influx in cyber-attacks and ransomware in our healthcare community. So, our intent is just to provide you with some basic information. Again, we have plenty of resources listed at the end of this presentation.

The learning objectives for this presentation are listed here on this slide.

This program is being recorded. A transcript of today's presentation, including the questions and answers received in the chat box, and the audio portion of today's program will be posted on Quality Reporting Center, shortly.

During the presentation, if you have a question, please put that question in the chat box located on the left side of the screen, and we will try our very best to respond to your question or point you to appropriate resources.

So, without any further ado, let me now hand things over to our speaker Melissa Thompson. Melissa?

Melissa Thompson: Thank you, Karen. Let's begin this discussion with the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA. As healthcare workers, we are familiar with this act. You know this is all about keeping patient information private. In the event of a data breach or cyber-attack, are you sure you have done everything to protect patient data?

Let’s take a look at HIPAA in a little more detail and how it relates to our subject today.

The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information and requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting Personal Health Information (PHI).

HIPAA is quite extensive. So, if you want more information specific to this, you can click on the Health and Human Services link here.

So, can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware? The answer is yes.

The HIPAA Security Rule requires implementation of security measures.

Some of these required security measures include implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to PHI and implementing security measures to mitigate or remediate those identified risks; implementing procedures to guard against and detect malicious software; training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

The Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI the entity creates, receives, maintains, or transmits and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

For those of you not aware, a covered entity is defined by HIPAA as any health plan, or any healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information, or PHI, in electronic form. For the sake of simplicity, in this presentation, we may simply use facility.

It is expected that covered entities and business associates will use this process of risk analysis and risk management not only to satisfy the specific standards and implementation specifications of the Security Rule but also when implementing security measures to reduce the particular risks and vulnerabilities to ePHI throughout an organization's entire enterprise, identified as a result of an accurate and thorough risk analysis, to a reasonable and appropriate level.

Facilities should ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; identify and protect against reasonably anticipated threats to the security or integrity of the information; protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce.

Cyber-attacks, either on your personal computer or your workplace, can be disastrous, as some of you may very well know. Hackers have incredible ways of breaking in.

Phishing. Everyone has heard this term. Phishing is the fraudulent attempt to obtain sensitive information or data and phishing is usually carried out in email spoofing, instant messaging, and test messaging.

Phishing emails are messages sent by individuals trying to "fish" for personal or financial information. Through phishing, a hacker may attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication, typically carried out by email spoofing or instant messaging that directs users to a site or a phone number that is fraudulent. These attempts are getting better every day at making their messages look authentic.

Phishing is only one example of how hackers can gain access.

A data breach is intentional or unintentional unauthorized access of secure or private/confidential information. In any instance, when information is accessed without authorization, it's a data breach. Common forms of data breaches are malware, phishing, denial of service, and ransomware. This however is not a comprehensive list.

The types of violations can vary and evolve as technology diversifies, but, to put it simply, the information in the wrong hands constitutes a data breach. Information can become compromised in many ways now; a cyber-attack is only one way. As the name implies, it's a confirmed incident when an unauthorized entity has accessed confidential, sensitive, or protected information. Big data is now the norm, as more devices become connected. Those valuable connections also become points of weaknesses. Data breaches can wreak havoc on the reputations of businesses and induce a ripple of after-effects that can leave lasting repercussions.

Examples of data breaches include human error. Errors cannot be avoided, people make mistakes, and information may get distributed without mal intent. Proprietary data can get sent accidentally to the wrong person, and uploads to public folders or misconfigured servers can bleed sensitive information. Theft or loss of devices: We all have devices. From smartphones to laptops, hard drives, USBs, and other data storage devices, data can easily get stolen, misplaced, lost, or disposed of incorrectly. Sensitive or protected information saved on those devices can end up in the wrong hands and lead to a more significant data breach. Employee data leak or theft: When a company terminates an employee or ends a contract with notice, that person may deliberately access protected information without permission and copy it. They may use or distribute it with malicious intent. Cyber-attacks: Hacking is the most apparent form of a data breach. Hackers use malware, phishing, social engineering, skimming, and scams to get access to sensitive and encrypted information.

