Welcome to PMI’s Webinar Presentation

Meet the Presenter...

Larry Neiswender

On the topic:

5 HIPAA Issues You Must Address with Your Team
Welcome to Practice Management Institute’s Webinar and Audio Conference Training. We hope that the information contained herein will give you valuable tips that you can use to improve your skills and performance on the job. Each year, more than 40,000 physicians and office staff are trained by Practice Management Institute. For 30 years, physicians have relied on PMI to provide up-to-date coding, reimbursement, compliance and office management training. Instructor-led classes are presented in 400 of the nation’s leading hospitals, healthcare systems, colleges and medical societies.

PMI provides a number of other training resources for your practice, including national conferences for medical office professionals, self-paced certification preparatory courses, online training, educational audio downloads, and practice reference materials. For more information, visit PMI’s web site at www.pmiMD.com

Please be advised that all information in this program is provided for informational purposes only. While PMI makes all reasonable efforts to verify the credentials of instructors and the information provided, it is not intended to serve as legal advice. The opinions expressed are those of the individual presenter and do not necessarily reflect the viewpoint of Practice Management Institute. The information provided is general in nature. Depending on the particular facts at issue, it may or may not apply to your situation. Participants requiring specific guidance should contact their legal counsel.

CPT® is a registered trademark of the American Medical Association.
5 HIPAA ISSUES YOU MUST ADDRESS WITH YOUR TEAM

Presented by
Larry Neiswender

Brought to you by
Practice Management Institute®

1. Technical training isn’t always technical
2. Guidance on e-mail and text messaging
3. Appropriate access for pertinent staff
4. Mobile device controls
5. Social media challenges
“Security Standards for the Protection of Electronic Protected Health Information”

HIPAA SECURITY RULE

HIPAA §164.308 Administrative safeguards

(A) **Risk analysis (Required)**
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
Guidance on e-mail and text messaging

1. You are (basically) not held accountable for emails and text messages you receive. You are **ALWAYS** held accountable for emails and text message you SEND.

2. Personally Identifiable Information must be encrypted at rest and in transmission.
In the Security Risk Analysis, you’ll find this question:

Is sensitive information transferred to external recipients? If so, are controls in place to protect sensitive information when transferred (e.g. with encryption)?

**Scope: What is Covered?**

- Electronic Protected Health Information ("E-PHI"):  
  - Protected health information  
  - Transmitted or maintained in electronic media  
- Not E-PHI:  
  - Electronic Transmission Media excludes:  
    - Transmissions of paper  
    - Transmissions by facsimile  
    - Voice by telephone  
    - because the information did not exist in electronic form before transmission

(DHHS Office for Civil Rights)

In the Security Risk Analysis, you’ll find this question:

Is sensitive information transferred to external recipients? If so, are controls in place to protect sensitive information when transferred (e.g. with encryption)?

**Lack of Transmission Security**

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. § 164.312(e)(2)(ii).  
- Applications for which encryption should be considered when transmitting ePHI may include:  
  - Email  
  - Texting  
  - Application sessions  
  - File transmissions (e.g., ftp)  
  - Remote backups  
  - Remote access and support sessions (e.g., VPN)

(DHHS Office for Civil Rights)
In the Security Risk Analysis, you’ll find this question:

Is sensitive information transferred to external recipients? If so, are controls in place to protect sensitive information when transferred (e.g. with encryption)?

“Security Rule Overview for Small Providers”

It says, “To understand the requirements of the Security Rule, it is helpful to be familiar with the basic concepts that comprise the security standards and implementation specifications.”

“Each Security Rule standard is a requirement: a covered entity must comply with ALL of the standards of the Security Rule with respect to the e-PHI it creates, transmits or maintains.”
It goes on to explain,

• "Many of the standards contain implementation specifications.
• "An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard."
• "Implementation specifications are either required or addressable."
• "A required implementation specification is similar to a standard, in that a covered entity must comply with it."

“For addressable implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the covered entity’s environment. After performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions. For example, all covered entities including small providers must determine whether “Encryption and Decryption” is reasonable and appropriate for their environment in accordance with Section 164.312(a)(1) of the Security Rule.”
“Factors that determine what is “reasonable” and “appropriate” include cost, size, technical infrastructure and resources. While cost is one factor entities must consider in determining whether to implement a particular security measure, some appropriate measure must be implemented. An addressable implementation specification is not optional, and the potential cost of implementing a particular security measure does not free covered entities from meeting the requirements identified in the rule.”

Guidance on e-mail and text messaging

Healthcare Email Fraud Attacks Have Increased 473% in 2 Years

HIPAA Journal Feb 14, 2019

A recent report from Proofpoint has revealed healthcare email fraud attacks have increased 473% in the past two years.

