Ekaru Connecting People With Technology

Technology Workshop

HIPAA – Security Risk Assessment: What's Next?

January 9, 2014

Microsoft Small Business Specialist

Microsoft CERTIFIED Partner

Welcome!

- Thank you for joining us today.
- In today's call we'll cover the Security Assessment and next steps.
- If you want to follow from your office, go to www.ekaru.com / Go to "What's New" near the bottom of the page. Presentation will open in a browser, click the down arrow in nav bar to advance slides.

Format

- Call is "Listen Only" to ensure call clarity.
  - (Reason: cut down on ambient noise, avoid "call on hold music" – a bit tough though, because I can't hear you!)
- If you have questions, please eMail to knoran@ekaru.com and we will try to include Q&A at the end of the call – we will be reviewing email live during the call.
- Call 978-692-4200 for help.

Workshop Mission

- Help your practice understand "what's next" after your Security Risk Assessment
- Review most common gaps
- Save you time in the process

These materials do not constitute legal advice and are for educational purposes only. The information in this webinar is based on current federal law and subject to change based on changes in federal law, the effect of state law or subsequent interpretative guidance.

Security Risk Assessment

- Security Risk Assessment
  - Needs to be complete by end of year
  - Involves identifying risks to confidentiality, integrity, and availability of patient information

- NEXT STEPS:
  - Attestation – Practices handle, and the EHR support team is available for help.
  - ***REMEDIATION*** - Don't wait, get started now!

HITECH

- The **Health Information Technology for Economic and Clinical Health (HITECH)** Act provides the **Department of Health & Human Services (HHS)** with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange.

  Under HITECH, eligible health care professionals and hospitals can qualify for Medicare and Medicaid incentive payments when they adopt certified EHR technology and use it to achieve specified objectives.

- HIPAA, MA Data Security Law

Next Steps

- Complete the Security Risk Analysis
  - 80 Items
- Remediate gaps
- Complete/update your documentation

Completed Assessment

- Folder includes:
  - Your practice assessment
  - Emerson Hospital assessment
  - Resources:
    - HIPAA Privacy and Security Toolkit
    - HIPAA Business Associate Agreement – SAMPLE
    - HIPAA Notice of Privacy Practices – SAMPLE
    - HIPAA Security Rule: Encryption FAQs

Next Steps: Security Policy

- Security Policy Document
  - Biggest gap in all assessments completed so far is either no written documentation, or major updates needed
  - Employee manual is good, but not sufficient
  - Must have a written document – not enough to just "do" the requirements.

Reminder: Physical Security

- Most assessment items and discussion have focused on electronic security.
- Don’t forget physical security!
- Parallel requirements.

Written Security Policy

- Sample Document is available from HealthIT.gov
- Sample is long – 85 pages
- Download on line, or we can email a copy.
- "Say what you do, and do what you say"

Written Security Policy

- *Sample* – Table of Contents:

Sample Strategy

- Use Sample Security Policy as a starting point.
- Identify relevant items and customize for your practice
- Get help as needed

Business Associate Agreements

- Does any vendor have access to confidential patient data? Have you discussed HIPAA Security and HITECH requirements with such vendor(s)? Is an up-to-date Business Associate Agreement in place for each vendor that has access to ePHI?
- Many additional questions on this topic.
- Sample copy in your package

Contingency Plans

- If you are required to operate in emergency mode, do you have procedures to enable you to continue critical business processes to protect the security of ePHI?
- Do you have a plan to temporarily relocate if you lose access to your physical location? Would ePHI be safeguarded at temporary locations? Are formal agreements in place for such a relocation?

Contingency Plans

- Have you trained staff on your contingency plan? Is there a contingency plan coordinator?
- Do you have an emergency call list?
- Have you identified situations in which your contingency plan must be activated?
- Is there a plan to restore systems to your normal operations?
- Have you tested your contingency plan?