Many healthcare organizations experienced a data breach in the past two years. Despite the sophisticated measures put in place by providers to prevent data breaches, they are still common.

Web applications connected to critical health information are vulnerable to cyber-attacks. Network penetration results also showed that hackers could easily access domain level admin privileges of most healthcare applications. As a result, the use of advanced technologies such as block-chain and cloud computing are necessary to ward off such attacks in the future.

Healthcare data breaches are the costliest to resolve. The average cost of a healthcare data breach is $7.13 billion globally and $8.6 million in the United States. The total cost of a data breach may have fallen across all regions and industry sectors, but healthcare data breach costs have increased by 10.5 percent year-over-year.

If your facility does experience a breach, notification is made to the U.S. Department of Health and Human Services Office for Civil Rights (OCR). You can file the breach online using the notification form to report the breach.

A facility must report a breach of unsecured protected health information.

A facility's breach notification obligation differs based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the number of individuals affected by a breach is uncertain at the time of submission, the facility should provide an estimate, and, if it discovers additional information, submit updates in the manner specified here. If only one option is available in a particular submission category, the covered entity should pick the best option and may provide additional details in the free text portion of the submission.

If a breach of unsecured protected health information affects 500 or more individuals, a facility must report the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice completing all of the required fields of the breach notification form.

If a breach of unsecured protected health information affects fewer than 500 individuals, a facility must report the breach within 60 days of the end of the calendar year in which the breach was discovered. A facility is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a facility may report such breaches at the time they are discovered.

What if hackers break through your system? What could happen? Let's talk about ransomware.

Ransomware is a type of malware or 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 deployed the malware, until a ransom is paid. Ransomware is a form of extortion. It's a malware that infects, overtakes, and locks your data, making it inaccessible unless a ransom is paid.

After the user's data are 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 exfiltrates data, or ransomware in conjunction with other malware that does so.

There are many types of threats. An advanced persistent threat, or APT, is a long-term cyber-security attack that continuously attempts to find and exploit vulnerabilities in a target's information systems to steal information or disrupt the target's operations. Although individual APT attacks need not be technologically sophisticated, the persistent nature of the attack, as well as the attacker's ability to change tactics to avoid detection, make APTs a formidable threat.

Any security incident impacting the confidentiality, integrity, or availability of protected health information, can directly affect the health and safety of citizens. APTs have already been implicated in several cyber-attacks on the healthcare sector.

One of the most dangerous tools in a hacker's arsenal is the *zero day* exploit or attack which takes advantage of a previously unknown hardware, firmware, or software vulnerability. Hackers may discover z*ero day* exploits by their own research, or probing, or may take advantage of the lag between when an exploit that is discovered and when a relevant patch or anti-virus update is made available to the public.

These exploits are especially dangerous because their novel nature makes them more difficult to detect and contain than standard hacking attacks.

The possibility of such an attack emphasizes the importance of an organization's overall security management process, which includes monitoring of anti-virus or cyber-security software for detection of suspicious files or activity. Though hackers may exploit *zero day* vulnerabilities to gain unauthorized access to an organization's computer system, appropriate safeguards, including encryption and access controls, may mitigate or even prevent unauthorized access to, or loss of, protected information. Once *zero day* vulnerabilities are made public, this information becomes accessible to both good and bad actors alike, which means facilities should have measures in place to be aware of new patches and for assessing the need to apply them.

Now, let me pause here a minute. When we use the term "actor" we are referring to people who are accessing your system. So, a good actor would be someone legitimately accessing your facility's system. A bad actor would be someone coming in with ill intent. That's the simple explanation, but you will hear that term as we move forward.

