How to Conduct and Implement a Security Risk Assessment (SRA)

September 12 & 13, 2016

MeHI
MASSACHUSETTS
eHEALTH INSTITUTE
at the MassTech
Collaborative

Overview

- Introduction
- Meaningful Use Objective for Security
- Key Security Areas and Measures
- Best Practices
  - Security Risk Analysis (SRA)
  - Action Plan
- Demonstration – BP: Secure™ Portal
- Questions

Introduction

Mark E. Ferrari, MS, PMP, CISSP, HCISPP
Vice President, Chief Information Security Officer
BluePrint Healthcare IT

Email: Mark.Ferrari@blueprinthit.com
Phone: 732.343.3502

What is MU Objective #1 all about?

Protect Patient Health Information	
Objective	Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.
Exclusion	No exclusion.

Meeting MU Objective #1

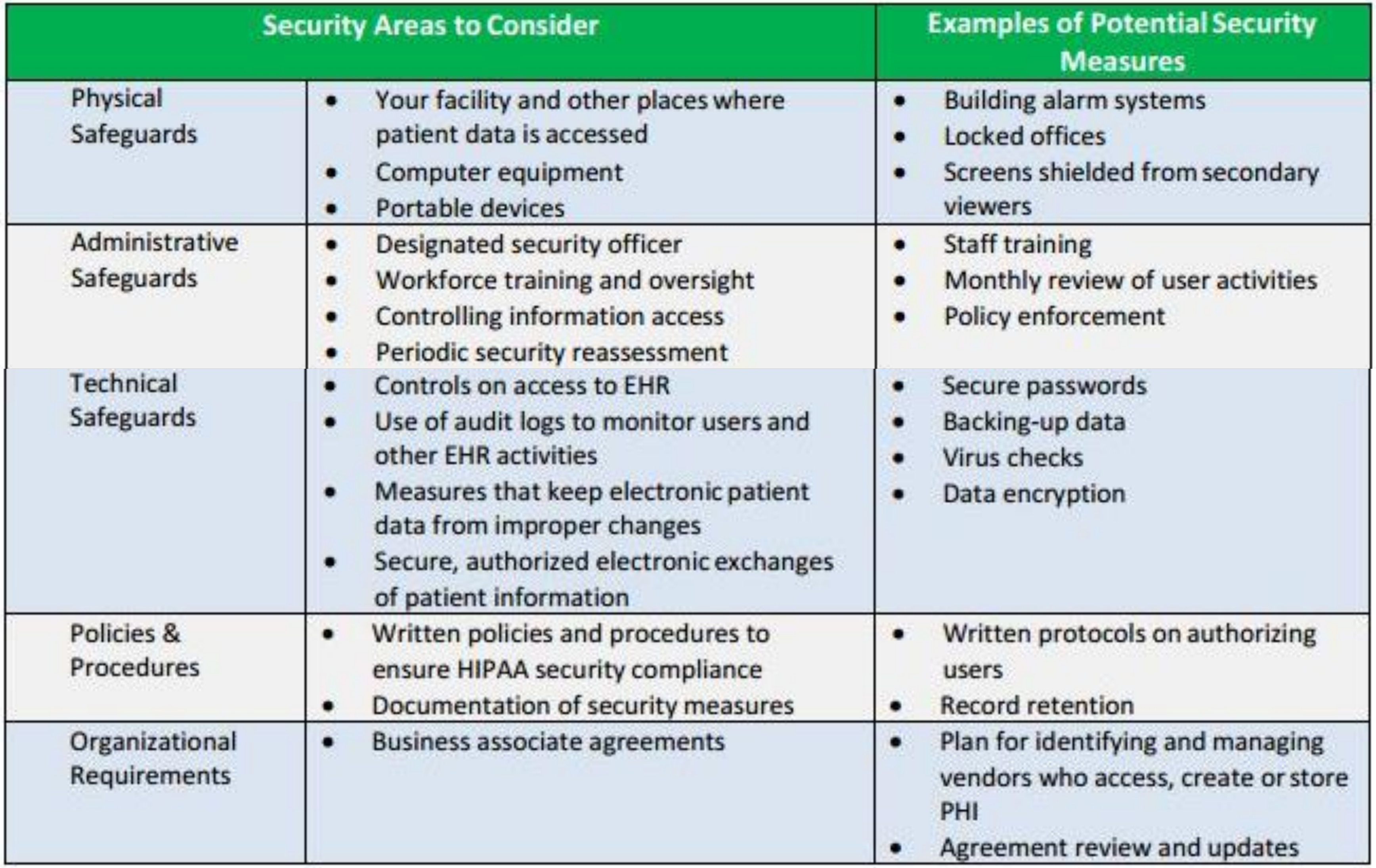
Specifics of the Measure:

1. Implement ***policies and procedures*** to prevent, detect, contain, and correct security violations.
2. ***Conduct an accurate and thorough assessment of the potential risks and vulnerabilities*** to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
3. ***Implement security measures sufficient to reduce risks and vulnerabilities*** to a reasonable and appropriate level.
4. ***Apply appropriate sanctions*** against workforce members who fail to comply with the security policies and procedures.
5. Implement procedures to ***regularly review*** records of information system activity, such as ***audit logs, access reports***, and security incident tracking reports.
6. Implement a mechanism to ***encrypt*** and decrypt electronic protected health information.
7. ***Equivalent alternative measures***

Meeting MU Objective #1

- Conduct a thorough assessment or review covering the key security areas for all locations
- Identifying threats, vulnerabilities, risks and deficiencies by reviewing:
  1. ***Physical safeguards***
  2. ***Administrative safeguards***
  3. ***Technical safeguards***
  4. ***Policies & procedures***
  5. ***Organizational requirements***

Meeting MU Objective #1



Security Areas to Consider		Examples of Potential Security Measures
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to ensure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Business associate agreements	• Plan for identifying and managing vendors who access, create or store PHI • Agreement review and updates

Best Practices – Completing a Security Risk Analysis

- Who should complete the SRA?
- When should the SRA be completed?
  - At least annually; during program year and before attestation
- How to document completion?
- How to address data encryption?
- What to do after system upgrades?
  - Deficiencies addressed/corrections made consistent with risk management process

Best practices – Creating an Action Plan

- Who should be involved in decision-making?
  - Demonstrate decision-maker commitment to and involvement in the process
- Assigning responsibility and accountability
- Creating a timeline
- Reviewing progress as a group
- Documenting progress
- Implementing a robust, ongoing risk management process

Tools for Performing an SRA

- Spreadsheets
- ONC SRA Tool - https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- BP: Secure™ - SRA Portal - http://mehi.masstech.org/services/meaningful-use-services-overview/privacy-security/securetm

BP: Secure™ Portal Demonstration

Questions

Questions?