Part 7: Best Practice Oversight and Governance

Presented by: Susan Clarke,
Health Care Information Security and Privacy Practitioner

June 5 & 6, 2018
Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)’ opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.
Learning Objectives

Best Practices for managing risk and oversight of your HIPAA compliance program. How Telehealth is impacted by HIPAA and importance of conducting a security risk analysis (SRA). How a SRA fits into Promoting Interoperability (formerly EHR incentive programs).
Acronyms...

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis
Privacy and Security Starts at the Top

• Designate a privacy and security officer
• Make sure that each has a job description
• Select a qualified professional to assist you with the Security Risk Analysis
• Promote a culture of protecting patient privacy
1. **People Strategy** - put people first

2. **Process Strategy** - then process

3. **Technology Strategy** - then technology. Select technology that will solve the problem, don’t find a problem to make use of the technology

**Governance vs. Culture**
- Governance is how the organization says it makes decisions and gets things done
- Culture is how the organization actually makes decisions and gets things done
- A large gap between Governance and Culture requires more communication
- Effective Program Strategy must account for both: “Culture eats Strategy for Breakfast”
Every organization faces risk

Clinical teams manage risk on a daily basis yet information risk management programs are often not as formal as needed.
Understanding and Managing Risks

**Patient Safety**
- Intentional or unintentional incidents
- Reliability, functionality, availability
- Misdiagnosis, treatment errors

**Clinical Operations**
- Downtime due to equipment availability
- Impact on hospital operations
- Reduced ability to deliver care

**Business & Financial**
- Reputation
- Revenue / Referrals
- Law suits / fines
- Stock value

**Privacy**
- Information (PHI, PII, credentials)
- Data breach (transmission intercept, device loss or theft)
- Intellectual property (clinical trials & research)

**Security**
- Device used as means for intrusion – beachhead attack
- Impact on network performance, e.g. alarm delays
- DDoS (origin of or impacted by)

**Indirect Risks**
- Patient trust
- Patient treatment decisions
- National Security
Develop an Action Plan (Risk Management Plan)

• Use Security Risk Analysis to identify threats and vulnerabilities
• Focus on high priorities and low hanging fruit
• Identify what needs to be done
• Who is going to do it
• When will it be done
Examples of Documentation to Keep

• Completed checklists
• Security Risk Analysis report(s)
• Risk management action plan
• Business associate (BA) agreements
• Trainings for staff
• System monitoring results
• Policies and procedures
• Meeting minutes
Business Associates

• Responsibilities are very similar to those of a covered entity (CE)
• CE is responsible for obtaining a BA agreement obligating the BA to safeguard protected health information
• Breach notification requirements must be met
• A covered entity can be a business associate of another covered entity.
• If a covered entity enlists the help of a business associate, then a written contract or other arrangement between the two must: 1) Detail the uses and disclosures of PHI the business associate may make; 2) Require that the business associate safeguard the PHI.
Organizations frequently underestimate the proliferation of ePHI within their environments.
Prevent with Education and Training

• Build your policies and procedures and train, train, train; including employees, volunteers, trainees and contractors
• Keep copies of your policies and procedures in an easy-to-find place
• Formally educate and train your workforce at least once a year or when changes happen
Burden of proof is on you...

- Policy and procedures are statements that you assert your intent to comply with regulations. *Important--you must follow.*
- When accountable but can’t control, consider cyber-insurance (might not cover BA breach).
- Have employees become your biggest asset not your biggest liability.
- Strong safeguards=evidence of compliance.
- Engaged and supportive leadership.
Document Your Process, Findings and Actions

• Records will be essential if you are audited
• Good faith effort can be the difference between a corrective action plan (CAP) and a fine
• Maintain records for six years
HIPAA and Telehealth

- Privacy, security and confidentiality issues must be addressed in telemedicine the same as in conventional medical practices.
- Telemedicine increases the frequency that PHI is available electronically, challenge to keep ePHI confidential.
- Technical safeguards like encryption provide safe harbor.
- No control over vendors actions or operations, clearly state in Business Associate agreements.
Sector/Jurisdiction specific, certain providers or types of information, consumer protection laws, state breach reporting.

