Welcome to PMI’s Webinar Presentation

Brought to you by:
Practice Management Institute®
pmiMD.com

Meet the Presenter…

On the topic:
Compliance Best Practices for Managing Cyber-related Risk

Larry Neiswender
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.
Larry Neiswender  
Founder and Managing Partner  
PROTECT EHR

- Microsoft Certified Systems Administrator  
- CompTIA Network + Certified  
- Practice Workflow and Health Information Technology Redesign Specialist

$2.5 Million Settlement  
Shows that Not Understanding HIPAA Requirements Creates Risk
Widespread HIPAA Vulnerabilities Result in $2.7 Million Settlement with Oregon Health and Science University

Stolen Laptop Bag Leads to $750,000 Fine for Oncology Group
Massachusetts HIPAA Case Outlines Series of Missteps
$230,000 in Penalties After Two Insider Breaches

$4.3 Million HIPAA Penalty for Three Breaches
M. D. Anderson Cancer Center Cited for Unencrypted Devices
OCR Fines Rhode Island Health System $400,000 Over Business Associates Agreements

Latest $2.5 Million HIPAA Settlement Warning to Health Plans,

Providers: Get HIPAA Compliant
270,000 Patients Potentially Affected by Med Associates Hacking Incident
Banner Health Contacts

3.7 Million People in Wake of Cyber Attack Discovery

14 Month Data Breach Discovered During a Ransomware Investigation: 300,000 Patients Impacted
Ransomware Attack on Dermatology Office Breaches More than 13,000 Patient Records

538,000 Patients Notified of LifeBridge Health Data Breach
Report: Facebook App Exposed
3 Million More Users' Data

Equifax: US Breached Victim Tally Stands at 146.6 Million
COMPLIANCE BEST PRACTICES FOR MANAGING CYBER-RELATED RISKS
10 Steps for Thwarting EHR Hackers

“It's bad enough that the number of security breaches of patient protected health information appears to be skyrocketing. But it feels downright creepy when the breach is at the hands of a hacker, as was the recent attack by Eastern European hackers that breached almost 800,000 Medicaid recipients in Utah.”

May 31, 2012

“OCR: Healthcare Organizations Unaware of Privacy Regulations”

APRIL 26, 2013
“Study Reveals Healthcare Industry Employees Struggling to Understand Data Security Risks”

“The recently published Beyond the Phish Report . . . has revealed healthcare employees have a lack of understanding of common security threats.”

“Overall, the healthcare industry performed second worst for security awareness, just ahead of the hospitality industry, with the survey highlighting several areas of weakness that could potentially be exploited by cybercriminals to gain access to healthcare networks and sensitive data.”

April 30, 2018

“Why the Anthem Data Breach Won’t be the Industry’s Wake-up Call”

February 11, 2015

Yes, it's the largest known security breach in the healthcare industry, but it's hardly the first. There are a lot of them, and the number of incidents keep rising. According to the Identity Theft Resource Center’s latest data breach report, released in January, data breaches are at an all-time high, the healthcare industry suffered the highest proportion of data breaches and the No. 1 cause of security breaches in 2014 overall was due to hacking.

This, despite the fact that the FBI warned the healthcare industry about cyberattacks a year ago.

So why does it keep on occurring, and why won't Anthem's security breach quell the tide?

For one, many healthcare entities still don't take security as seriously as they should, even though HIPAA has been around for almost 20 years.

Just look at this study of more than 1,000 physician practices published by NueMD last month. It found that 23 percent of them didn't even have a HIPAA compliance plan, only one third had performed a security risk assessment of their electronic patient protected health information, even though both HIPAA’s security rule and the Meaningful Use program require it; and 36 percent didn't know that the HITECH Act of 2009 imposed new compliance obligations on them.
Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people.

After filing their breach report, Anthem discovered cyber-attackers had infiltrated their system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email.

...the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.
In addition to the impermissible disclosure of ePHI, OCR’s investigation revealed that Anthem failed to conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2014.

