Welcome to PMI's Webinar Presentation

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

Meet the Presenter…

On the topic:
HIPAA Compliance:
What to learn from the mistakes of others

Larry Neiwender
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.
HIPAA Compliance: What to learn from the mistakes of others

Presented by:
Larry Neiswender
Founder and Managing Partner
PROTECT EHR

Triple–S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement
Stolen Laptop Bag Leads to $750,000 Fine for Oncology Group

Medical Research Institute to Pay $3.9 Million in HIPAA Settlement
Business Associates Failure to Safeguard Nursing Home Residents PHI Leads to $650,000 HIPAA Settlement

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

Advocate Healthcare Settles Potential HIPAA Penalties for $5.55 Million
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
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

Healthcare Organizations at Much Higher Risk of Ransomware Attack than Financial Institutions
Ransomware Attack on Dermatology Office Breaches More than 13,000 Patient Records

270,000 Patients Potentially Affected by Med Associates Hacking Incident

Report: Facebook App Exposed 3 Million More Users' Data
270,000 Patients Potentially Affected by Med Associates Hacking Incident

Lack of Ransomware Protections Could Violate FTC Act
Business Email Compromise Attacks Dominate 2017 FBI Internet Crime Report
New File-less Code Injecting Ransomware Bypasses Antivirus

Hackers Hide Cyber Attacks in Social Media Posts
Malware Installed on Florida Hospital Websites May Have Provided Access to PHI
Unencrypted Portable Devices are a HIPAA Breach Waiting to Happen

HIPAA COMPLIANCE
WHAT TO LEARN FROM THE MISTAKES OF OTHERS
“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.”

Marla Durbin Hirsch

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

WHAT CAUSED THESE ENTITIES TO GET IN THESE PRECARIOUS POSITIONS IN THE FIRST PLACE?

WHAT COULD THEY HAVE DONE TO PREVENT THESE CIRCUMSTANCES?
A 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.

A breach can take many forms. Some can be a simple mistake

“Protected Health Information Sent to Incorrect Fax Recipient Over Several Months”
June 27, 2018

“Faxes containing the protected health information (PHI) of a patient have been sent to an incorrect recipient by OhioHealth’s Grant Medical Center over a period of several months – a violation of patient privacy and the Health Insurance Portability and Accountability Act (HIPAA).”
Other breaches are obviously intentional

“Protenus Report Highlights Extent of Insider Breaches in Healthcare”
May 4, 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.”

And we’re seeing more frequently, breaches aren’t limited to medical practices.

“HHS Imposes $100,000 Fine on Shuttered Facility for 2015 HIPAA Violation”
February 14, 2018

HHS' Office For Civil Rights is setting a precedent that it doesn't take HIPAA violations lightly by imposing a $100,000 fine on Filefax, a now-closed medical records management company, for a breach that occurred in 2015.

An OCR investigation confirmed an unauthorized individual left the medical records of roughly 2,150 patients at the shredding and recycling facility, unsecured. Those documents contained patients' protected health information.
And we’re seeing more frequently, breaches aren’t limited to medical practices.

“Equifax: US Breach Victim Tally Stands at 146.6 Million”
May 8, 2018

“Equifax said on Friday that in response to requests for additional information, it’s shared more breach details with several U.S. Congressional committees. Notably, the data broker said that its breach investigators found that consumers had uploaded images of various government-issued identity documents that were exposed in the attack, including 38,000 driver’s licenses, 12,000 Social Security or taxpayer ID cards, and 3,200 passports.”

And we’re seeing more frequently, breaches aren’t limited to medical practices.

“ER Staffing Firm Breach Raises Complex Questions”
May 10, 2018

“On Tuesday, USACS Management Group Ltd., reported to the Department of Health and Human Services a hacking / IT incident involving email and impacting 15,552 patients, according to HHS’ Office for Civil Rights HIPAA Breach Report Tool website.”

“The incident is listed on the HHS site as involving a business associate. Canton, Ohio-based USACS provides emergency medicine management and other services to about 210 hospitals in 22 states. That includes staffing hospital emergency departments with doctors, nurse practitioners and physician assistants.”
HHS – “WALL OF SHAME”

ENTITIES CURRENTLY UNDER INVESTIGATION

INVOLVING 500 OR MORE PATIENT RECORDS

NAME OF THE COVERED ENTITY

STATE

CE TYPE

NUMBER OF INDIVIDUALS AFFECTED

TYPE OF BREACH

LOCATION OF BREACHED INFORMATION (EMR – paper 
/ film – Network server – laptop – desktop computer

HOW DID THIS HAPPEN?

WHAT DID THEY FAIL TO DO?

We went back to the beginning to define what a breach is . . .

We’ve identified that a breach can happen to almost anyone . . .

Maybe it would be beneficial to see how just one kind of breach started
WHERE DID RANSOMWARE COME FROM?

JOSEPH POPP

100’s of people did it anyway!!!

RANSOMWARE ATTACK IMPACTS 6,500 JEMISON INTERNAL MEDICINE PATIENTS  FEBRUARY 23, 2018

“The investigation into the security breach revealed an unauthorized individual had gained access to Jemison Internal Medicine’s computer system and had access for a period of approximately three months.”
THE NUMBER ONE PROBLEM OCCURING IN MEDICAL OFFICES TODAY . . .

STARTED BEFORE THERE WAS HIPAA

STARTED BEFORE THERE WAS EMR SOFTWARE

STARTED BEFORE THERE WAS THE INTERNET

STARTED BEFORE THERE WAS MEANINGFUL USE OR MACRA

On June 20, 2016, Sylvia Burwell, Secretary of the Department of Health and Human Services released a inter-agency technical guidance document speaking exclusively about ransomware.

“Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015.”
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:

“Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.”

“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.”
In 2016 – almost every “Cyber” article that you saw involved the encrypting and stealing of data. That data was being sold on the dark web.

But by 2017, cybercriminals were getting lazy. Look at this article from December 2016.

**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.”

“. . . a breach has occurred because the e-PHI 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.”

HOW DO YOU PROVE THAT YOU DID NOT LOSE CONTROL OF DATA?
If a breach occurs, but you cannot confirm that the data was neither viewed nor copied, . . .

is it a reportable breach?

Valley Anesthesiology and Pain Consultants Reports
882,590 Record Data Breach Aug 16, 2016

The attacker succeeded in installing malware on the PC which took periodic screenshots and sent the images to a command and control center. The malware also recorded keystrokes entered on one of the Center’s computers.

While it was confirmed that an individual had gained access to a system containing PHI, no evidence was uncovered to suggest that PHI had actually been accessed or copied. However, it was not possible to rule out the possibility that sensitive data were viewed.
Medical Data Of 33,000 BJC Healthcare Patients Exposed Online For Eight Months  March 14, 2018

While the investigation didn’t find evidence of an unauthorized individual accessing the data, access couldn’t be ruled out with a high degree of certainty.

New York Surgery And Endoscopy Center Discovers 135,000 Record Data Breach  March 5, 2018

The rapid detection of the malware limited the time the hackers had access to the server and potentially prevented patients data from being viewed or copied. However, while no evidence of data access or data theft was discovered, it was not possible to rule either out with a high degree of certainty.

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.

Business Email Compromise Attacks Dominate 2017 FBI Internet Crime Report
June 29, 2018

Spate of Phishing Attacks on Healthcare Organizations Sees 90,000 Record Exposed
May 10, 2018

So far this year there have been three data breaches involving the hacking of email accounts that have exposed more than 30,000 records.
Class Action Lawsuit Claims UnityPoint Health Mislead Patients over Severity of Phishing Attack

May 8, 2018

As with many other healthcare data breaches, PHI was exposed as a result of employees falling for phishing emails.

UnityPoint Health told patients no reports had been received to suggest that their PHI had been accessed, stolen, or misused.

Ruling Reaffirms Individuals Cannot File HIPAA Lawsuits

June 22, 2018

“The ruling once again reaffirmed a longstanding precedent that individuals cannot file a lawsuit, known as a "private cause of action," for alleged HIPAA violations.”

Privacy attorney Kirk Nahra of the law firm Wiley Rein offers a similar assessment: "There has never been a HIPAA private cause of action, and that’s been clear since the early days. The fight now is over whether plaintiffs can use HIPAA as a measuring stick for some other kind of tort claim - although even then they still typically need to prove damages.”
“The plaintiffs allege Horizon BCBS willfully and negligently violated the Fair Credit Reporting Act (FCRA) – in addition to a number of state laws – by failing to adequately protect their personal information. The plaintiffs claim that the unauthorized transfer of personal information was a violation of FCRA and that the transfer, in itself, constitutes a cognizable injury.”

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

If you are any kind of medical facility, and regardless of size, recognize that you are just a viable a target to Cybercriminals as anyone else.

Recognize that information can get out of your control in ways you never thought about.

**Man's antenna picks up PHI from pagers at 5+ hospitals**

A Johnson County, Mo., man using an antenna to pick up TV channels on his laptop received unencrypted patient information from several local and distant hospitals . . . as well as some hospitals in Kentucky and Michigan.

According to the *Star*, the man — downloaded the software for free and purchased the antenna commonly used by radio or tech hobbyists for just $30.
AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

If you create, maintain, transmit or receive Personally Identifiable Information, you are required to:

Conduct a Security Risk Analysis

Possess documentation covering compliance – especially for any transaction that is related coding or billing for services AND policies and procedures covering the HIPAA Privacy and Security Rules.

Training that not only encompasses the HIPAA regulations but look for a company that also trains employees how NOT to fall for Phishing scams.

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

EMPLOYEES SHOULD NEVER

OPEN PERSONAL EMAILS ON COMPANY COMPUTERS
GO TO SOCIAL WEBSITES ON COMPANY COMPUTERS
DOWNLOAD ANYTHING INCLUDING SCREEN SAVERS
CONNECT ANY DEVICE TO A COMPANY COMPUTER – INCLUDING PHONES – NOT EVEN TO CHARGE OR LISTEN TO MUSIC
If you retain or maintain Personally Identifiable Information, that information must be encrypted.

$4.3 Million HIPAA Penalty for 3 Breaches

June 18, 2018

A lack of device encryption will cost a Texas-based cancer treatment center $4.3 million in civil monetary penalties from the Department of Health and Human Services.

In a statement Monday, the HHS Office for Civil Rights said it was granted a summary judgment by an HHS administrative law judge, who ruled that The University of Texas MD Anderson Cancer Center violated the HIPAA privacy and security rules. The judge approved OCR imposing $4.3 million in penalties in the aftermath of its investigations into three breaches involving unencrypted devices.

ONE LAST THING TO TRY TO DO

TO CORRECT ONE OF THE MOST DAMAGING MISCONCEPTIONS ABOUT HACKING AND RANSOMWARE
“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 CSAIL
Thank You!

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

Larry Neiswender
Founder and Managing Partner
PROTECT EHR

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