Rhode Island Quality Institute

Security Risk Assessments:
What You Need to Know

Tuesday, October 17, 2017

RIQI Hosts:

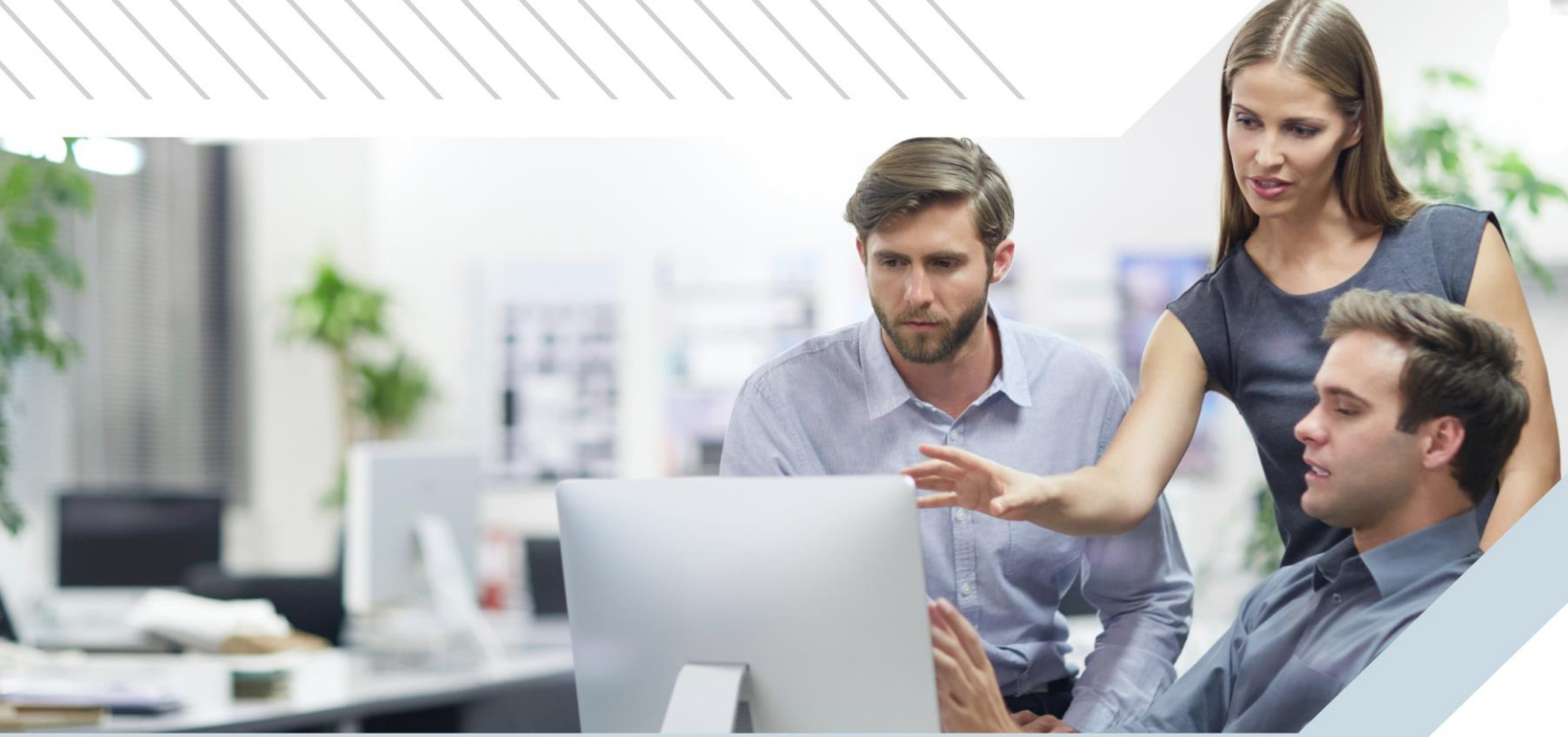
Sue Dettling, PCMH CCE, *Consulting Services Manager*

Margaret M. Menna, MBA, *Senior Training & Education Specialist*

NetCenergy Presenters:

Donald Nokes, *President*

Tom King, *Security Consultant/Project Manager*



NetCenergy HIPAA Compliance

HIPAA Security Risk Assessments

NetCenergy
Powering IT Solutions

Agenda / Table of Contents

1. What is a Security Risk Assessment?
2. What are the requirements?
3. What is required of a compliant Risk Assessment
4. Next steps

Health Risk Assessment

What is a Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their healthcare organization.

Why is it required?

A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk.

Omnibus Law Effective 3/27/2013

What are HIPAA Covered Entities and Business Associates required to do?