“More Than Half of Hospitals Hit with Ransomware in Last 12 Months” 4/7/16

Healthcare Attorneys Call Cybersecurity a Growing Concern 10-13-16

Overlooking Risks Leads to Breach, $400,000 Settlement 4-12-17

Ransomware Attack Reported by Dallas Senior Living Community 5-16-17
4-Month Data Breach Discovered During Ransomware Investigation – 300,000 Patients Impacted 7-26-17

Proposed Senate Bill Would Fine, Jail Execs Who Conceal Data Breaches 12-1-17

Cybercriminals Turning to Smaller Providers and Health IoT in 2018 1-8-2018

More Than 60% of Healthcare Orgs Saw Cyberattack in Past Year, Survey Finds 3-14-18

Insider Data Breaches Continue to Plague the Healthcare Industry 3-21-18

SamSam Hackers Hit Indiana’s Allied Physicians of Michiana 5-22-18

LabCorp Goes Down After Network Breach, Putting Millions of Patient Records at Risk 7-17-18

SamSam Ransomware Hackers Bank $6 Million and Counting from Victims 8-3-18
Insider Data Breaches Continue to Plague the Healthcare Industry 3-21-18

SamSam Hackers Hit Indiana’s Allied Physicians of Michiana 5-22-18

LabCorp Goes Down After Network Breach, Putting Millions of Patient Records at Risk 7-17-18

SamSam Ransomware Hackers Bank $6 Million and Counting from Victims 8-3-18

THERE ARE MULTIPLE POTENTIAL PROBLEMS AND THEY'RE COMING FROM EVERYWHERE!
THERE ARE MULTIPLE POTENTIAL PROBLEMS AND THEY’RE COMING FROM EVERYWHERE!

Hacking
Ransomware
Phishing (email) campaigns
Third-party Entities
  • Cloud Services
  • Websites
Cryptomining
Employees
best prac·tice  noun

plural noun: best practices

1. Commercial or professional procedures that are accepted or prescribed as being correct or most effective.

COMPLIANCE

In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws policies, and regulations.
Breach - A breach of protected health information ("PHI") is defined as the acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.
For a long time, the question existed as to whether or not ransomware was to be considered a breach of patient confidentiality.

In 2016, HHS put out a document called:

**FACT SHEET: Ransomware and HiPAA**

And this question was asked and answered:

**Question:** Is it a HIPAA breach if ransomware infects a covered entity’s or business associate’s computer system?

**Here was their answer:**

“**When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, . . .**

a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.”
Unsecured Protected Health Information

Means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

Notification obligation only applies to “Unsecured PHI”

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals.
- Acceptable methods of securing PHI are encryption and destruction.
- Loss or compromise of PHI that has been encrypted or properly destroyed does not trigger the duty to notify or report.
“When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, . . . 

a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.”

“$475,000 fine marks first HIPAA enforcement action over breach notification timing”

From Healthcare Dive - January 10, 2017

“Presence Health reported on January 31, 2014, that paper records containing the PHI of 836 individuals were missing. The problem is that the breach had been discovered on October 22, 2013, over three months earlier.”

“While there have been some headline-grabbing sanctions for large data breaches over the years, this is the first sanction based solely on a delay in reporting a breach.”
If a breach occurs, but you **cannot confirm** that the data was acquired, accessed, used or disclosed . . .

*is it a reportable breach?*

What if data is **NOT encrypted** but simply locked up to the point where a practice can’t get to it?

*is it a reportable breach?*
“When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, . . .

a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.”

IBM: 70% of Businesses Paid Cybercriminals to Unlock Ransomware  Dec 15, 2016

Ransomware has grown in popularity over the past two years and 2016 has seen record numbers of attacks on businesses.

Cybercriminals see ransomware as an easy way to make money. Rather than having to infiltrate a system, steal data, and sell those data on the black market – a process that can take months before payment is received – a ransomware infection usually results in quick payment of funds. Payments are typically received within 7 days of infection.
An important distinction in the world of cybercrime begins to happen at this point.

*From the Institute for Critical Infrastructure Technology comes this interesting observation:*

“Ransomware cyber-criminals are unique. Different from other types of criminals who attempt to exfiltrate or manipulate data where it is stored, processed, or in transmission, ransomware criminals only attempt to prevent access to the data.”

“Hackers, in general, worry about what they can steal. Ransomware criminals concern themselves with what they can disrupt.”

