Security Risk Analysis Myths and Facts

Source: Office of the National Coordinator Guide to Privacy and Security of Health Information

Myth	Fact
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.
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.
I have to outsource the security risk analysis.	**False.** It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
A checklist will suffice for the risk analysis requirement.	**False.** Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific risk analysis method that I must follow.	**False.** A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.
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 ractice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.
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. For more on reassessing your security practices, please see http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy_security_framework/1173.
Before I attest for an EHR incentive program, I must fully mitigate all risks.	**False.** The EHR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period.
Each year, I'll have to completely redo my security risk analysis.	**False**. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting

Myth	Fact
	period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.

HIPAA Security Rule

Administrative Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Security Management Process	164.308(a)(1)	**Risk Analysis**	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)	**none**	(R)
Workforce Security	164.308(a)(3)	**Authorization and/or Supervision**	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	**Isolating Healthcare Clearinghouse Function**	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	**Security Reminders**	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	**Response and Reporting**	(R)
Contingency Plan	164.308(a)(7)	**Data Backup Plan**	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)	**none**	(R)
Business Associate Contracts	164.308(b)(1)	**Written Contract or Other Arrangement**	(R)
Physical Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Facility Access Controls	164.310(a)(1)	**Contingency Operations**	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)	**none**	(R)
Workstation Security	164.310(c)	**none**	(R)
Device and Media Controls	164.310(d)(1)	**Media Disposal**	(R)
		Media Re-use	(R)
		Media Accountability	(A)
		Data Backup and Storage (during transfer)	(A)

Technical Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Access Control	164.312(a)(1)	**Unique User Identification**	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption (data at rest)	(A)
Audit Controls	164.312(b)	**none**	(R)
Integrity	164.312(c)(1)	**Protection Against Improper Alteration or Destruction of Data**	(A)
Person or Entity Authentication	164.312(d)	**none**	(R)
Transmission Security	164.312(e)(1)	**Integrity Controls**	(A)
		Encryption (FTP and Email over Internet)	(A)

Items marked (R) are Required. Items marked (A) are Addressable.

HIPAA Implementation Specifications are identified as being *Required* or *Addressable*. Addressable specifications are sometimes confused as being Optional, which is not true. The US Department of Health & Human Services says *"a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative."* If you believe that an Addressable specification is not reasonable or appropriate, you must document you r decision. *http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html*

For a Meaningful Use Security Risk Analysis, a HIPAA Assessment, or outsourced HIPAA Security Officer Services, contact Mike Semel at Semel Consulting .

mike@semelconsulting.com or 888-99-SEMEL (888-997-3635)

Get more information about the 2013 HIPAA Omnibus Final Rule at
http://www.semelconsulting.com/industry-news/blog/ and
http://www.emrapproved.com/hitsecurity/ .

Webinar: http://youtu.be/HjntGn3GH0M

Omnibus Rule tips – click here to download the PDF:
http://www.emrapproved.com/pdf/LearningLunch021112_Omnibus_Slides.pdf