Welcome to PMI’s Webinar Presentation

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

Meet the Presenter…

On the topic:
Looking at Security from 360 Degrees

Larry K. 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.
Looking at Security From 360 Degrees

Larry Neiswender  
Founder and Managing Partner  

• Microsoft Certified Systems Administrator  
• CompTIA Network Plus Certified  
• Practice Workflow and Health Information Technology Redesign Specialist  

• Worked with practices in the Meaningful Use program since 2011  

• Sub-contractor for the North Texas Regional Extension Center and the Dallas/Ft. Worth Hospital Council
Looking at Security From 360 Degrees

HIPAA ???

Microsoft Certified Systems Administrator
How would you define **SECURITY** in your office?

We use that anti-virus stuff
We change the locks on the doors when somebody leaves
We have an alarm system

(Does everybody have a different code to the alarm system?)

How would you define **SECURITY** in your office?

A lapse in security can be the most devastating thing to happen to medical practices in today’s environment.

In the event of some devastating incident such as a fire or storm,
The practice can repair the office,
The practice can buy new furniture but . . .

a practice cannot purchase anything to repair the reputational harm that comes from the violation of confidential patient information.
## STARTING FROM THE BEGINNING - PROPERLY

<table>
<thead>
<tr>
<th><strong>HIPAA PRIVACY RULE</strong></th>
<th><strong>HIPAA SECURITY RULE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STANDARDS</strong> for</td>
<td>Security <strong>STANDARDS</strong></td>
</tr>
<tr>
<td>Privacy of Individually</td>
<td>for the Protection of</td>
</tr>
<tr>
<td>Identifiable Health</td>
<td>Electronic Protected</td>
</tr>
<tr>
<td>Information</td>
<td>Health Information</td>
</tr>
</tbody>
</table>

What is Electronic Protected Health Information, (e-PHI)?

It’s Individually Identifiable Health Information . . . In an electronic format

*It’s not exclusive to just records held in Electronic Medical Record Software!*

---

### The preamble to the Security Rule

“The HIPAA Security Rule, 45 CFR Part 160 and subparts A and C of Part 164, applies only to protected health information in electronic form and requires covered entities to implement certain **administrative**, **physical** and **technical** safeguards to protect this electronic information.”

Here’s the key to that question, “How would you define security in YOUR environment?” and why the answers I get when I ask it are so revealing.

Practices are expected to develop safeguards in all three of those areas and that covers a lot more ground than most have ever thought about.
Why are STANDARDS so important?

“Security Rule Overview for Small Providers”
(Published by the Department of Health and Human Services)

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.”

The term “maintains” will have significance in just a moment but it has caused some confusion so, here are a couple definitions that will help to understand this term.

1. To keep in an existing state (as in repair, efficiency, or validity)
2. To preserve from failure or decline.

“MAINTAINS”
AN IMPORTANT AND CONFUSING TERM
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.”
Right from the beginning, there’s a problem.

Look at the last part of the required specification. “... and availability of electronic protected health information held by the covered entity.”

Doesn’t that sound a lot like that Standard that talked about e-PHI that the practice creates, transmits or maintains?

Today . . . trying to avoid some of the bureaucratic over-reach, some practices say, “My EMR is cloud-based so I’m not holding e-PHI. So, I shouldn’t have to have the Security Risk Analysis performed.”

Changing times does not mean changing responsibility

First off, when this rule was written, there were no cloud-based EMR’s so everybody was holding patient data. But go back to a statement in that document, “Security Rule Overview for Small Providers”.

Remember, it said, 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.”

Well, if you’re using an EMR, you’re definitely creating e-PHI . . .
If your EMR is now cloud-based, you’re definitely transmitting e-PHI . . . and, We’ve already talked about maintaining or holding are considered the same thing so anyway you choose to look at it, a Security Risk Analysis must be done.
The Security Risk Analysis Is Important

Notice that this statement doesn’t ask if you’re holding or maintaining e-PHI.

They don’t care which EMR you’re using.

They don’t care how many patients you have.