---

**THIRD-PARTY ENTITIES**

**EMR PROVIDERS**

**BUSINESS ASSOCIATES**

- BILLING COMPANIES OR CLEARING HOUSES
- CLOUD PLATFORMS
- WEBSITES
EMR PROVIDERS

Greenway Health Ransomware Attack Stops 400 Clients from Accessing EHR’s

It is unclear whether the ransomware infection resulted in, EHR data being encrypted although clients were temporarily prevented from accessing the cloud-based intergy EHR / medical management platform.

Greenway Health has not announced which Ransomware variant was involved, how the ransomware was installed on its system, and whether all data were recovered from backups or if the ransom demand was paid.

EMR PROVIDERS

Allscripts Recovering from Ransomware Attack That has Kept Key Tools Offline

The ransomware attack started on Thursday, January 18 at around 02:00 a.m. EST, and by 06:00 a.m. EST was a full blown ransomware incident, which required that incident response teams from Microsoft and Cisco be called in to assist. The Allscripts outage impacted approximately 1500 small physician practices who were left without access to their EHR or claims submission applications.
Before cloud services can be used by healthcare organizations for storing or processing protected health information (PHI) or for creating web-based applications that collect, store, maintain, or transmit PHI, covered entities must ensure the services are secure.

Even when a cloud computing platform provider has HIPAA certification, or claims their service is HIPAA-compliant or supports HIPAA compliance, the platform cannot be used in conjunction with ePHI until a risk analysis – See 45 CFR § 164.308(a)(1)(ii)(A) – has been performed.

A risk analysis is an essential element of HIPAA compliance for cloud computing platforms. After performing a risk analysis, a covered entity must establish risk management policies in relation to the service – 45 CFR § 164.308(a)(1)(ii)(B). Any risks identified must be managed and reduced to a reasonable and appropriate level.

A HIPAA Business Associate is any person or entity who performs functions on behalf of a covered entity, or offers services to a covered entity that involve access being provided to protected health information (PHI).

The HIPAA definition of Business Associate was modified by the HIPAA Omnibus Rule to include any entity that “creates, receives, maintains, or transmits” PHI. The latter two clearly apply to providers of cloud computing platforms.
Penalties for Cloud-Related HIPAA Violations

The Department of Health and Human Services’ Office for Civil Rights has already settled cases with HIPAA-covered entities that have failed to obtain Business Associate Agreements before uploading PHI to the cloud, as well as for risk analysis and risk management failures.

St. Elizabeth’s Medical Center in Brighton, Mass agreed to settle its case with OCR in 2015 for $218,400 for potential violations of the HIPAA Security Rule after PHI was uploaded to a document sharing service, without first assessing the risks of using that service.

Phoenix Cardiac Surgery also agreed to settle a case with OCR for failing to obtain a Business Associate Agreement from a vendor of an Internet-based calendar and email service prior to using the service in conjunction with PHI. The case was settled for $100,000.

In 2016, OCR settled a case with Oregon Health & Science University for $2.7 million after it was discovered ePHI was being stored in the cloud without first obtaining a HIPAA-compliant Business Associate Agreement.
WEBSITES
Malware Installed on Florida Hospital Websites May Have Provided Access to PHI
The HIPAA Journal May 3, 2018

Three websites used by Florida Hospital have been infected with malware that has potentially allowed the threat actors behind the attack to obtain patients’ protected health information.

PHI access has not been confirmed and no reports have been received to suggest any protected health information has been misused. Patients are being informed of the breach and, out of an abundance of caution, have been offered complimentary credit monitoring services.

MALVERTISEMENTS

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.”
CRYPTO-CURRENCY MINERS

This can be defined as the malicious use of (YOUR) infected system resources in order to mine (create) cryptocurrency. This is also known in the security world as drive-by mining.

So, what is Crypto-Currency Mining?

CRYPTO-CURRENCY MINERS

The simplest explanation is to say that this is how bitcoins and other cyber-currencies are generated.

This basically means that bad actors will use any means necessary to get into your system for the purpose of using your computing power to complete difficult mathematical computations that will win them cyber-currencies such as bitcoins.
Tennessee Hospital’s EHR Hacked by Cryptocurrency Mining Software
February 8, 2018

Parsons, Tennessee-based Decatur County General Hospital is notifying 24,000 patients of a breach, stemming from a hacker remotely installing software onto its electronic health record software to generate digital currency.