In the event a timely patch is not available, or cannot be immediately implemented (such as when testing is needed to ensure that the patch works with components of an entity's information systems), an entity may consider adopting other protective measures such as additional access controls or network access limitations to mitigate the impact of the *zero day* vulnerability until a patch is available.

So, to put this into perspective, let's use an example of a combination APT and *zero day* threat. This is a relatively known threat. You may have heard of it.

APTs and *zero day* threats are dangerous enough by themselves. An APT using a *zero day* exploit can threaten computers and data all over the world. One such example is the *EternalBlue* exploit. *EternalBlue* targeted vulnerabilities in several of Microsoft's Windows operating systems. Soon after the *EternalBlue* exploit became publicly known, the *WannaCry* ransomware was released and began spreading, eventually infecting hundreds of thousands of computers around the world.

The damages due to *WannaCry* infections are estimated to be in the billions of dollars. Analysis of *WannaCry* found that it used *EternalBlue* to spread and infect other systems. One of the organizations most impacted was the United Kingdom's National Health Service (NHS), which had up to 70,000 devices infected, forcing healthcare providers to turn away patients and shut down certain services. Several HIPAA covered entities and business associates in the United States were also affected by this cyber-attack.

Facilities should be mindful that ransomware attacks often occur after prior instances of unauthorized access and malware infection. A threat sometimes needs to have access and privileges on a victim's information system in order to initiate the infection. Further, certain types of ransomware have been observed to "piggyback" into a system, using other malware as a tool for deployment. Proper implementation of several HIPAA Security Rule provisions can help covered entities and business associates prevent, mitigate, and recover from ransomware attacks.

As part of health insurance reform, the department of health and human services does have security standards found in the *Federal Register.*

Risk analysis and risk management: Covered entities and business associates are required to conduct a thorough and accurate assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their ePHI and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Identifying and addressing technical vulnerabilities within information systems and information technology infrastructure is crucial to preventing ransomware attacks. Successful ransomware deployment often depends on exploitation of technical vulnerabilities such as outdated software, unsecured ports, and poor access management. Implementing effective security tools including anti-malware software and intrusion detection/prevention solutions can also help prevent, detect, and contain attacks. Identifying and reducing these potential risks and vulnerabilities is key to making an organization a less inviting target.

Information System Activity Review: If ransomware is able to overcome an organization's first level of defenses and enter the organization's network and information systems, effective system monitoring, then a review will be critical to detecting and containing the attack. Identifying anomalous activity, especially such activity executed with elevated privileges, can be crucial to identifying an attack in progress. Covered entities and business associates are required to regularly review records of information system activity. Such records can include audit logs, access reports, and security incident tracking reports.

Security awareness and training should be carried out for information. System users remain one of the weakest links in an organization's security posture. Social engineering, including phishing attacks, is one of the most successful techniques used by threat actors to compromise system security. A training program should make users aware of the potential threats they face and inform them on how to properly respond to them. This is especially true for phishing emails that solicit login credentials. Additionally, user training on how to report potential security incidents can greatly assist in an organization's response process by expediting escalation and notification to proper individuals.

"Security Incident Procedures" refers to an organization's incident response. Procedures can greatly limit the damage caused by a ransomware attack. Organizations may consider addressing ransomware attacks specifically within its response policies and procedures as mitigation actions may vary between different types of incidents. Quick isolation and removal of infected devices from the network and deployment of anti-malware tools can help to stop the spread of ransomware and to reduce the harmful effects of such ransomware. Response procedures should be written with sufficient details and be disseminated to proper workforce members so that they can be implemented and executed effectively. Further, organizations may consider testing their security incident procedures from time to time to ensure they remain effective. Familiarity with the execution of security incident procedures should reduce an organization's reaction time and

increase its effectiveness when responding to an actual security incident or breach. Identifying and responding to suspected security incidents is key to mitigating potential harm following an intrusion.