They want proof of a Security Risk Analysis.

---

<table>
<thead>
<tr>
<th>Security Risk Analysis</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>On every audit request from Figliozzi and Company</td>
<td>Security Risk Analysis is Important</td>
</tr>
</tbody>
</table>
While we’re clearing up misconceptions, let’s take on one more.

The vast majority of providers had never heard of the SRA until the Meaningful Use program was introduced making the SRA a mandatory reporting item but, because Meaningful Use was under CMS, and because Meaningful Use was voluntary, some practices made the assumption, “I don’t accept Medicare or Medicaid so I don’t have to do the SRA.”

FACT: If you utilize electronic medical records, you are REQUIRED to have the Security Risk Analysis performed whether you accept ANY kind of insurance or accept NO insurance.

PERFORMING THE SECURITY RISK ANALYSIS
(A simple 2-step process)

Q&A  (National Institute of Standards and Technology)
(57 questions)

“Scope of the Assessment: It is necessary to identify where e-PHI is created, received, maintained, processed, or transmitted.”

“Ensure that the risk assessment scope takes into consideration the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).”
PERFORMING THE SECURITY RISK ANALYSIS
(A simple 2-step process)

Inventory – (Create, Maintain, Transmit, Receive)

People and Processes: “Any asset(s) which processes, transmits or stores e-PHI. The assets may be used in an operational or administrative capacity, . . . As long as the asset usage impacts e-PHI usage, then it should be listed.“

“Examples could include devices such as Desktop PCs, Fax Machines, Photo Copiers, Scanners, Mobile Computing Devices, Cell Phones/Smart Phones, Storage Servers, Monitors, Phones, Pagers, Network Connections, Internet Routers, Printer(s), Teleconferencing Equipment, Dictaphones, Software, Medical Equipment, Specialized Medical Devices (such as X-Ray, EKG, or EEG) or Portable Storage devices such as Thumb Drives.”

Technology: “This would be a list that exclusively contains the software package(s) which process e-PHI.”

“This may be any computer program from specialized medical software to the Microsoft Office suite of products such as Excel, Word or Access. *Any software or computer program which processes, transmits or stores e-PHI would be categorized in this section.*”
LOOKING AT SECURITY FROM 360 DEGREES

Administrative

§164.316 The Policies and Procedures and Documentation Requirements

(a) Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart,

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(2) Implementation specifications:
   (i) Time limit (Required) Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. AND,

   (iii) Updates (Required) Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

The Employee Handbook does NOT meet this requirement.

Administrative Questions from the Security Risk Analysis

“Do you have documented information security policies and procedures?”
No Smoking in or around the practice
No personal phone calls on company phones
No sexual harassment
Paid Time Off
No public comments about the practice on social websites

Administrative Questions from the Security Risk Analysis

“Do you have documented information security policies and procedures?”

Advocate Health Care Network (Advocate) has agreed to a settlement with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), for multiple potential violations of the Health Insurance Portability and Accountability Act (HIPAA) involving electronic protected health information (ePHI).

“We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI is secure,” said OCR Director Jocelyn Samuels. “This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level.”

“OCR’s investigations into these incidents revealed that Advocate failed to:
• conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
• implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center;”

“Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million”
From the Department of Health and Human Services
Aug 4, 2016

“The combined breaches affected the ePHI of approximately 4 million individuals.”
In an interview a couple years ago, Mac McMillan was asked about the Security Analysis and other **required** documentation.

First, it was interesting that he singled out three requirements that he obviously feels are some of the most important.

Next, in comparing having these requirements successfully met by practices of different sizes, it was interesting to see his recognition of the toll some of the more prevalent requirements took on small practices.

“There are no good or easy answers,” explains McMillan. “The problem is that they have the same set of requirements that the big guys have. The only difference is the scope of them and how you would actually address some of them, **but they still have to do the basics.**

• They have to conduct that risk analysis.
• They still have to produce those policies and procedures, and,
• They still have to train their workforce.”

§164.310 Physical safeguards.

(b) **Standard:** Workstation use.

*Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*

Do you have something in place and acknowledged by all employees that stipulate specifically things such as:

• Employees will **NOT** open personal emails on company computers
• Employees will **NOT** access social websites on company computers
• Employees will **NOT** surf the web or shop on company computers

---

**Administrative Questions from the Security Risk Analysis**

“Have formal acceptable use rules been established for assets?”

“Example assets include data, computer equipment, communications equipment, etc.”
§164.310 Physical safeguards (d) (1) Standard: Device and media controls.

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility and the movement of these items within the facility.

“Cancer Care reported a HIPAA security breach to the Office for Civil Rights, after an unencrypted server backup media and laptop was stolen from an employee’s car. Officials discovered the device contained the protected health information, Social Security numbers and insurance data for some 55,000 patients.”

“Not only did the oncology practice fail to conduct an enterprise-wide risk analysis when laptop and device were stolen, it also had no written policy in place addressing or controlling the removal of electronic media from its locations.”

“Additionally, the practice will also need to develop and put in place an enterprise-wide risk management plan that addresses security risks, data systems and portable electronic devices. It also must update its policies and employee training program, all of which are to be reviewed by HHS.”

“Oncology Group Slapped with $750K HIPAA Fine”
From Healthcare IT News
September 15, 2015

"Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information,"
OCR Director, Jocelyn Samuels
Administrative Questions from the Security Risk Analysis

“Do you work with third parties, such as IT service providers, that have access to your patient’s information?”

a) “Does your organization have Business Associate agreements in place with these third parties?”

§164.314 Organizational requirements.
(a) (1) Standard: Business associate contracts or other arrangements.

(2) Implementation specifications (Required).

(i) Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will—

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

“North Memorial Health Care of Minnesota has agreed to pay $1,550,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information.”

“Two major cornerstones of the HIPAA Rules were overlooked by this entity,” said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). “Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure.”

“In addition to the $1,550,000 payment, North Memorial is required to develop an organization-wide risk analysis and risk management plan, as required under the Security Rule. North Memorial will also train appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan.”

The Office for Civil Rights – The Federal Trade Commission – The Office of the Attorney General
Three Agencies – Three actions - $4,000,000.00 in fines
ONE LAPTOP!
“The Department of Health and Human Services Office for Civil Rights on Friday reached a $400,000 settlement with Rhode Island-based Care New England Health System (CNE) for failing to update its business associate agreement with Woman & Infants Hospital (WIH) of Rhode Island.”

“The latter, in 2012, reported the loss of unencrypted ultrasound backup tapes affecting approximately 14,000 patients, according to an announcement. CNE provided technical support and information security services to the hospital, but a BA agreement initially signed in 2005 was not updated until 2015, and did not include revisions required under the HIPAA Omnibus Final Rule covering business associates.”

§164.308(6)(i) Administrative safeguards

**Standard:** Security incident procedures. Implement policies and procedures to address security incidents.

**Defined as:** the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**(ii) Implementation specification: Response and Reporting (Required)**

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
“Presence Health itself reported the breach, but not within 60 days of discovering the problem, as is required by law.”

“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.”

“$475,000 fine marks first HIPAA enforcement action over breach notification timing”
From Healthcare Dive
January 10, 2017

“The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has taken action against a healthcare facility for failing to report a breach of unsecured protected health information (PHI) in a timely manner.”
§164.310 Physical safeguards.

A covered entity must, in accordance with §164.306:

(a) (1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(b) (1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Physical Questions from the Security Risk Analysis

"Do you have effective physical access controls (e.g., door locks) in place that prevent unauthorized access to facilities and a facility security plan?"

b) "Is there a facility security plan?"

c) "How are physical access controls authorized (who is responsible for ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with ePHI)?"
“The United States Court of Appeals for the Third Circuit has ruled that a class action lawsuit filed by customers of Horizon Blue Cross Blue Shield whose protected health information was exposed when two laptop computers were stolen from its New Jersey offices does have standing, even without proof of harm.”