By February 18, 2010, among other things, all Covered Entities and Business Associates must do the following…

- Comply with HIPAA's Security Rule - Implement specific policies & procedures; and implement physical, administrative, and technical safeguards to protect medical data.
- Follow HIPAA's Privacy Rule – Protect medical data from misuse; and follow the terms of new or existing Business Associate contracts
- Train all employees on HIPAA Security – Employees must be trained to provide the strongest protections to medical data and proof of training must be maintained.
- Provide "Breach Notifications" if Medical Data is Compromised or Lost – Covered entities must comply with breach notification rules and Business Associates must promptly notify their medical entity partners – and in some cases, patients – if medical data in their possession is compromised or lost.
- Other Requirements Also Apply – This is not a comprehensive list. These items are only a portion of what Covered Entities and Business Associates must do to comply.

Highlights of ONC Guidance

As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction:

SECURITY RISK ANALYSIS MYTHS AND FACTS	
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 meaningful use 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.
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.

To learn more, visit the Privacy and Security Resources page at http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources gov.

Highlights of ONC Guidance

As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction:

SECURITY RISK ANALYSIS MYTHS AND FACTS	
MYTH	FACT
Security Risk Assessment Is only required Once	Assessment must be performed annually and when a major change occurs to the practice

OCR Risk Assessment Requirements

1. Scope of the Analysis
2. Data Collection
3. Identify and Document Potential Threats
4. Assess Current Security Measures
5. Determine the Likelihood of Threat
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk
8. Finalize Documentation
9. Periodic Review and Updates to the Risk Assessment

Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

Willful Neglect Penalties

Table 3: Tiered Civil Monetary Penalties

Standard of Culpability	Penalty	Maximum Penalty
Did not know of the violation and by exercising reasonable diligence would not have known of violation	Corrective action without penalty	No penalty--however, subject to discretion of Secretary.
Unknowing Violations	At least $100 per violation	Not to exceed $25,000 in a calendar year
Violation due to reasonable cause, not willful neglect	At least $1000 per violation	Not to exceed $100,000 in a calendar year
Violation due to willful neglect	At least $10,000 per violation	Not to exceed $250,000 in a calendar year
Violation is due to willful neglect and the violation is not corrected within 30 days of the first date the person liable for the penalty knew or should have known that the violation occurred.	At least $50,000 per violation	Not to exceed $1,500,000

SRA puts you on the path to “Reasonable Diligence”

The Audits continue!

CMS to expand audits of attesting providers.

The Centers for Medicare and Medicaid Services (CMS) has expanded audits of attesting providers (those stating that they have met “Meaningful Use” requirements) under the HITECH Act. CMS announced its plan to audit 10% of attesting providers… “being found deficient on any one measure, will cause a provider to be out of compliance. In this case, CMS will recoup the provider’s entire stimulus.”
In addition, the first issue to be addressed in an audit will be the medical practices security risk assessment.

It's Not Just the Audits!

It's the Fines that have been Assessed!

Corrective Action Plan (CAP) Requirement	$1.2M AHP	$1.7M WLP	$400K ISU	$50K HONI	$1.5M MEEI	$2.3M CVS	$1.0M Rite-Aid	$1.5M BCBS TN	$1.0M MGH	$100K PHX	$865K UCLA	$1.7M AK DHSS
Establish a Comprehensive Information Security Program				X		X						
Designate an accountable Security Owner					X	X						
Develop Privacy and Security policies and procedures					X		X	X	X	X	X	X
Document authorized access to ePHI		X										
Distribute and update policies and procedures					X		X	X	X	X	X	X
Document Process for responding to security incidents		X		X	X		X	X	X	X	X	X
Implement training and sanctions for non-compliance					X		X	X	X	X	X	X
Conduct Risk Analysis / Establish Risk Management Process	X	X	X	X	X	X	X	X	X	X	X	X
Implement Reasonable Safeguards to control risks			X	X	X	X	X	X	X	X	X	X
Regularly review records of information system activity			X									
Implement reasonable steps to select service providers						X						
Testing and monitor security controls following changes					X	X	X	X	X	X	X	X
Obtain assessments from qualified independent 3rd party					X	X	X	X	X	X	X	X
Retain required documentation	X			X	X	X	X	X	X	X	X	X

$13.5+M

How it Works – HIPAA Security Compliance

- **Three types of input to a HIPAA risk assessment:**
  - Administrative Safeguards -164.308
  - Physical Safeguards -164.310
  - Technical Controls – 164.312

  Accurate Documentation is also required – 164.316

- **Technical Controls is the most difficult to answer 630+ or more settings on every Windows machine x's the number of machines**
- **Import or input UTM / IPS / Firewall Syslog data**
- **Import or input SCAP Vulnerability Scanner data**
- **Finalize and generate Compliance Reports**
- **Utilize the 'Gap' and HIPAA reports to prioritize deployment of recommended remediation**

How it Works – What we do

1. **Meet with practice managers to**
   - Conduct site inspection
   - Examine existing (if any) HIPAA required documents

2. **Import or input SCAP Vulnerability Scanner data**
3. **Finalize and generate Compliance Reports**
4. **Submit reports and Executive Summary to Security Officer**
5. **Utilize the 'Gap' and HIPAA reports to prioritize deployment of recommended remediation's**

