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.
Welcome to PMI’s Webinar Presentation

Meet the Presenter…

<table>
<thead>
<tr>
<th>Rose B. Moore</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMC, CMIS, CMOM, CMCO, CCP, PCS, CEC, CERT, CMA-opth</td>
</tr>
<tr>
<td>Faculty</td>
</tr>
<tr>
<td>Practice Management Institute</td>
</tr>
</tbody>
</table>

On the topic:

HIPAA Security Breaches: The Proactive Approach
HIPAA Security Breaches: The Proactive Approach

Presented by
Rose B. Moore
CMC, CMOM, CMIS, CMCO, CCS-P
Faculty, Practice Management Institute

HIPAA: Health Insurance Portability and Accountability Act

Hippocrates, physicians pledged to respect confidentiality in these words:
“What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.”
HIPAA

The World Medical Association’s Declaration of Geneva states:
“\text{I will respect the secrets which are confided in me, even after the patient has died.}”

HIPAA Breaches

Breach – unauthorized acquisition of data or access to data, risk of harm

It has been ten years since Congress has passed HIPAA. Since that time, healthcare organizations have worked tirelessly to maintain the privacy and security of patient health information. We have seen many approaches to HIPAA security from the non-compliant “wait and see” to the overly compliant “protect at all costs.”
“The number one priority of security is to know where the data is how it is accessed and how it flows through your organization.”

-Andrew Hicks
National Healthcare Practice Director, Coalfire

In the past, “security” meant keeping the paper charts filed under lock and key.
Now with electronic health records, we have easy access between healthcare providers, but there is also high risk of access from outside entities. Cyber-criminals are always on the attack to access personal information creating chaos for our patients, organizations, and associated entities.
HIPAA was designed and created to make sure that healthcare facilities, medical practices, and insurers keep patient information secured from unintended access, in addition to obtaining other data security goals. This is an ongoing commitment and can be very costly. How costly is up to the healthcare facility/practice.

HIPAA

Before the arrival of HIPAA, there were no formal privacy standards in place for protecting medical records. In addition to doctors and nurses, insurance companies, billing clerks, front desk receptionist, and other employees had access to patient records without any restrictions on what could be done with that information once it had been accessed.
Cyber Attacks…

…continue to be a serious threat.
Private sector business have experienced massive data breaches.
Maintaining privacy of patients’ healthcare records is one of the goals of HIPAA to solve, and its requirements have changed as technology has changed.

The more sophisticated the attacks, the more sophisticated approach to security, all while still providing an easily accessible and user-friendly system that can be used by a large team of employees.
To avoid data breaches and HIPAA penalties, IT experts have had to become acquainted with the issues of compliance and security, while understanding that equal effort must be devoted to each one.
Compliance vs. Security

Compliance and security are priorities for any organization. Both carry important distinctions and responsibilities. Please know that complying with HIPAA does not automatically guarantee a secure environment.

Policies and Procedures

HIPAA requires password policies to restrict access to sensitive data. Establishing security should be the first item of business since that will reduce threats of all kinds and then your HIPAA compliance can be built out from there.
IT

It is up to the organization’s IT specialists to enact a comprehensive strategy that protects all manner of data before implementing national standards including establishing encryption techniques. Encryption is a mandatory requirement under HIPAA. HIPAA’s security rule specifies that safeguards be in place to ensure the integrity and confidentiality of PHI.

Encryption

Full disk encryption (FDE) also known as whole disk encryption is often used on laptops since it is effective in the case of physical theft. FDEs are not recommended for servers or any device that is on most of the time. Logical (role-based) encryption is more effective when securing data that resides on always-running servers.

Encryption keys should always be stored in a separate location as the encrypted data without sacrificing convenience to the end user.
Certification

A trustworthy vendor will be able to deliver an encryption program that will work in a variety of settings through any transportation method and provide reliable security. A critical component to look for when it comes to encryption is certification, which will convey that a company is a professional and experienced one that can be a trusted partner for your organization.

Certification from the National Institute of Standards and Technology (NIST) named best practice.

Safe Harbor

Safe Harbor frees an organization from the obligation of announcing a breach as long as that organization can prove it has taken the appropriate steps to render that data “unusable, unreadable or indecipherable to unauthorized individuals,” according to HIPAA.
Business Associates

Business Associate is a person or organization that has access to patient records or handles patient data as part of its services.

A business associate often refers to a cloud storage provider that helps guide compliance efforts, but a business associate is any third-party vendor that supplies a product or service to a covered entity. They also must be held to the same HIPAA standards as the covered entity it works for.

HITRUST

HITRUST certification is the only way that you can say you are “HIPAA-certified.”

To achieve this certification, you must have far more controls in place than you do to satisfy the HIPAA requirement.
Security Breaches

Security breaches can also lead to HIPAA fines for not having an effective system in place to protect data.

Understanding how security and HIPAA overlap and where they separate from each other will help you to budget adequately.

Ignorance of the rules and laws is no excuse and can become a quick financial burden if not taken care of in the beginning.

Proactive Approach

Taking a proactive approach to security, including steps necessary to achieve Safe Harbor status, can greatly reduce the chance of having to face this kind of situation. A key factor in that approach is being able to reasonably assess the spectrum of risks that present for your organization and create a risk management plan for reducing them.
Risk Assessment

NO ONE IS IMMUNE FROM ATTACKS!
Your organization should perform a comprehensive risk assessment.
This is actually a security requirement – “knowing where the data is and how it is accessed, how it flows through your system.”
A huge part of your risk assessment will be the process of discovery. This is a partnership between your IT team and your practice to determine how your data is handled and accessed.

Risks

• External Attacks
• Employee Errors
• System Glitches
• Business Associates Errors
Proactive Tips

• Encourage a culture of security.
• Conduct a proper risk assessment.
• Encrypt your data the right way.
• Patch your system.
• Monitor your system.
• Get the right people in place and ensure they have the proper training.

Pay Attention to the Signs

• Don’t sacrifice security in favor of compliance.
• Don’t ignore potential vulnerabilities.
• Don’t wait for a breach to happen before you take action.
• Don’t consider security and compliance to be the same thing.
• Don’t assume a secure infrastructure will last forever.
• Don’t take on responsibilities without guidance.
Tips, Tools, and Techniques

• Create internal policies that help your staff understand the importance of security and the part each team member plays.
• Stay current with security updates and patches to keep up with threats and constantly evolve.
• Develop a plan that regularly identifies potential vulnerabilities in your attack surface.
• Prioritize security efforts and implement effective counter-measures to alleviate the risks.

Questions?

• Thank you for your attendance!
• Get your questions answered on PMI’s Discussion Forum:
  http://www.pmimd.com/pmiForums/rules.asp