- Informed consent for telemedicine.
- Mental health information.
- Substance abuse information.
- HIV/AIDS/communicable disease data.
- Genetic data.
- Marketing restrictions.

HIPAA & HITECH
Telehealth Privacy Considerations

• Notice of Privacy Practices, Website Privacy Statement, Terms of Use, Online “pop-up” authorization, electronic signature, informed consent to Telemedicine.

• State laws vary, if multiple States use strictest to standardize processes.

• There must be a private and uninterrupted space in which the equipment is kept where the client/patient will consult with the provider.

• Providers and patients using televideo equipment often speak louder than normal.

• HIPAA laws that govern use, disclosure and breach must be followed faithfully.

• There should be a door that closes and is able to be locked.

• A telephone is needed as backup in case the televideo connection drops.
Telehealth Security Considerations

• Data Security including encryption, authentication and data storage.
• Challenge of protecting ePHI as it moves through the healthcare system.
• A robust IT department will support telehealth security requirements.
• Telehealth access to the local EHR, use of consumer data, deidentification for mining and re-sale.
• Some medications require a “wet signature.”
• Credentialing staff, this can be a lengthy process.
• Telehealth may be unfamiliar territory for security professionals.
Perform a Security Risk Analysis

• Conducting a security risk analysis is a process of identifying, estimating, and prioritizing information security risks that could compromise the Confidentiality, Integrity and Availability of protected health information in a health care facility. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

• Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

• Examples: EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); removable media.
A Goal Without a Plan is Just a Wish

Promoting Interoperability formerly Meaningful Use (MU)
Merit Based Incentive Payment System (MIPS)
Advancing Care Information (ACI) Performance Category
Security Risk Analysis Transition Measure

Objective: Protect Patient Health Information
Measure: Security Risk Analysis
What Do You Need to Do?

MIPS/ACI/MU

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 data created or maintained by CEHRT in accordance with requirements in 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 MIPS eligible clinician’s risk management process.
Your CEHRT determines which measures set you can report

• If your EHR system is a 2014-certified CEHRT, you must select the **2017 ACI transition measures set**

• If your EHR system is a 2015-certified CEHRT, you can choose to report either the **2017 ACI transition measures set** or the **ACI measures set**

• Either measure requires that a Security Risk Analysis be performed or reviewed
Timing of the Security Risk Analysis

• It is acceptable for the security risk analysis to be conducted outside the MIPS performance period

• SRA must be conducted within the calendar year of the MIPS performance period (January 1st – December 31st)
It’s Not Easy

1. System Characterization
   - Create an inventory of applications and systems
   - Group assets: Applications and support systems (workstations, laptops, network, etc.)

2. Threat Identification
   - Identify reasonably anticipated threats
   - Consider: Acts of nature, acts of man, and/or environmental threats

3. Control Assessment
   - Assess: What controls are in place?

4. Vulnerability Identification
   - Assess: What controls are missing?
   - Identify how applications or systems could be exploited

5. Likelihood Determination
   - Decide: What is the probability of each threat occurring?

6. Impact Analysis
   - Rate possible impacts as: High, Medium, Low
   - Evaluate: What would the risk identified do to my organization?

7. Risk Determination
   - Calculate a risk score

8. Recommended Controls
   - Provide recommendations to reduce or manage risks appropriately

9. Results Documentation
   - Create a summary of key findings, recommendations and estimates to implement
   - Document management’s decisions: Mitigate, transfer, or accept risk

Reprinted with permission from: Susan Lucci and Tom Walsh Consulting, LLC
The Risk Management Plan

To meet the Risk Management requirement of this measure you must:

• know what is wrong,
• how you will fix it,
• when you will fix it,
• and who will fix it.
If you are not a HIPAA guru....

Consider getting help from a qualified professional

Verify that they will provide you with:

• Security Risk Analysis
• Risk Management Plan
• Training Plan
• Policies and Procedures
• Customer Support
Keep Up With the Changes

• Join the OCR Privacy and Security Listservs

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html
Please let me know how I can help?

For assistance please contact:

Susan Clarke: sclarke@mpqhf.org, (307) 248-8179
Questions