“Two unencrypted laptop computers containing the personal information of 839,000 plan members were stolen from Horizon BCBS’s headquarters in Newark, NJ. Stored on the laptops were names, addresses, birth dates, Social Security numbers, medical histories, demographic data, lab test results, insurance information, and other care-related data.”

§164.310 Physical safeguards.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(a) (1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Physical Questions from the Security Risk Analysis

“Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?”
TO LOG OR NOT TO LOG – THAT IS THE QUESTION

Physical Questions
from the
Security Risk Analysis

Non-Employee / Workman
Log Form

Why would a

Be necessary?

A TRUE STORY

There is a doctor’s office outside of Dallas who had carpenters come in at the doctor’s request to do work on his office.

Several days after the work was completed, one of the workmen came into the office and said to the receptionist, . . . I’m missing one of my tools and I believe I may have left it here when we were doing the work for the doctor.

The receptionist recognized the man because he had been there for a few days. She told him to go back to where the work had been done to see if he could find his missing tool.

A few minutes later, the workman left telling her, yes, he had found what he had left behind.

Sometime later it was discovered that what the workman had left behind was –

The doctor’s Petty Cash box!

The practice did not log the presence of non-routine persons and therefore had no way of proving that the workman had ever been there.

Walking out with money isn’t a HIPAA violation but what if it had been a thumb-drive or a laptop or paper records?

Representative: (Print Name) ______________________________
Company: _________________________ Phone: ______________
Date Work Performed: _______________  Time In: _____________
Work to be done:  ________________________________________
__________________________________ Time Out: ____________

Representative: (Print Name) ______________________________
Company: _________________________ Phone: ______________
Date Work Performed: _______________  Time In: _____________
Work to be done:  ________________________________________
__________________________________ Time Out: ____________

Representative: (Print Name) ______________________________
Company: _________________________ Phone: ______________
Date Work Performed: _______________  Time In: _____________
Work to be done:  ________________________________________
__________________________________ Time Out: ____________

Representative: (Print Name) ______________________________
Company: _________________________ Phone: ______________
Date Work Performed: _______________  Time In: _____________
Work to be done:  ________________________________________
__________________________________ Time Out: ____________
“Are systems and networks monitored for security events? If so, please describe this monitoring.”

“Are third party connections to your network monitored and reviewed to confirm authorized access and appropriate usage?”

“Do formal change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability (e.g., Virus or Spyware) patching activities?”

These are all actual questions in the SRA but let’s talk about the areas that cause the most trouble.

**Technical Questions from the Security Risk Analysis**

Articles that deal specifically with the technical aspects of violations are seldom seen because the violations of the rules are what is written about. Here are a few actual questions found in the SRA dealing specifically with controlling technology.
What is a Vulnerability Scan?

The automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Technical Questions from the Security Risk Analysis

“How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems?”

This is page One of an actual Vulnerability Scan report run on just ONE computer.

<table>
<thead>
<tr>
<th>Data Breach Risk Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment completed on: 2017-01-19T03:13:32Z</td>
</tr>
<tr>
<td>IP: 127.0.0.1</td>
</tr>
<tr>
<td>OS: Windows 10</td>
</tr>
</tbody>
</table>

Unprotected Data Summary

<table>
<thead>
<tr>
<th>Unprotected Data Count by Type</th>
<th>Potential Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>14,515</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>8</td>
</tr>
<tr>
<td>Visa Credit Card</td>
<td>2</td>
</tr>
<tr>
<td>American Express Credit Card</td>
<td>2</td>
</tr>
</tbody>
</table>

Total Potential Risk: $2,930,178.00

Vulnerability Summary

<table>
<thead>
<tr>
<th>Vulnerability Count by Severity</th>
<th>Percentage of Vulnerabilities by Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>Vendor</td>
<td>%</td>
</tr>
<tr>
<td>Adobe</td>
<td>16%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>69%</td>
</tr>
<tr>
<td>Oracle</td>
<td>10%</td>
</tr>
</tbody>
</table>

Technical Questions from the Security Risk Analysis

“How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems?”
HIPAA §164.312 Technical safeguards

(e) (1) **Standard: Transmission security.**
Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) **Implementation specifications:**

(i) **Integrity controls (Addressable).**
Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

§170.302 General certification criteria for Complete EHRs or EHR Modules.

