A Case Study:

The Top Ten Trends: Recommendations for Medical Practices evaluated for Security Risk Assessment

American Society of Ophthalmic Administrators
Annual Symposium & Congress, April 25-29, 2014
Boston, MA

Presented by Mike Manere, Founder/Partner of MedSafe & John Bell, MBA, COE, CMPE, Practice Administrator - North Suburban Eye Associates

Financial Disclosure

Important Note to Attendees of this lecture:

As a Founder/Partner of MedSafe/TCS, Mr. Manere has a financial interest in this presentation. Mr. Bell is the Practice Administrator of North Suburban Eye Associates and has no financial interest in this presentation.

Learning Objectives

After conducting over 750 Security Risk Assessments, MedSafe has created a listing of the top ten deficiencies that medical practices continue to struggle with. By listing these deficiencies, it is our hope that ophthalmic practices can see where their medical colleagues are continuing to miss the mark for Security Risk Assessments and provide a template for overcoming these within their own practices. This is also important data for properly attesting for MU and meeting the requirements for the HIPAA Omnibus Final Rule.
Introduction

Over the last two years, MedSafe has conducted over 750 Security Risk Assessments for medical practices. We have identified the top ten HIPAA-HITECH issues that these practices have experienced. We will explore why these are problem areas and how they can be remediated.

These privacy and security topics relate to the content of the Office of Civil Right's 2012 HIPAA pilot program.

Security Risk Assessments will remain part of the healthcare privacy and security discussion.

Security Risk Assessment (SRA)

What we hear from practices:

• Why should we conduct the SRA?
• What initiated the interest.........

  Meaningful Use Attestation
  M/Use Attestation Audits
  HITECH CE Requirements
  Random Privacy/Security Audits

Benefits of the required SRA....

• Minimize liability and breach potential
• Prepares CEs for random audits
• Enhance patient privacy and security
• Establish standards of practice
• Establishes specific goals for organizations
• Educate personnel on regulations and policies; engage and communicate
OCR HIPAA Audit program

Every covered entity is eligible for an audit.
§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 PHI / ePHI.

According to HHS:
- Each covered entity is required to conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity and availability of ePHI.
- The CE must then make decisions on how to address the findings from the assessment and manage those risks.
- Items that are deemed addressable at the time of the assessment must be documented and evaluated for appropriateness, and if not appropriate, alternate methods must be considered and implemented.

The Security Risk Assessment should be reviewed and updated on an on-going basis.
Security Risk Assessment requires:

- Identification of ePHI vulnerabilities
- Documentation of ongoing corrective action
- Documentation of existing security elements
- Education of employees
- Communication of implemented policies including personnel sanctions
- PHI/ePHI risk management & physical security

Security Risk Assessment ePHI Vulnerability Trends

TREND “1” DOCUMENTATION OF SECURITY RISK ASSESSMENT

- Has your organization documented ongoing evaluation and corrective action?
- The Federal Government states that ongoing evaluation of security vulnerabilities and corrective action is required.
- Is your organization prepared for a random privacy/security audit?
- Is your organization prepared to effectively manage a breach of PHI/ePHI?
  What measures were in place at the time of the breach, to prevent or minimize the probability, risk or impact of a breach?
Once the initial assessment is conducted, and the privacy/security vulnerabilities have been identified and documented, this is where the work begins.

What next………?

• Upon receipt or completion of the SRA recommendations report, this document may be filed away, with no further action taken or documented.
• Once vulnerabilities are identified and documented, the CE is responsible to take corrective action on an ongoing basis.
• Document all actions taken.
• Document existing security measures.
• Take a proactive approach.

“We took no further action…. Why is that a problem?”

Increased fines and penalties for willful neglect under Omnibus Final Rule:
“We knew it was, or might become a problem, and we did nothing to correct it.”
**BREACH AND LIABILITY**

- Increased likelihood for breach:
  During a breach investigation, will the practice have the capability of producing documentation reflecting reasonable measures taken to protect PHI/ePHI?
- Increased CE liability
  If a breach occurs as a result of the inaction of the CE……
  **THE COVERED ENTITY IS RESPONSIBLE!**

---

**TREND “2”**

Secure Business Associate Agreements

Covered Entities (CEs) are required to secure Business Associate Agreements (BAAs) with its Business Associates (BAs).
Initially, some CEs may believe that they have no Business Associates, or they may have continued to share PHI/ePHI with Business Associates without the appropriate agreements in place.