The infected server contained patient names, Social Security numbers, addresses, dates of birth, clinical data and insurance information.

While it appears the hackers’ intent was to leverage the cryptocurrency software, the investigation was unable to definitively prove hackers didn’t view or access patient data. All impacted patients are being offered one year of free credit monitoring.
Cryptojacking Displaces Ransomware as Top Malware Threat

New coin mining malware jumped an astronomical 1189% in the first three months of this year compared with the last three months of 2017, surging from 400,000 to 2.9 million detected pieces of malware.

What if data is **NOT** encrypted but simply locked up to the point where a practice can’t get to it?

*is it a reportable breach?*
A New Strain of Ransomware Targets Healthcare; Cyberattack Causes Disruptions at NHS Hospital

Cybersecurity analysts have uncovered a previously undocumented strain of ransomware aimed at the healthcare industry and spread through targeted phishing emails that contain a malicious attachment.

Wannacry is a ransomware worm that spread rapidly through OVER 300,000 computers in over 150 countries in May 2017.

$300 per computer

A New Strain of Ransomware Called Petya

Petya was discovered in March 2016, and was immediately flagged as the next step in Ransomware evolution.

Petya is a family of ransomware that infects the master boot record and prevents the computer from booting.

NOTPETYA was a later version that purported to be ransomware however, this variant was modified so that it is unable to actually revert its own changes.
HOW DO WE PROTECT OURSELVES FROM ALL OF THESE POSSIBILITIES?

TAKE STEPS TO LEARN WHAT IS GOING ON IN THIS INDUSTRY AND WHAT IS HAPPENING AROUND YOU.

FOR EXAMPLE . . .
Business Email Compromise Attacks Dominate 2017 FBI Internet Crime Report

The FBI has released its 2017 Internet crime report.

In 2017, there were 301,580 complaints made to IC3 about Internet crime, with 25,344 reports of phishing incidents resulting in losses of $29,703,000. However phishing likely played a part in many other categories of crimes such as credit card fraud and corporate and personal data breaches.

1.13 Million Patient Records Exposed in Q1, 2018

The latest Breach Barometer report shows the records of 1,129,744 patients and health plan members has been viewed by unauthorized individuals, exposed, or stolen in the first quarter of 2018. Data breaches occurred at a rate of more than one per day, with 110 healthcare data breaches reported in Q1.

142 healthcare data breaches in Q2, 30% caused by repeat offenders

More than 3 million patient records were breached between April and June, highlighting an even bigger issue: risk increases over time without proper education or reporting.

The healthcare sector suffered 142 healthcare data breaches from April through June, nearly 3 times the number reported in the first part of the year.

What’s worse is that about 30% of those breaches were caused by repeat offenders from within the same organizations.
Protenus Report highlights extent of insider breaches in healthcare

The quarterly breach barometer report from Protenus provides insights into the extent to which insiders are violating HIPAA Rules and snooping on patient health information.

Insider breaches are a major problem in healthcare, yet many insider breaches go undetected. When insider breaches are identified, it is often months after the breach has occurred. One healthcare employee was recently discovered to have been accessing medical records without authorization for 14 years.

BEST PRACTICES FOR MANAGING CYBER-RELATED RISKS

HAVE A SECURITY RISK ANALYSIS PERFORMED ANNUALLY
What is HIPAA certification?  

March 6, 2018

Many vendors would like HIPAA certification to confirm they are fully compliant with HIPAA rules and understand all aspects of the health insurance portability and accountability act (HIPAA), but is it possible to obtain HIPAA certification to confirm HIPAA compliance?

Many companies claim they have been certified as HIPAA compliant or in some cases, that they are ‘HIPAA certified’. However, ‘HIPAA certified’ is a misnomer. There is no official, legally recognized HIPAA compliance certification process or accreditation.