A contingency plan should be in effect. An effective and robust contingency plan is essential to recover from a ransomware attack. Proper implementation of this provision will allow an organization to continue to operate critical services during an emergency and recover ePHI. Because patient health and safety may be impacted, tolerance of system downtime is low and ePHI availability requirements are high. A covered entity or business associate must backup ePHI and ensure that it is accessible and recoverable in the event of a ransomware attack. Organizations should keep in mind that threat actors have recently been actively targeting backup systems and backup data to prevent recovery. Maintaining recoverable, secure, and up-to-date backups is one of the most important safeguards against ransomware attacks.

So, you may be asking yourself: How can your facility detect if their computer systems are infected with ransomware?

Well, unless ransomware is detected and propagation halted by malicious software protection or other security measures, your facility would typically be alerted to the presence of ransomware only after the ransomware has encrypted data and alerted the facility to its presence to demand payment.

However, in some cases, a facility's workforce may notice early indications of a ransomware attack that has evaded the entity's security measures. HIPAA's requirement that an entity's workforce receive appropriate security training, including training for detecting and reporting instances of malicious software, can assist facilities in preparing their staff to detect and respond to ransomware.

Indicators of a ransomware attack could include a user's realization that a link was clicked on, a file attachment opened, or a website visited may have been malicious in nature. An increase in activity in the central processing

unit, or CPU, of a computer and disk activity for no apparent reason may be due to the ransomware searching for, encrypting, and removing data files. An inability to access certain files as the ransomware encrypts, deletes and re-names and/or relocates data and detection of suspicious network communications between the ransomware and the attackers' command and control server(s), this last indicator would most likely be detected by IT personnel via an intrusion detection or similar solution.

The FBI does not recommend paying the ransom demanded by the initiator of the ransomware attack, as payment does not guarantee that a facility's data will be returned, and payment could provide encouragement for further ransomware attacks. The FBI has noted that there have been instances where the decryption key was not provided after the ransom was paid, or the data was corrupted when it was returned. The FBI recommends always reporting ransomware incidents to law enforcement to prevent future attacks and to enable a criminal investigation to be initiated.

Now, having said that, ransomware negotiating companies state that 99 percent of the time hackers deliver a decryption tool to the hostage companies or organizations once the ransom was paid. The decryption tool re-enables data access.

A ransomware negotiating firm reported an increase in average ransomware payments for all industries, not just healthcare, up 60 percent to $178,254.

We are going to discuss this again a little later in the presentation when we discuss the case studies.

Security incident procedures, including procedures for responding to and reporting security incidents, are also required by HIPAA. An entity's security incident procedures should prepare it to respond to various types of security incidents, including ransomware attacks. Robust security incident procedures for responding to a ransomware attack should include processes to detect and conduct an initial analysis of the ransomware; contain the impact and propagation of the ransomware; eradicate the

instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation; recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information) and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

Part of a deeper analysis should involve assessing whether or not there was a breach of PHI as a result of the security incident. The presence of ransomware (or any malware) is a security incident under HIPAA that may also result in disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack.

Because ransomware denies access to data, maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Because some ransomware variants have been known to remove or otherwise disrupt online backups, entities should consider maintaining backups offline and unavailable from their networks.

Additional activities that must be included as part of an entity's contingency plan include disaster recovery planning, emergency operations planning, analyzing the criticality of applications and data to ensure all necessary applications and data are accounted for, and periodic testing of contingency plans to ensure organizational readiness to execute such plans and provide confidence they will be effective.

During the course of responding to a ransomware attack, an entity may find it necessary to activate its contingency plans. Once activated, an entity will be able to continue its business operations while continuing to respond to and recover from a ransomware attack. Maintaining confidence in contingency plans and data recovery is critical for effective incident response, whether the incident is a ransomware attack or fire or natural disaster.

Here on this slide is a quick-response checklist that you should follow in the event of a cyber-attack.

A facility must execute its response and mitigation procedures and contingency plans. For example, the entity should immediately fix any technical or other problems to stop the incident. The facility should also take steps to mitigate any disclosure of protected health information, which may be done by the entity's own information technology staff or by an outside entity brought in to help.