The Secretary adopts the following general certification criteria for Complete EHRs or EHR Modules. Complete EHRs or EHR Modules must include the capability to perform the following functions electronically and in accordance with all applicable standards and implementation specifications adopted in this part:

(s) **Integrity.**

(1) **In transit.** Verify that electronic health information has not been altered in transit in accordance with the standard specified in §170.210(c).

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(2) **Exchange.** An encrypted and integrity protected link must be implemented.
**HIPAA §164.312 Technical safeguards**

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

   (iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

(e) (1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

   (2) **Implementation specifications:**
   (ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

**§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.**

The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(a) **Encryption and decryption of electronic health information.**

   (1) **General.** A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key **must be used.**
The laptop bag included the member’s computer, which was encrypted and did not contain electronic protected health information (ePHI), and a computer server backup media, which was not encrypted and contained the ePHI of approximately 55,000 individuals. The OCR investigation revealed that CCG failed to properly secure the ePHI contained on the backup media, and did not have in place a written policy regarding the removal of hardware and electronic media containing ePHI into and out of its facilities. The investigation also revealed that CCG failed to conduct an assessment or implement policies and procedures addressing the incident.

§164.310 Physical safeguards

(d) (1) **Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

HIPAA §164.312 Technical safeguards

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

(e) (1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) **Implementation specifications:** (ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

“Stolen laptop bag leads to $750,000 fine for oncology group”
From McGuireWoods LLP
September 14, 2015

“OCR opened its investigation following a report that a CCG workforce member left a laptop bag unattended in his car, where it was stolen by a third party.”

“Is sensitive data encrypted when stored on laptop, desktop and server hard drives, flash drives, backup tapes, etc.?”
“Security Rule Overview for Small Providers”

“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.”

Ever heard of the Safe Harbor Rule?

Here is the definition of unsecured protected health information: “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 [of the Department of Health and Human Services (HHS)] under section 13402(h)(2) of Public Law 111-5.” [78 Federal Register 5695]

Note the following from the Final Rule: “Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information – that is, the information is not considered ‘unsecured’ in such cases.” [78 Federal Register 5639] Finally, “[w]e encourage covered entities and business associates to take advantage of the safe harbor provision of the breach notification rule by encrypting limited data sets and other protected health information pursuant to the Guidance. If protected health information is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.” [78 Federal Register 5644]
§164.310 Physical safeguards (cont’d)

(d) (1) **Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) **Implementation specifications:**

   (i) **Disposal (Required)** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Technical Questions from the Security Risk Analysis

“Are there security procedures for the decommissioning (replacement) of IT equipment and other devices?”

“The U.S. Department of Health and Human Services has settled with Affinity Health Plan, a New York-based managed care plan, for HIPAA violations to the tune of $1,215,780 after a photocopier containing patient information was compromised.”

“Affinity officials were informed by CBS Evening News that, as part of an investigatory report, the television network had purchased a photocopier, previously leased by Affinity that contained confidential medical information on its hard drive. Affinity estimated that up to 344,579 individuals may have been affected by this breach.”

“Moreover, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.”

“At $1.2 Million, photocopy breach proves costly”

From Healthcare IT News
August 14, 2013

“An HHS Office for Civil Rights investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives.”
On June 20, 2016, Sylvia Burwell, Secretary of the Department of Health and Human Services released an 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 over a year, 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.”

“Unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised, based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.”
Cyber criminals lock an organization, such as a medical practice, out of its computer data and demand digitally paid ransom in exchange for an decryption key to regain access to the information.

There are two different kinds of Ransomware to worry about.
One is called Crypto-Ransomware.
The other is referred to as Locker-Ransomware.

Who is Joseph Popp?

There are multiple ways for cyber crooks to get into our systems but there are two ways that outweigh everything else combined.