---

**Why BAAs?**

- BAAs protect the Covered Entity
- BAAs make protecting PHI/ePHI a shared responsibility.
- BAAs are a BA’s written promise to protect PHI/ePHI in accordance with federal laws.
- Without BAAs, the CE is essentially sharing PHI with no written promise to protect it and with no shared liability.
- BAAs are required.
Who are my organization’s Business Associates?

Examples:
Software Vendor with ePHI/PHI Access
Shredding Service
IT Service Provider
Answering Service
Billing Service or Clearinghouse
Collection Agency
Transcriptionists
Record Archival Service
Appointment Reminder Service

---

TREND “3”
CONTROL ePHI ACCESS

User-specific user names & passwords for EMR, EHR, PM and OS are required.
Without controlled access, the CE loses its ability to:
• conduct accurate internal audits
• conduct accurate employee audit trails
• research breach incidents
• preserve employee accountability
• effectively monitor ePHI access
• preserve ePHI Security

---

ePHI ACCESS

• The HIPAA Security Rule requires that each individual who has access to electronic personal information must verify their identity before gaining access.
• The HIPAA Security Rule requires users to have individual unique passwords.
**PASSWORDS**

• Procedures must be followed for creating, changing, and safeguarding passwords.
• They must be kept confidential (i.e., not shared with anyone else, or left next to the computer on a “Post-It” note) and should be changed on a regular basis to ensure security.

**Controlled ePHI Access**

• Personnel must be trained to log-out of ePHI applications when workstations/devices are unattended. Failure to secure ePHI in this manner may result in unauthorized access to ePHI, even when automated time-out features are in place.
• When a device is left unattended, the user is required to log-out and re-enter his or her password upon return.
• Minimizing an open program is not an effective security measure.

**What exactly, is required?**

For any and all programs containing ePHI, AND for the operating system:
• User-specific user names and passwords
• Automated prompts requiring users to change their passwords every ninety days
• Users must store passwords securely.
• Log out of unattended ePHI programs to protect ePHI, to preserve individual user accountability and the integrity of the audit process.
TREND “4”
Implement Privacy & Security Policies

Written policies alone, are not enough.

Once the CE has developed written policies and procedures, these documents require:

• The signature of the approving authority
• A written effective date
• Implementation; *Is the practice compliant with its own policies?*
• Communication is key. Distribute policies to relevant staff and providers. Communicate expectations and sanctions for noncompliance.

---

Policies and Procedures

• DOCUMENT
• APPROVE
• IMPLEMENT
• COMMUNICATE
• ENFORCE

---

TREND “5”

ENCRYPT DEVICES

* laptops, tablets, smart phones, hard drives *

• Encryption is a method of converting an original message of regular text into encoded text. There is a low probability that anyone other than the receiving party, or one with a key to the code, would be able to decrypt the information.
• When encryption is present, secure documentation of the encryption for production in the event of an audit.
Encryption: Federal Guidelines

- An Addressable Implementation Specification of the HIPAA Security Rule discusses how practices should evaluate encryption as a method of protecting electronic protected health information from unauthorized use or disclosure, whenever deemed appropriate, reasonable, and feasible.
- Under the Security Rule, methods are not specified. However, under the HITECH Act Breach Notification Rule, specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, (or the PHI is not destroyed according to guidance), then the PHI is termed “unsecured.”
- If a breach occurs of unsecured PHI, individuals, the HHS, and the media must be notified of a breach.
- Encryption renders PHI unreadable and undecipherable; thus theft of an encrypted device will not warrant a breach notification process.

SCENARIO: STOLEN LAPTOP

Would you rather:

1) Decide to encrypt the laptop and secure documentation of the encryption; If it is stolen, theft of an encrypted device does NOT constitute a breach and the notification process is not required.

OR

2) Decide NOT to encrypt the laptop; If it is stolen, begin the large-scale breach reporting process:
   - Notify the federal government
   - Submit annual reports to the federal government
   - Posted online to the HHS “Wall of Shame”
   - Post notice on practice website
   - Submit individual notifications to each patient in database
   - Notify the media

TREND “6”

Conduct regular employee audit trail reports

- Monitor employee activity & ePHI Access;
- What is an employee audit trail process?
- The Security Rule requires that hardware, software, and/or procedural mechanisms be implemented that record and examine activity in information systems that contain or use electronic protected health information (ePHI).
- Secure documentation that audit reports are conducted on a regular basis. A quarterly frequency is recommended.
Audit Trail Reporting

As required by the HIPAA Security Rule, CEs must have mechanisms available for auditing and reviewing access and system activity of information system(s), and must perform routine access and activity audits.