You should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule. If a law enforcement official tells the facility that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.

You should report all cyber-threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. The Office for Civil Rights, or OCR, does not receive such reports from its federal or HHS partners.

Lastly, you must report the breach to the OCR, as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify individuals without unreasonable delay, but no later than 60 days after discovery, and OCR within 60 days after the end of the calendar year in which the breach was discovered.

The department of Health and Human Services has this Cyber-Attack Response Checklist in the event of exposure to this kind of attack. This summarizes what we just discussed.

As mentioned early in the presentation, healthcare facilities continue to be targets of various types of cyber-attacks. The following are just two such attacks.

First up, an attack on a hospital. The background on our first case study is a general medical and surgical hospital which has 424 beds and more than 500 doctors who saw over 16,000 patients. The initial ransom request was 40 Bitcoin with the equivalent payout of $17,000.

With this particular situation, the computer system was hit by a ransomware virus called *Locky*, which locks users out and won't send a decrypting key unless a ransom is paid.

Since the CEO stated that the attack was random and Symantec says *Locky* is spread usually via a malicious Word document disguised as an invoice, they felt it was likely the attack occurred because an employee mistakenly clicked on an email attachment that was actually a phishing scam.

Some members of the staff reported to their supervisors that they were unable to access their network.

This is a screen shot image of the notification sent by the hackers. This is letting them know that all of their files have been encrypted and the facility would need a private key to enter the secret server.

Immediately following discovery, an internal emergency was declared, and the computer system taken offline.

Some departments, including Radiation Oncology were told not to turn on their computers at all. Doctors told reporters they were unable to access patient's medical histories and could not share x-rays, CT scans, and other medical tests. Some patients were diverted to nearby hospitals, and staff had to resort to doing patient admissions and other record-keeping by pen and paper.

The hospital paid the ransom in Bitcoin, which remember, was equivalent to approximately $17,000.

Unfortunately, law enforcement wasn't notified about the breach until after the hospital had already paid the ransom. After the ransom was paid, and they had cleared the malware, they obtained their files.

As we talked about previously, and as it is outlined in the checklist, it is recommended to call in authorities before paying ransom.

Now, let's look at an example involving an Ambulatory Surgical Center (ASC). In this example, the specialty also had physician offices in their organization. They announced a ransomware attack on their facility potentially compromised the PHI of up to 400,000 patients. The requested ransom was $14,649.09 to be paid in cryptocurrency.

The ASC discovered the attack, immediately launched an investigation into the breach, and contracted an IT security provider to assist with the investigation. As with the hospital example, employees were not able to access any patient files or data.

Investigators discovered that the hackers had deployed ransomware to encrypt files on their servers. The encrypted files contained patient information such as names, driver's license numbers, social security numbers, and other types of protected health information.

The ASC and the IT security provider stated they went through their systems with a fine-tooth comb and eventually determined that it was unlikely that the hackers had stolen any of the sensitive information, but, due to the nature of the ransomware and how the infection first began, there cannot be a guarantee.

The ASC stated that patients are at low risk of hackers using their data for nefarious purposes and becoming victims of fraud. Following HIPAA's Breach Notification Rule, notification letters were sent to affected patients out of an abundance of caution.

The ASC then addressed the vulnerability that hackers exploited to gain access to the network server. This ASC stated that it is in the process of reviewing internal protocols and procedures to mitigate the risks of a future ransomware attack occurring.

The ASC did not contact law enforcement and revealed that they agreed to pay the hackers $14,649.09 in cryptocurrency to recover the patient files.

The ASC received notice from the hackers that encrypted the files just a few short hours before several patients were scheduled for surgeries. In this notice, the hackers made it clear that the ASC would not have access to patient information until they were paid a fee. The ASC later stated, "We quickly determined that the health and well-being of our patients was the number one concern, and, when we made the payment, they gave us the decryption key so we could immediately proceed unlocking the data."