These email attacks are highly targeted and typically involve the spoofing of email addresses to make emails appear to have been sent internally or from a trusted individual.

For the report, Proofpoint analyzed more than 160 billion emails sent by organizations in 150 countries between Q1, 2017 and Q4, 2018.

95% of targeted healthcare organizations experienced attacks using their own trusted domain and 100% of attacked organizations had their domain spoofed in attacks on their business partners and patients.
Appropriate access for pertinent staff

In the Security Risk Analysis, you’ll find these questions:

• Do you have a formal access authorization process based on 'least privilege' (employees are granted the least amount of access possible in order to perform their assigned duties) . . . ?
• How are systems and applications configured to restrict access only to authorized individuals?
• Are user IDs for your system uniquely identifiable?
• Do you have a process to review user accounts and related access?
**Appropriate access for pertinent staff**

**Study Reveals 75% of Employees Lack Security Awareness**
HIPAA Journal – October 25, 2018

**53% of Healthcare Data Breaches due to Insiders and Negligence**
HIPAA Journal – November 22, 2018

The healthcare industry has had more than its fair share of hacking incidents, but the biggest threat comes from within. The actions of healthcare providers, health insurers, and their employees cause more breaches than hacking, malware, and ransomware attacks.

“53% of all breaches were found to have originated from inside healthcare organizations.” “One quarter of all the cases were caused by unauthorized access or disclosure – more than twice the amount that were caused by external hackers,”

---

**Most Common Security Weaknesses in Healthcare Identified**
HIPAA Journal – December 28, 2018

The analysis revealed almost 37% of high and critical risks were in three areas:
- User authentication
- Endpoint leakage
- Excessive user permissions

The cybersecurity best practice of limiting the use of admin accounts and restricting the systems and data that end users can access was often not adopted by healthcare organizations.

The failure to restrict access to drives and networks not required by users to perform their work duties increases risk. By restricting user permissions, if credentials are compromised, the damage that can be caused will be restricted. Healthcare organizations should adopt the principle of least privilege and should only give users access to data and networks that they require to perform their work duties.
Who has rightful access to and who is looking at confidential patient data?

“Brooklyn Emergency Room Worker Accused of Stealing and Selling Patients’ PHI”

“Healthcare Worker Charged with Criminally Violating HIPAA Rules”

“Medical U of South Carolina fired 13 employees for 'snooping' in patients' medical records in 2017”

Palisades Medical Center in New Jersey suspended 27 workers without pay for a month for looking at the medical records of actor George Clooney, who had been treated there after a motorcycle accident.
Who has rightful access to and who is looking at confidential patient data?

UCLA Medical Center took steps to fire at least 13 employees and suspended at least six others for snooping in the medical records of pop star Britney Spears during her hospitalization in its psychiatric unit. In addition, six physicians faced discipline.

Who has rightful access to and who is looking at confidential patient data?

Ronald Reagan UCLA Medical Center was fined $95,000 by the California Department of Public Health for failing to stop employees from accessing singer Michael Jackson's records. Two hospital workers and two contract employees were terminated.
UCLA Health System agreed to pay $865,000 to the federal government to resolve allegations that its employees violated federal patient privacy laws by snooping in the medical records of two celebrity patients. Separately, in January 2010, a former UCLA employee pleaded guilty to four counts of illegally reading medical records, mostly from celebrities and other high-profile patients, and was sentenced to four months in federal prison.

Five workers and a student research assistant were fired for inappropriately accessing records at Cedars-Sinai Medical Center in Los Angeles. One of those was reportedly reality TV star Kim Kardashian, who gave birth to her daughter at the hospital the prior month.
“Dozens’ of Northwestern Memorial Hospital Employees Fired for Accessing Jussie Smollett’s Medical Records”

After Smollett was treated at Northwestern Memorial Hospital, curiosity got the better of some employees who searched for Smollett on the hospital’s system, some of whom accessed his chart and viewed his medical records.

Some employees that were terminated have spoken to the media about the incident. CBS Chicago claims dozens of hospital employees have been terminated for the HIPAA violations. NBC Chicago has also reported there have been at least 50 terminations for snooping.

MOBILE DEVICE CONTROLS
Mobile Device Controls

In the Security Risk Analysis, you’ll find the following questions:

• Does a list of ‘accepted mobile devices’ (e.g., smart phones, cell phones) exist based on testing?
• Is sensitive information transferred to external recipients?
• Have formal acceptable use rules been established for assets? Example assets include data assets, computer equipment, communications equipment, etc.