It is also required that each covered entity use these mechanisms to audit and review computer system(s) for appropriate access and activity by users.

The practice must monitor software activity reports such as audit logs and access reports on all information systems that contain ePHI.

MONITOR - BE AWARE

• HHS enforcement sanctions increase substantially if a breach occurs and the practice should have been aware of a security breach, but had not performed internal audits and was therefore, not aware of a breach.

Audits

• It is recommended that covered entities inform personnel that regular monitoring of user activity is conducted.
• Users should know that they are accountable for system activity that takes place under their log-in.
• The audit trail reports must be retained for a period of at least six years.
How does a CE conduct an audit?

- Secure specific instructions from the EMR software vendor(s).
- Identify what information the software has the capability of monitoring.
- Example: Can the program identify which users viewed a patient record, or is it restricted to identifying only when changes are made to a record?
- Document the audit protocol.
- Generate and retain quarterly reports in support of the protocol.

**TREND “7”**

Preservation of ePHI and Other Data

Does the practice have DOCUMENTATION of:

- ePHI Backup & Test
- Local Server Backup & Test
- Disaster Recovery Plan & Test
- Emergency Mode Process & Test
- Encryption

Is valued information backed up?

This is a Required HIPAA Security Implementation Specification.

Identify what data requires backup:
- EMR, local data, PM System, Financials

Secure documentation of the backup process AND documentation that the process has been tested.
TREND “8”
Notice of Privacy Practices

Is your Notice of Privacy Practices compliant with current regulatory elements?

Is having a current Notice of Privacy Practices enough?

Is your practice compliant with posting and distribution requirements?

Notice of Privacy Practices (NoPP) Requirements

Practices are required to:
• Have a current Notice of Privacy Practices.
• Post the notice conspicuously in the practice.
• Post the notice on the practice’s website.
• Make the new notice available to existing patients.
• Distribute the notice to new patients at first encounter prior to provision of service

Notice of Privacy Practices (NoPP) Requirements (con’t.)
• Attempt to obtain and retain a copy of the written acknowledgment of receipt of the Notice of Privacy Practices.
• Except in emergency situations, the practice must make a good faith effort to obtain a new patient’s signed acknowledgment of receipt of the notice.
• If written documentation cannot be obtained, the practice must record its efforts to obtain the acknowledgment and the reason why it was not obtained.
NoPP Content

- Employees should read the Notice of Privacy Practices and become familiar with its content.
- Patient rights are defined within the notice.
- Employees should be prepared to facilitate provision of patient requests to assert their rights, including disclosure restrictions or record amendment requests.

TREND “9”
PHYSICAL PHI SECURITY

- Secure storage of PHI documents; physical measures to reduce breach risk
- Original records must be secured in such a way that only employees have access to the records.
- Original records should never be left alone with the patient or patient’s representative, or in any area that can be accessed by the public.

Considerations

- Are patient charts stored securely?
- Are patient care documents visible to unauthorized individuals?
- Are PHI storage areas restricted to only those with a need to access?
Measures

- Locks
- Keys
- Cabinets
- Doors
- Signage
- Windows
- Interior security
- Restricted access

Privacy Considerations

Facilities must ensure that staff members protect confidential patient information. Typical breaches include billing areas, which are not private enough to allow confidential discussions of financial situations. Such an arrangement may be viewed as insensitivity to patient’s needs with respect to confidentiality and may prompt the filing of a complaint.

TREND "10"

Personnel Training

Covered Entities are required to train their employees. Providers and staff are accountable for compliance with privacy and security regulations….

…and with practice policies!

Do they know what’s expected?
Training Requirements

- Practices must have records of training for all staff on the practice’s privacy or security practices, policies and procedures.

- The practice must train all members of its workforce on the HIPAA policies and procedures with respect to PHI/ ePHI, as necessary and appropriate for the members of the workforce to carry out their function within the practice.

A practice must provide training:

(A) to each member of the practice's workforce by no later than the compliance date for the practice;

(B) to each new member of the workforce within a reasonable period of time after the person joins the practice's workforce; and

(C) to each member of the practice's workforce whose functions are affected by a material change in the policies or procedures within a reasonable period of time after the material change becomes effective.

Reference: 45 C.F.R 164.530, 164.308