Breach Notification

- The **Breach Notification Rule** requires covered physician practices to notify affected individuals, the Secretary of the U.S. Department of Health & Human Services (HHS) and, in some cases, the media when they discover a breach of a patient's unsecured PHI.
- Proper use of **encryption** can help avoid these notification requirements

Employee Training

- Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training?

Re-Purposing Equipment

- Do you destroy data on hard drives and file servers before disposing the hardware?
- Are workforce members trained as to the security risks of re-using hardware and software that contain ePHI?

Anti-Virus, Malware

- Have you installed anti-virus and other anti-malware protection software on your computers? Do you use it to guard against, detect, and report any malicious software? Do you protect against spyware?
- Do workforce members update the virus protection software when it is routed to them?
- Do you prohibit workforce members from downloading software they brought in from elsewhere? (digital family photos, games, books, music, etc.)

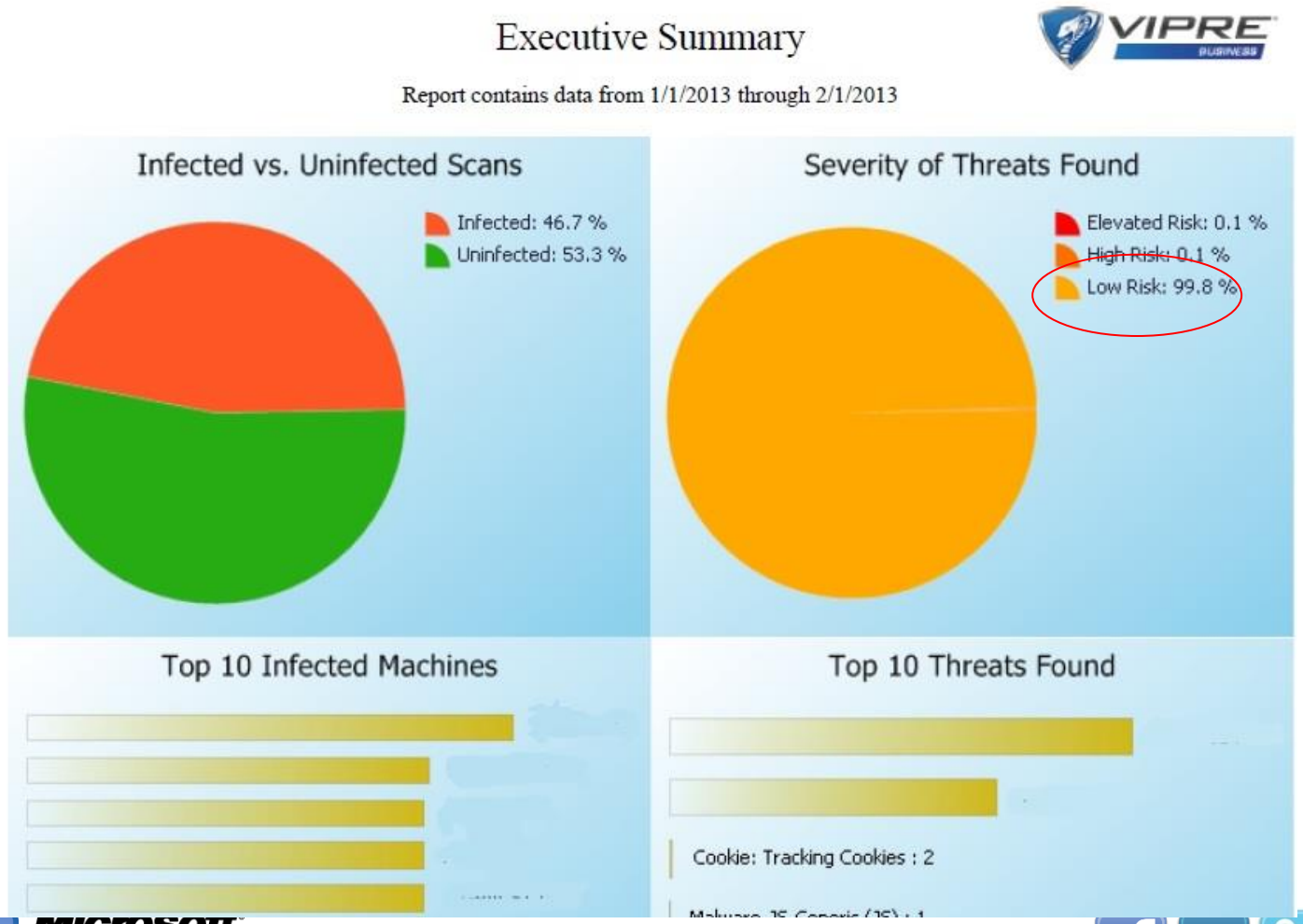
Technology: Consider Managed Services

- Don't "Guess" if systems are up to date
- Automatic reporting for compliance and peace of mind.
- Antivirus
- Anti-Malware
- Security Patching
- Third party Patching

Managed Service

Desktop	Logged On User	Operating System	Available	Antivirus	MalwareBytes	Free Disk Space	S.M.A.R.T	Security Updates	Critical Updates	Third Party Patch
A		Microsoft Windows XP 5.1								
B		Windows Vista (TM) Ultimate 6.0								
C		Windows 7 Professional 6.1								
C	User	Windows 7 Home Premium 6.1								
E		Microsoft Windows XP 5.1								
F		Windows Vista (TM) Business 6.0								
G	User	Microsoft Windows XP 5.1								
H	User	Microsoft Windows XP 5.1								
I		Microsoft Windows XP 5.1								
J	User	Microsoft Windows XP 5.1								
K		Microsoft Windows XP 5.1								
L	User	Microsoft Windows XP 5.1								
M		Microsoft Windows XP 5.1								
N	User	Microsoft Windows XP 5.1								
O		Microsoft Windows XP 5.1								
P		Microsoft Windows XP 5.1								
Q	User	Microsoft Windows XP 5.1								
R		Microsoft Windows XP 5.1								
S		Microsoft Windows XP 5.1								
T		Microsoft Windows XP 5.1								
U	User	Microsoft Windows XP 5.1								
V		Microsoft Windows XP 5.1								
W	USer	Microsoft Windows XP 5.1								