---

BEST PRACTICES FOR MANAGING CYBER-RELATED RISKS

HAVE A SECURITY RISK ANALYSIS PERFORMED ANNUALLY

HAVE DOCUMENTED POLICIES AND PROCEDURES THAT COVER –
  THE HIPAA PRIVACY RULE
  THE HIPAA SECURITY RULE
  CODING AND BILLING COMPLIANCE

INVEST IN EMPLOYEE TRAINING THAT INCLUDES –
  HIPAA
  (TEXAS HOUSE BILL 300)
  HOW TO RECOGNIZE PHISHING CAMPAIGNS
IF YOU DON’T HAVE AN ACTUAL FIREWALL – GET ONE!

DO NOT BELIEVE THAT THE DEVICE PUT IN BY YOUR INTERNET SERVICE PROVIDER WILL PROTECT YOU FROM ANYTHING!

BEST PRACTICES FOR MANAGING CYBER-RELATED RISKS

INVEST IN ACTUAL CYBER INSURANCE

Cybersecurity Insurance: How Underwriting is Changing

Cybersecurity insurers, faced with growing demand, are looking for new ways to better measure their risks. So some are moving toward more carefully scrutinizing the cybersecurity postures of their potential clients.

The common underwriting practice, has been for insurers to use "pen-and-paper questionnaires where they would ask various questions about how those companies protect themselves, and then they would blindly trust the answers the companies provided."

Now, some insurers are taking a different approach.

"Insurance companies started discovering as the breaches continued to intensify that they were sitting on billions of dollars of [potential] exposure.... It's very much like the mortgage meltdown crisis where they have no idea of the risk that they could bear. So insurance companies are beginning to think about objective ways to measure cybersecurity."
Actual questions from just one application for coverage

“The following items must be included with your application:”

“Copies of written network and privacy policies”

“Do you have a compliance program in place for both HIPAA and billing errors?”

“Do you have a written network security and privacy policy?”

“Do all employees with access to computer systems receive training in computer-system security issues and procedures?”

Actual questions from just one application for coverage

“The following items must be included with your application:”

“Do you have network security policies and procedures that include:

- “Antivirus software and protection for all computers?”
- “Firewalls for all internet access points?”
- “A software-update process, including installation of security-related software patches, on a regular basis?”

Practice Management Institute
www.pmiMD.com
Webinar/Audio Conference
November 1, 2018
Actual questions from just one application for coverage

“The following items must be included with your application:"

“Do you encrypt data that contains Protected Health Information stored on laptop computers, smartphones and similar devices, and portable media such as thumb drives and backup tapes?”

IS CYBER-COMPLIANCE A TERM WE MAY SOON HEAR?

IF SO, HOW CAN WE PREPARE?
BEST PRACTICES FOR MANAGING CYBER-RELATED RISKS

1. SECURITY RISK ANALYSIS – REQUIRED BY HIPAA SECURITY RULE

2. DOCUMENTED POLICIES AND PROCEDURES – REQUIRED BY HIPAA PRIVACY AND SECURITY RULES

3. DOCUMENTED OFFICE, CODING AND BILLING COMPLIANCE POLICIES

4. EMPLOYEE TRAINING – REQUIRED BY HIPAA PRIVACY AND SECURITY RULES

5. OBTAIN AN ACTUAL FIREWALL – NOT SOMETHING INSTALLED BY YOUR ISP

6. HAVE YOUR IT COMPANY OR DEPARTMENT INSTALL SHARE FILES WHERE ALL “MY DOCUMENT” FOLDERS ARE SAVED TO – NOT ON THE INDIVIDUAL COMPUTERS OF ANY KIND

7. BACK UP ALL IMPORTANT DOCUMENTATION – NOT JUST PATIENT RECORDS AND HAVE A REMOTE “AIR-GAPPED” BACKUP

8. DO THE ACTUAL BUY-UP OF CYBER-INSURANCE. DON’T BELIEVE THAT THE AMOUNT OF COVERAGE IN YOUR MEDICAL MAL-PRACTICE POLICY IS ANYWHERE NEAR ENOUGH
“The adage is true that the [YOUR] security systems have to win every time.”

“The attacker only has to win once.”
Dustin Dykes, CISSP

“There are two kinds of companies today. Those that have experienced a security breach and those that don’t know it yet.”

Howard Shrobe, Director
Cybersecurity, MIT – Computer Science and Artificial Intelligence Laboratory
Thank You!

Protect EHR, LLC
P. O. Box 820611
North Richland Hills, TX  76182
817-999-0595
Email: info@protectehr.com