Email
Social Websites

WHY?

“How ransomware became a billion-dollar Nightmare for businesses”
FROM: The Atlantic September 3, 2016

“According to an FBI tally, ransomware attacks cost their victims a total of $209 million in the first three months of 2016, a stunning surge upward from $24 million in all of 2015."

“The company’s, (Datto) survey of 1,100 IT professionals found that nearly 92 percent had clients that suffered ransomware attacks in the last year, including 40 percent whose clients had sustained at least six attacks.”
In a 2015 Healthcare and Cyber Security Survey, KPMG found four fifths of US respondents said cyber attacks had compromised their information technology.

That's a LOT of other guys.

“Human error a leading cause of cyber security incidents” April 27, 2016
(Taken from a Verizon Enterprise Solutions Report)

“About 30 percent of phishing emails were opened, an increase from the 23% reported in 2015.”

“You might say our findings boiled down to one common theme -- the human element.”

“Healthcare orgs at much higher risk of ransomware attack than financial institutions”
From Healthcare DIVE July 28, 2016

“Healthcare organizations computer networks are 114 times more likely to suffer ransomware attacks than those at financial institutions, and 21 times more likely than schools and universities.”
“Over the past two years, ransomware has grown to become one of the biggest cybersecurity threats. While most infections are random, the healthcare industry has been targeted in 2016 and the outlook for 2017 remains bleak.”

"Many healthcare organizations attacked with ransomware have been able to make a full recovery by deleting systems and reconstituting data from backups. However, there have been numerous cases over the past 12 months when data restoration from backups has failed."

"In October last year, MalwareHunterTeam reported that there are more than 200 distinct ransomware families, each containing a myriad of ransomware variants. In 2016, ransomware revenue surpassed the $1 billion milestone."

“One of the latest developments is fileless ransomware. Since no files are downloaded onto the victim’s computer, traditional signature-based detection systems fail to identify the threat.”

“The Department of Health and Human Services’ Office for Civil Rights has recently issued guidance for HIPAA covered entities on ransomware to help covered entities deal with the increased threat of ransomware attacks.”

“Now the Federal Trade Commission (FTC) has warned businesses that they must do more to deal with the ransomware threat. The failure to implement appropriate defenses against ransomware could constitute a violation of the FTC Act.”

“Ramirez, (FTC Chair Edith Ramirez), explained that “A company’s unreasonable failure to patch vulnerabilities known to be exploited by ransomware might very well violate the FTC Act.” “If companies are found to have violated the FTC Act by failing to implement appropriate defenses, the FTC can issue stiff financial penalties.”
LOOKING AT SECURITY FROM 360 DEGREES

Administrative

Physical

Technical

Cybercrime and Ransomware

So what should practices do?

Your ounce of prevention

- Recognize the significance of the threat and that it’s not only going to happen to the other guy.

- Acknowledge what it was that caused problems for organizations that are similar to yours.

- Realize that there are some very basic things you can do TODAY in your prevention process.

Step 1
Recognition

Step 2
Learn from other’s mistakes

Step 3
Start preparing the basics
### Start with fulfilling REQUIRED items

<table>
<thead>
<tr>
<th>Get a Security Risk Analysis</th>
<th>Have documented Policies and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Do NOT</strong> expect your IT contractor to understand the level of liability that you as a medical practice operate under.</td>
<td>The purpose of documented Policies and Procedures is to demonstrate “forethought”.</td>
</tr>
<tr>
<td><strong>Do NOT</strong> expect your IT contractor to have a sufficient understanding of HIPAA regulations.</td>
<td>Beware of “templates” for policies. Policies and Procedures are supposed to be YOUR policies and procedures.</td>
</tr>
<tr>
<td><strong>Beware</strong> of IT companies that offer the Security Risk Analysis as an added service.</td>
<td>Make sure your employees understand your Policies and Procedures.</td>
</tr>
</tbody>
</table>