Example of Executive Summary

- June 5, 2016
- **Executive Summary**
- This xyz practice's security risk assessment examined and addressed security risks, security incidents and systems used to create, maintain, receive or transmit Xyz practice's patients confidential health related information. This assessment also reviewed Xyz practice's administrative documents as they pertain to HIPAA regulations. This risk assessment was a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of patient health records. The risk assessment, used allowable methodologies under NIST 800-30 rev 1. Due to the nature of health care and the importance of keeping patient health data confidential, there should be a very low risk tolerance. The consequences of not taking all available steps to protect health information are extremely costly, and this risk assessment identified deficiencies that threaten patient health data. This assessment was focused on health data that is contained in Xyz practice's internal system, and does not include external collection and storage of data. The risk assessment uses the US Government's security framework developed by the National Institute of Standards and Technology (NIST) for assessing the security of internal computer systems. Adversarial threats include risks from malicious insiders and malicious outsiders. Non-adversarial threats include environmental factors and human error.
- The assessment engagement was conducted by Tom King, NetCenergy's Security Advocate, and the findings are based on the information provided by xyz practice, which is assumed to be accurate. Therefore, potential vulnerabilities are that Xyz practice's answers are not audited and that all information provided by xyz practice was assumed to be valid.
- The risk assessment is valid for a maximum of one year.
- As part of the engagement the following services were provided by NetCenergy:

Example of Executive Summary

- On May 27, 2015 a discovery and consultation with Xyz practice's designated Security Officer, Dr. xyz was conducted, which included an interview and complete physical review of the RI facility. Only two vulnerabilities were noted and listed under **Physical** below.
- A complete review of Xyz practice's current policies and procedures relevant to data security were performed and it was noted that there were no HIPAA required policies and procedures. Those required policies and procedures are listed in Appendix H. Additional necessary HIPAA required documents were also non-existent and are listed under **Administrative**.
- A comprehensive evaluation of Xyz practice's technology environment was conducted and risks noted in the GAP Analysis Report were minimal and will be reviewed by Dr. xyz. **See Technological**.
- The data gathered was combined and analyzed on the basis of HIPAA security requirements. The results identified deficiencies and vulnerabilities (see Appendix F, Risk Assessment Chart) using the ACR2 risk calculation methodology.
- A GAP analysis report (see Appendix A, Gap Analysis Report) was created identifying priorities for resolution for HIPAA compliance.
- A report, with findings and remedies will be presented to Dr. xyz. This report can be used as documentation that a HIPAA security risk assessment has been completed and to demonstrate that they are making the best possible effort to meet the regulations. Reports will appear in the attached appendices.
- **Physical**
- An inspection of the Xyz practice's RI physical site revealed only two vulnerabilities. They are as follows:
- A non-patient visitors log needs to be maintained at the receptionist counter with company represented, date of visit, and time in and time out noted. Also, an updated Patient Privacy Notice required by HIPAA should be available at the front desk for distribution to patients.
- **Administrative**

Example of reports generated during a risk assessment.

Appendices

- GAP Analysis Report (Report detailing deficiencies in priority order)
- HIPAA Security Rule Compliance Report (Details deficiencies per HIPAA regulations)
- HIPAA Audit Framework (Demonstrates the same structure auditors would use while conducting audit)
- NIST Update Report (Details deficiencies and progress by NIST standards)
- Safeguard Status Report (HIPAA and NIST safeguard status per Risk Assessment)
- Risk Assessment Chart (Graph illustrates risk scores based on assessment)
- HIPAA Status Report (Details status of deficiencies and progress by HIPAA regulations)
- Required HIPAA Documents – Policies and Procedures, D-R Plan, employee access agreements, HIPAAA training documentation and copies of visitor log files.

Challenges

- Physicians and staff are generally too busy to efficiently and effectively accomplish a security risk assessment to meet the compliance requirements
- Physicians and staff usually find that constructing required HIPAA required documents is a very daunting task
- Deficiencies must be noted and progress must be shown that there is a real effort to mitigate those deficiencies
- Required HIPAA Security staff training must be conducted and documented for all staff (including temporary workers) and documentation must be maintained for 6 years.

Summary

- To be in full compliance with HIPAA requirements an initial SRA must be conducted with annual reviews.
- “Compliance is not a destination, it is a journey. The Initial SRA’s executive summary, report provides you with a roadmap for your journey.”
- We can help you get started on your journey

Resources

NetCenergy

Donald Nokes, President (dnokes@netCenergy.com)
Tom King, Security Consultant/Project Manager (tking@netcenergy.com)
Tyler Deckman, Client Services Representative (tdeckman@netcenergy.com)

Rhode Island Quality Institute TCPi Transforming Clinical Practice Initiative current care

- Optimizing your EHR to produce data
- Meaningful Use attestation and Quality Measure Reporting
- NCQA Patient Centered Medical Home (PCMH) recognition support
- Accessing all of your patient data in one place through CurrentCare
- Using health IT to improve care coordination

Sue Dettling, PCMH CCE, Consulting Services Manager (Sdettling@riqi.org)