X		Microsoft Windows XP 5.1								
Y	User	Windows 7 Professional 6.1								
Z	User	Windows 7 Professional 6.1								

Antivirus Report



Documentation / Compliance

- Recommendation: Medsafe.com
  - Compliance Specialists
  - Online Training
  - Documentation Portal

Next Steps

- Start your remediation NOW
- Plan ahead for the next few months to get it done
- Audits have started!

Myths…

From HealthIT.gov

- **The security risk analysis is optional for small providers.**

False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.

- **Simply installing a certified EHR fulfills the security risk analysis MU requirement**.

False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR. …

Myths…

- **My EHR vendor took care of everything I need to do about privacy and security.**

False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.

- **My security risk analysis only needs to look at my EHR**.

False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone).

Myths…

- **I only need to do a risk analysis once.**

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

Government Audits

- HHS Office of Civil Rights "OCR" has established a an audit protocol.
- 170 potential audit areas
- Available on-line: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Government Audits

Rule
vities &
nplaint

Check All | Uncheck All

Export as CSV | Export as XML

All (169) Security (78) Privacy (81) Breach (10)

Show All entries

Search: Clear

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	HIPAA Compliance Area
§164.308	§164.308(a)(1): **Security Management Process §164.308(a)(1)(ii)(a)** - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity,...	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and avail...	Required	Security
§164.308	§164.308(a)(1)(i): **Security**	Acquire IT Systems and Services	Inquire of management as to whether formal or	Required	Security

Must have formal documentation

Significant Penalties

- Civil Penalties:

HIPAA Violation	Penalty Range	Annual Maximum
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 - $50,000 per violation	$1.5 million
Individual "knew, or by exercising reasonable diligence would have known" of the violation, but did not act with willful neglect	$1,000 - $50,000 per violation	$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 - $50,000 per violation	$1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation	$1.5 million