### Then go to the next important steps

<table>
<thead>
<tr>
<th>Employee Training</th>
<th>Have “phishing” tests run on your office.</th>
</tr>
</thead>
<tbody>
<tr>
<td>While employee “Security” training is a requirement under HIPAA, get additional training that deals specifically with Cybercrime and Ransomware.</td>
<td>“Phishing” tests are simulated attacks on your office. Fake emails are sent to all of your employees and usually have some sort of attachment. The purpose is to see:</td>
</tr>
<tr>
<td><strong>Do not allow on practice devices:</strong> Checking personal emails</td>
<td>1. Who will open emails from persons they don’t recognize.</td>
</tr>
<tr>
<td>Going to social websites</td>
<td>2. Who will click on attachments without knowing what they are about.</td>
</tr>
<tr>
<td>Shopping or surfing the web</td>
<td></td>
</tr>
</tbody>
</table>
### Then go to proven technical aids

<table>
<thead>
<tr>
<th>Get a quality Firewall installed</th>
<th>Get true Virus protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device that your Internet Service Provider put in your office is <strong>NOT</strong> sufficient to protect a medical practice against the onslaught of Cyber activity. A good firewall – when it is set up properly – will automatically notify your IT department or contractor when certain types of attempted activities take place.</td>
<td>The “protection” that came with your computer when you bought it is generally <strong>NOT</strong> sufficient to protect a medical practice. Anti-virus and Malware protection should, in their description of what they guard against, specifically address Ransomware.</td>
</tr>
</tbody>
</table>

### Then go to proven technical aids

<table>
<thead>
<tr>
<th>Vulnerability Scans</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability scans are probably the most overlooked, <em>inexpensive</em> tool at your disposal. Unfortunately, the vast majority of IT contractors have never provided them. <strong>WARNING:</strong> Many IT companies will tell you that they are running these but, if they cannot provide you with a <em>written report</em> each time, they are NOT doing these scans.</td>
<td>Monitoring is nothing more than a software program that continuously looks for certain things in IT systems. Once setup, it takes no time or effort on the part of the IT department or contractor <em>UNLESS SOMETHING HAPPENS.</em> You don’t have the time or expertise to watch over your IT system. Somebody needs to.</td>
</tr>
</tbody>
</table>
Warnings you should pay attention to

“2016 a banner year for EHR security breaches”
From: Fierce Healthcare  December 29, 2016  Marla Hirsch, JD

“Security breaches of electronic protected health information (ePHI) continue to plague the healthcare industry—and the trend shows no signs of abating.”

“More than 25 million patient records were reportedly compromised as of October 2016. And then, in November, the cases spiked: There were 57 health data breaches—the most in any one month this year, according to the Protenus Breach Barometer.”

“What’s even more concerning is that inside employees were responsible for more than half of November's breaches, a notable increase from past months.”

“Many of these breaches are due to lax compliance with some of the most basic requirements of HIPAA, despite the fact that the law has been on the books for 20 years.”

Warnings you should pay attention to

IF YOU THINK COMPLIANCE IS EXPENSIVE –

TRY NON-COMPLIANCE

Former U.S. Deputy Attorney General Paul McNulty
Warnings you should pay attention to

“Any organization that marginalizes cybersecurity to the bottom of the budget . . . is going to be breached by cyber criminals and advanced persistent threats alike.”

Institute for Critical Infrastructure Technology (ICIT)

Warnings you should pay attention to

“The adage is true that the [YOUR]security systems have to win every time.”

“The attacker only has to win once.”

Dustin Dykes, CISSP
Larry Neiswender,
Founder and Managing Partner
Microsoft Certified Systems Administrator
Practice Workflow and Health Information Technology Redesign Specialist

We Provide:
• Security Risk Analysis (over 300 performed)
• Security Policy and Procedure Documentation
• Employee Security Training
• Provides assistance to practices being audited for HIPAA violations

Protect EHR, LLC
Providing BIG practice services for the small and solo practice in ALL disciplines

P. O. Box 820611
North Richland Hills, TX 76182

817-999-0595
Email: info@protectehr.com
Website: www.protectehr.com