Now, these are just a couple of examples. In both of these examples, the facilities paid the ransom. We stated earlier the FBI recommends not paying the ransom, but the ransomware negotiation companies state that, 99 percent of the time, hackers do deliver a decryption tool once the ransom is paid.

There are certainly healthcare facilities that did not pay ransom because they had real-time access to their data.

That brings up the question of backing up your data. In addition to encryption, you should fully back up your data. If you have your data in an alternate location, you can use that instead of being at the mercy of the cyber-attack. It may seem obvious, but look at the ransomware cases, two of which we just discussed. Both facilities felt they had no option but to pay the ransom because they needed the data.

In addition to having data backed up, healthcare organizations can help protect themselves from ransomware attacks succeeding by essentially backing up their systems and configurations. This particular kind of backup is what many in information security and software circles call a "gold image."

Another option is the cloud. Should data be stored in the cloud or not? That's a good question.

Many health providers prefer to move their infrastructure to the cloud. Cloud services allow data to be stored in multiple locations. This can be beneficial if there is a fire, natural disaster, or power outage, or as we are discussing, a cyber-attack; It can provide reassurance that critical business functions or operations will not be interrupted.

The cloud is an off-premise system in which data needs are outsourced to a third-party provider. These providers are trusted to perform updates, maintenance, and manage security. The downside is you are placing responsibility for your data with someone else. There is also a lack of standardization within the cloud. There is no clear guideline that unifies the various cloud providers. Thus, it becomes more challenging with various sectors for which these providers offer services.

Customer service is another risk of moving your data to the cloud. If there is ever a data breach or security update you need immediately applied, you will need to speak to the provider as soon as possible. Since healthcare providers have PHI, be prepared to invest in a cloud provider that can provide a level of service that meets your needs.

It is important to verify the cloud provider's security standards are appropriate. Make sure they have up-to-date procedures on patching and actively upgrade their equipment. Also, review their security policies as they pertain to the cloud environment. Your provider should have an actively managed compliance program that verifies their adherence to the various regulatory requirements and security standards.

PHI should never be stored in the cloud unless it is encrypted while in storage. Your data should also be encrypted when being uploaded to or downloaded from the cloud. Only certain members of your organization who are required access should be able to decrypt the data. Your organization should create policies that detail the circumstances that this information can be decrypted. All of this should be reviewed and agreed upon in the terms of service within your agreement with the cloud service provider.

The biggest risk for cloud computing is you never know how the provider will perform. Hackers aren't going away and will keep trying to access your data. As technology advances, so do the risks that come with adopting them.

We have become a digital world with cell phones, social media, email, even watching this presentation now. So, let's talk about some recommended everyday precautions.

Creating a strong password is easier than you think. Follow these simple tips to shake up your password protocol.

Use a long passphrase. You should consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then, add in some punctuation and capitalization.

Don’t make passwords easy to guess. Do not include personal information in your password such as your name or pet names. This information is often easy to find on social media, making it easier for cyber-criminals to hack your accounts.

Avoid using common words in your password. Substitute letters with numbers and punctuation marks or symbols. For example, the @ can replace the letter “A” and an exclamation point (!) can replace the letters “I” or “L.”

Get creative. Use phonetic replacements, such as “ph” instead of “f,” or make a deliberate or obvious misspelling such as replacing the “i” in smile with a “y.”

Keep your passwords on the downlow. Don’t tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.

Unique account, unique password. Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It’s important to mix things up. Find easy-to remember ways to customize your standard password for different sites.

Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If multi-factor authentication is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token. This sort of authentication is what you will use when you sign into your HARP account.

Social media. Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. For your hospital or ASC, you may use some form of social media as well.

So, how can you be proactive to stay safe online?

Remember, there is no Delete button on the Internet. Share with care. Even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it.

Update your privacy settings. Set the privacy and security settings to your comfort level for information sharing. Disable geotagging, which allows anyone to see where you are, and where you aren't, at any given time.