Mobile Device Controls

Mobile Devices and Protected Health Information (PHI)

The use of mobile devices in the workplace can be convenient and productive, but organizations should realize the risks associated with increased usage of mobile devices – especially when mobile devices are used to create, receive, maintain or transmit electronic PHI (ePHI). Entities regulated by the HIPAA Privacy, Security, and Breach Notification Rules (the HIPAA Rules) must be sure to include mobile devices in their enterprise-wide risk analysis and take action(s) to reduce risks identified with the use of mobile devices to a reasonable and appropriate level.
OCR Draws Attention to HIPAA Patch Management Requirements

Patch Management: A Major Challenge for Healthcare Organizations

To ensure patches can be applied, it is essential for IT teams to have a complete inventory of all systems, devices, operating systems, firmware, and software installed throughout the organization. Regular scans should also be conducted to identify unauthorized software.

Employee Mistakes and System Errors are a Larger Threat to Data Security than Hackers or Insiders

With the proliferation of both IoT devices in general and in the workplace, as well as the ubiquity of employee-owned devices in workplaces and BYOD policies, IT departments are being made responsible for ensuring the security of these devices.
Mobile Device Controls

RDP Backdoors Cost Just $10 on Dark Web: How to Avoid Getting Hacked
Healthcare IT News – July 25, 2018

Over the last six months, brute force attacks on Remote Desktop Protocols have become a common headline. Consider the cases of LabCorp, the city of Atlanta, multiple health systems, Colorado Department of Transportation and others.

Most recently, in fact, Cass Regional Medical Center’s EHR went down for a week after a brute force attack on its RDP.

What’s worse is that a recent report from McAfee found that RDP backdoors are being sold on the dark web for just $10.

RDP is a common function used to allow remote access into a network, often by third-party vendors and the like. The function is commonly installed standard with Windows, and once a party logs in, that computer can be used or controlled remotely by a legitimate party -- or a hacker.

So how can an organization remain in control? If you don’t need it, don’t enable it.
Social Media Challenges

In the Security Risk Analysis, you’ll find these questions:

• Have formal acceptable use rules been established for assets? Example assets include data assets, computer equipment, communications equipment, etc.

• Have policies been communicated to your employees? Are periodic security reminders provided?

• Is there a standard approach for protecting network devices to prevent unauthorized access/ network related attacks and data-theft?

• Are systems and networks monitored for security events?
Social Media Challenges

Limitations on the use of company devices

• **NO** personal emails on company computers
• **NO** Social websites on company computers
• **NO** shopping or surfing the web on company computers
• **NO** personal devices plugged into company computers – including charging of phones

You are required to know EVERY place where PII could possibly be.  
**IT MUST BE ENCRYPTED AT REST!**

MALVERTISEMENTS

Homeland Security Issues Ransomware Alert for Networked Systems  
April 4, 2016

DHS issued a ransomware alert in conjunction with the Canadian Cyber Incident Response Centre to warn individuals and organizations.

The US Department of Homeland Security issued a ransomware alert through the US Computer Emergency Readiness Team (US-CERT) to organizations that use networked systems, warning them of the potential dangers stemming from this type of malware.

“Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading,” the alert states. “Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed **without the user’s knowledge.**”
Social Media Challenges

Investigation Launched Over Snapchat Photo Sharing at M. M. Ewing Continuing Care Center - HIPAA Journal – July 19, 2018

Certain employees of a Canandaigua, NY nursing home have been using their smartphones to take photographs and videos of at least one resident and have shared those images and videos with others on Snapchat – a violation of HIPAA and serious violation of patient privacy.

An investigation into the sharing of images of abuse of nursing home residents was launched by ProPublica in 2015. The investigation revealed the practice was commonplace, with several nursing home employees discovered to have performed similar acts. The investigation revealed there had been 22 cases of photo sharing on Snapchat and other social media platforms and 35 cases in total since 2012.

More recently, a nursing assistant at the Parkside Manor assisted-living facility in Kenosha, WI, was discovered to have taken photos of an Alzheimer’s patient and posted the images of SnapChat. When the violation was discovered, the nursing assistant was fired for the HIPAA breach.

Texas Nurse Fired for Social Media HIPAA Violation - HIPAA Journal – September 13, 2018

A nurse at a Texas children’s hospital has been fired for violating Health Insurance Portability and Accountability Act (HIPAA) Rules by posting protected health information on a social media website.

The pediatric ICU/ER nurse worked at Texas Children’s Hospital and posted a series of comments on Facebook about a rare case of measles at the hospital. While the nurse did not post the child’s name on Facebook, her job was listed on her profile along with the hospital where she worked, and information about the boy and his condition.