Significant Penalties

- Criminal Penalties:
  - Covered entities and specified individuals whom "knowingly" obtain or disclose individually identifiable health information in violation of the HIPAA requirements face a fine of up to $50,000, as well as imprisonment up to one year.
  - Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison.
  - Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Technology Requirements

- Physicians should also note that HIPAA is considered a "floor,". States such as Massachusetts have requirements that go above and beyond what the federal government requires. (**MA Data Security Law**)

Technology requirement #3

- "(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."
- ***Do not email personal information. Instead use encrypted email or encrypted file transfer.***
- *Maintain wireless network encryption.*
- *WPA NOT WEP Encryption*
- *Password protection is NOT encryption!*

eMail Encryption

- Sign up for a free trial at http://voltage.ekaru.com/

Technology requirement #5

- "Encryption of all personal information stored on laptops or *other portable devices**;"
- *We recommend TrueCrypt or PGP encryption to mount encrypted drives.*
- *Full disk Encryption*
- *Hardware encryption if available*

* *If technically feasible*

Technology Requirement #5

- Do all portable devices need to be encrypted? - YES – whenever technically feasible. Also, DVDs and flash drives should be encrypted.
- Laptops: PGP or Truecrypt – You MUST remember your encryption key!

Smart Phones

- iPhone Encryption: http://support.apple.com/kb/ht4175

Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode. This provides an additional layer of protection for your email messages attachments, and third-party applications.

iPhone Encryption

Enable data protection by configuring a passcode for your device:

- Tap **Settings > General > Passcode**.
- Follow the prompts to create a passcode.
- After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.

- **Passcode tips**
- Use these passcode settings to maximize passcode security:
- Set Require Passcode to Immediately.
- Disable Simple Passcode to use longer, alphanumeric passcodes.
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.

Security in the news…

Microsoft Patch Tuesday brings critical Explorer, Outlook fixes

Update Flash, Shockwave ASAP! Adobe also patches Acrobat and Reader

'Master key' to Android phones uncovered

A "master key" that could give cyber-thieves unfettered access to almost any Android phone has been discovered by security

"Patch Tuesday"

- Day the Microsoft releases security patches for all products.
- Second Tuesday of the month

Security TechCenter > Security Bulletins > Microsoft Security Bulletin Summary for September 2013

Microsoft Security Bulletin Summary for September 2013

Published: Tuesday, September 10, 2013

Version: 1.0

This bulletin summary lists security bulletins released for September 2013.

Support ends for Windows XP

Desktop operating systems	Latest service pack	End of extended support
Windows XP	**Service Pack 3**	**April 8, 2014**
Windows Vista	Service Pack 2	April 11, 2017
Windows 7 *	Service Pack 1	January 14, 2020
Windows 8	Not yet available	January 10, 2023

Start planning now if you have Windows XP systems

Windows XP… planning

- As a general rule, we don't recommend updating just the operating systems for PCs older than three years old.
- Best solution in most cases is a replacement PC

"Third Party" Patching

- Adobe Acrobat
- Adobe AIR
- Adobe Flash Player
- Adobe Reader
- Adobe Shockwave Player
- Apple iTunes
- QuickTime
- Mozilla Firefox
- Java Development Kit
- Java Runtime Environment

Remider: Physical Security

- Paper records locked
  - Access is limited by ROLE
    - Locked Practice
    - Locked Office
    - Locked File Cabinet
- Locked office
- Alarm if possible…

Review

- UNDERSTAND Risks
- DOCUMENT Policies "Say what you do"
- COMPLY "Do what you say"
- TRAIN
- REVIEW – Conduct a risk assessment at least annually

Thank You!:

For more information or
to schedule a security assessment:

Ekaru
Connecting People with Technology
978-692-4200
www.ekaru.com

Sign up for Ekaru's free Technology Advisor e-newsletter