Connect only with people you trust. While some social networks might seem safer for connecting because of the limited personal information shared through them, keep your connections to people you know and trust.

Never click and tell. Limit what information you post on social media, from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings, online and in the real world. Keep your social security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are, and where you aren't, at any given time.

Report suspicious or harassing activity. Work with your social media platform to report and possibly block harassing users. Report an incident if you've been a victim of cyber-crime. Local and national authorities are ready to assist you.

We have already discussed the significant financial loss when a cyber-attack occurs.

Again, cybercriminals often rely on human error, employees failing to install software patches or clicking on malicious links, to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure.

Treat business information as personal information. Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information, or PII, through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.

Technology has its limits. As “smart” or data-driven technology evolves, it is important to remember that security measures only work if used correctly by employees. Smart technology runs on data, meaning devices such as smartphones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches.

Be up to date. Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don’t have to think about it and set your security software to run regular scans.

Social media is part of the fraud toolset. By searching Google and scanning your organization’s social media sites, cyber-criminals can gather information about your partners and vendors, as well as human resources and financial departments. Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms.

It only takes one time. Data breaches do not typically happen when a cybercriminal has hacked into an organization’s infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure.

Be wary of unusual sources, do not click on unknown links, and delete suspicious messages immediately.

As a quick summary, remember these tips.

Clicking without thinking is reckless. Just because you can click, it doesn't mean you should. Malicious links can do damage in several different ways, so be sure to inspect links and ensure they're from trusted senders before clicking.

Use two-factor authentication. It's important to have a strong password, but it's even more imperative to have two-factor, or multi-factor, authentication. As we talked about earlier, this method provides two layers of security measures. So, if a hacker can accurately guess your password, there is still an additional security measure in place to ensure that your account has not been breached.

Look out for phishing scams. With over 3 billion fake emails sent daily, phishing attacks are some of the greatest cyber-security threats, as they are very easy to fall for. Remember, in a phishing attack, a hacker will pose as someone that the recipient may be familiar with to trick them into opening a malicious link, divulging important credentials, or opening software that infects the recipient's system with a virus. The best way to be on the lookout for phishing scams is by avoiding emails from unfamiliar senders, looking for grammatical errors or any inconsistencies in the email that looks suspicious, and hover over any link you receive to verify where the destination is.

Keep track of your digital footprint. When you monitor your accounts, you can ensure you catch suspicious activity. It's important to keep track of your digital footprint, including social media, and to delete accounts you're not using, while ensuring you set strong passwords that you change regularly.

Keep up with updates. Software patches can be issued when security flaws are discovered. If you find these software update notifications to be annoying, you're not alone, but you can consider them the lesser of two evils when weighing up rebooting your device versus putting yourself at risk for malware and other types of computer infection.

Connect securely. You might be tempted to connect your device to an unsecured connection, but, when you weigh the consequences, it's not worth it. Only connect to private networks when possible, especially when handling sensitive information.

Back up your data. These days, storage doesn't cost much. There's no excuse not to have a backup of important data. Back it up on a physical location and on the cloud. Remember, malicious threats and hackers don't always want to steal your data, but sometimes the end-goal is to encrypt or erase it, as we talked about earlier and saw in our examples. Back it up to have an ultimate recovery tool.

Remember, you're not immune, no one is. The most harmful thought you can have is "it won't happen to me," or "I don't visit unsafe websites." Cyber-criminals don't discriminate in targeting all sorts of users. Be proactive. Simple cyber-security tips like these can go a long way in preventing a catastrophe.

That concludes our presentation on cyber-attacks. I'm going to turn things back over to Karen.

Karen VanBourgondien: Thank you, Melissa. That was a lot of information and very informative. Again, we do have resources at the end of this presentation. Many of the resources link to more resources. So, it is quite a bit of information at your disposal. So, again, that's all we have today. We really appreciate your joining us. We hope this information is useful for you in preventing cyber-attacks, ransomware, etc.

Have a great day everyone. Thanks again!