However, as this incident shows, the patient does not need to be mentioned by name in order for them to potentially be identified. If any personally identifiable protected health information is posted on social media without consent first being obtained from the patient, it constitutes a violation of the HIPAA Privacy Rule.
Social Media Challenges

**NEVER RESPOND TO COMMENTS ON ANY SOCIAL MEDIA SITES!!**

Facebook  
Twitter  
YouTube  
Tumblr  
Pinterest  
Skype  
LinkedIn  
Instagram

**TECHNICAL TRAINING THAT ISN’T ALWAYS TECHNICAL**

- REGULATIONS  
- LAWS  
- STANDARDS  
- CONTROL  
- RISK  
- POLICY  
- GOVERNANCE  
- STRATEGY  
- SECURITY  
- PRACTICES  
- RULES  
- HIPAA  
- POLICY & PROCEDURES MANUAL
Technical training isn’t always technical

In the Security Risk Analysis, you’ll find this question:

Have your employees been provided formal information security training?

Administrative
Physical
Technical

Let me show you a sort of silly comparison.

Technical training isn’t always technical

You know what an appendectomy is but . . . Could you perform one?
Technical training isn’t always technical

It’s the same way with technology! You understand what a network is but could you put one together that is secure?

But there are some things you need to be aware of.

Technical training isn’t always technical

The single most important piece of hardware you can possess is a PROPERLY INSTALLED AND CONFIGURED FIREWALL.
Vulnerabilities in Fax Machines Can Be Exploited to Gain Network Access and Exfiltrate Sensitive Data

“. . . research was mainly focused on HP’s OfficeJet Pro all-in-one fax printers, although the same flaws exist in many other manufacturers’ fax machines including those manufactured by Epson and Canon. HP was alerted to the issue, which has now been patched, although other manufacturers’ devices remain vulnerable. In many cases, software on the all-in-one-printers cannot be updated. Correcting the flaw will only be possible by upgrading to newer devices.”

The study suggests all businesses that still use fax machines, including healthcare organizations, should determine whether their fax machines are capable of being updated and ensure all software is kept up to date. If updates are not possible, upgrading the devices is recommended and the printer-fax machines should be located on secure networks separate from those on which protected health information is stored.
Technical training isn’t always technical

HIPAA §164.308 Administrative safeguards

(A) Risk analysis (Required)
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Technical training isn’t always technical

Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients’ protected health information – May 6, 2019

OCR’s investigation further found that Touchstone failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its electronic PHI (ePHI), and failed to have business associate agreements in place with its vendors, including their IT support vendor and a third-party data center provider as required by HIPAA.
Technical training isn’t always technical

HIPAA §164.308(4)(i)
(C) Access establishment and modification
Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

HIPAA §164.308(5)(i)
(C) Log-in monitoring
Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password Management
Procedures for creating, changing, and safeguarding passwords.

DO YOU SEE THE TERM “PASSWORDS” ANYWHERE IN HERE?
OCR has fined a Colorado hospital $111,400 for the failure to terminate a former employee’s access to a web-based scheduling calendar, which resulted in an impermissible disclosure of 557 patients’ ePHI.

Further, the web-based calendar used by PSMC had been provided by a company (Google) that had not signed a business associate agreement with PSMC.

Without a BAA in place, PSMC had not received satisfactory assurances that Google would safeguard the ePHI contained in the calendar.

Unless a signed BAA is obtained by a covered entity prior to using the service in connection with any ePHI, it constitutes a HIPAA violation.
“OCR Draws Attention to HIPAA Patch Management Requirements”

“70% of medical devices will be running unsupported Windows operating systems by January: report”  Fierce Healthcare – May 15, 2019

Microsoft support for devices running Windows 7, Windows 2008 or Windows mobile is planned to expire by January 14. Running unsupported operating systems poses a risk that may expose vulnerabilities and has the potential to impact regulatory compliance.

“Despite Microsoft Patch, Attacks Using WANNACRY Exploit on the Rise”  Health IT Security – May 21, 2019

“While Microsoft released a patch for this vulnerability long before WannaCry, nearly 1 million devices are still vulnerable to attack.”

“Report: 40% of Healthcare Organizations hit by WannCry in past six months”  Fierce Healthcare – May 21, 2019
“When it comes to healthcare cybersecurity, the costs of inaction can be staggering. Every second a device remains noncompliant extends the window of vulnerability and increases the risk factor – exposing healthcare organizations to significant patient safety, financial and business consequences.”

1. Technical training isn’t always technical
   Employees
2. Guidance on e-mail and text messaging
   Employees
3. Appropriate access for pertinent staff
   Employees
4. Mobile device controls
   Employees
5. Social media challenges
   Employees
QUESTIONS?