HIPAA Security

What's the Risk?

The Office of Civil Rights (OCR) continues to increase its investigations, enforcement, and imposing higher post-breach monetary payments due to breach incidents. Beasley's 2018 Breach Briefing reported that the cause of OCR's increased activity is in part, due to:

> *…entities' failure to comply with HIPAA's privacy and security rules, which have been on the books since 2003 and 2005. Hot button issues for OCR include failing to encrypt portable devices, conduct security risk assessments and enter into business associate agreements with vendors holding PHI.*[1]

Any business with electronic protected health information (ePHI) runs the risk of preventable information losses. When considering where PHI resides, most people think about the medical record as the source to secure and protect. Yet many devices in the typical office practice, such as copiers, fax machines, printers, and tablet computers, are able to store large quantities of information. Some medical devices also have an internal memory. These include electrocardiogram machines, portable diagnostic imaging devices such as ultrasound units, and laboratory analyzers. Finally, a surprising amount of ePHI can be found on electronic storage devices, such as CDs, USB flash drives, memory cards, external hard drives, and servers. Theft or loss of portable storage devices continue to result in healthcare information privacy breaches.

When Is This Risk an Issue?

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) addresses the required technical and nontechnical safeguards to secure electronic protected health information (ePHI). The Security Rule protects a subset of PHI that includes all information created, received, maintained, or transmitted in electronic form. The Office of Civil Rights (OCR) is responsible for enforcing the Security Rule. A data breach can be costly, consisting of legal fees, forensic fees, regulatory enforcement actions, fines and penalties, business interruptions, and reputational damage.

Administrative Safeguards

The Security Rule mandates that practices perform risk analysis as the first step in their security management processes. The activities required in the risk analysis include:

- Evaluate the likelihood and impact of potential risks to e-PHI.
- Implement appropriate security measures for the risks identified.
- Document what measures were chosen and the rationale for choosing those measures.
- Ensure continuous, appropriate security measures are maintained.[2]

Updated: November 2018

Other administrative safeguards include developing and implementing policies and procedures to protect ePHI, workforce security, training, backup plans, and business associate contracts. When OCR is investigating a breach, they request entities to produce their risk analysis, implemented security measures, policies, and procedures. If OCR determines the analysis is not at the appropriate level or the measures identified have not been implemented, the practice is at risk for receiving heavy fines, penalties, and/or corrective actions.

Physical Safeguards

Practices are expected to establish appropriate physical safety measures to protect all equipment with ePHI from unauthorized physician access. Data on reported breaches clearly show that failure to implement and follow physical security measures results in theft and unauthorized access. Inappropriately disposing equipment containing ePHI without performing media sanitization is another security risk.[3]

Sanitization refers to a process that renders the data inaccessible.[4] In other words, the data are removed from the media. Effective sanitization techniques and storage media tracking are critical to protecting sensitive data against unauthorized disclosure.[5] When donating, recycling, or even transferring equipment and/or medical devices with stored ePHI, it is essential that organizations "ensure that no easily re-constructable residual representation of the data is stored on the media after it has left control of the organization."[6]

A sample ***Certificate of Sanitization*** is available in the National Institute of Standards and Technology (NIST) Draft Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization* at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. NIST provides guidance on sanitization methods for several types of media, including:

- Hard copy storage: paper and microforms.
- Networking devices: routers and switches.
- Mobile devices: smartphones.
- Office equipment (copy, print, fax, and multifunction machines).
- Legacy magnetic media (floppies, zip disks, reel, and cassette format magnetic tapes).
- External locally attached hard drives (USB).
- Optical media (CD, DVD).
- Flash-based storage devices.[7]

Technical Safeguards

The Security Rule requires policies and procedures be implemented to protect and control access using technical safeguards. Safeguards include access control, person authentication,

transmission security, and integrity controls to prevent ePHI alteration or destruction. The Security Rule does allow some scalability; each standard is required, but the implementation specifications deemed addressable allow the practice to assess reasonable and appropriate security measures. Practices should consider in their assessment:

- Size, complexity, and capabilities.
- Technical, hardware, and software infrastructure.
- Cost of the security measures.
- Likelihood and possible impact of potential risks to ePHI.[8]

Document all assessments and decisions, and implement some type of security measure that would meet the standard's requirements (deciding against implementing a security measure is not an option). Ineffective security measures and lack of a thoughtful implementation plan can increase the level of fines and penalties if a breach occurs. Outside forces can compromise health information integrity. Attacks on networks by hackers and malware can cause major damage to EMR systems. They typically require costly investigations that involve legal services, forensics, notification, credit monitoring, and possibly crisis management and public relations assistance.[9]

See the NIST Security Risk Assessment Tool at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment.

How Can I Reduce Risk?

Compliance with Security Rule standards is required regardless of the size of the practice. It requires practices to conduct periodic risk analyses of ePHI security. It is essential that the risk analysis includes consideration of all locations where and devices on which ePHI is created, viewed, and stored. Maintain a current comprehensive inventory of all equipment with an internal memory, and include the equipment in the annual security risk analysis. Implement administrative, physical, and technical safeguards to comply with the Security Rule and protect the security of ePHI.

Implement Administrative Safeguards	
Perform a security risk analysis	• Perform a risk analysis for the practice. Identifying and analyzing potential risks helps to determine which security measures to implement. At a minimum, include the following in the risk analysis:

Implement Administrative Safeguards	
	○ Identify all equipment and devices containing ePHI and all sources of information. Include all ePHI that is created, collected, transmitted, and stored, regardless of the storage medium. Consider ePHI in EHRs, mobile devices, and medical devices, as well as in "the cloud" or on servers, hard drives, and portable storage media (e.g., external hard drives, USB flash drives, and any type of disc). ○ Determine potential risks and vulnerabilities of each, and evaluate the likelihood and impact of a security breach and its threat to ePHI. ○ Identify and implement security measures to address vulnerabilities. ○ Document and save the assessment and implemented security measures and the rationale for selecting those measures. ○ Monitor and maintain security measures continuously. • Review the ONC's HIT Security Risk Assessment Tool at: ○ https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment.
Develop a security management process	• Develop security management processes, policies, and procedures that address compliance with Security Rule standards.
Designate a security officer	• Ensure the designated security officer understands their responsibilities in developing and implementing the practice's security policies and procedures.
Authorizing access to ePHI	• Develop policies and procedures that address how persons are authorized to access ePHI based on the user's role and responsibilities (role-based access).

Implement Administrative Safeguards	
Provide ongoing training and monitoring	• Ensure all office staff members, physicians, and other workforce members undergo training on its security policies and procedures as necessary and appropriate for them to carry out their functions. Monitor staff member ePHI use and access, and implement appropriate corrective actions for any policy and procedure violations.
Implement data backup procedures for ePHI	• Establish and implement procedures that routinely backup ePHI. Ensure backup procedures allow for easy retrieval and recovery after events that damage systems containing ePHI.
Assess and reassess security policies and procedures	• Perform periodic assessments of the security management process, policies, and procedures to identify any new vulnerabilities and/or potential noncompliance with the Security Rule.
Maintain a written contract with all business associates	• Obtain a written contract or agreement with business associates that create, receive, maintain, or transmit ePHI. Ensure contracts include assurances of proper ePHI safeguards and HIPAA-compliant products.
Ensure comprehensive EMR vendor contract is in place	• Ensure the EMR vendor contract clearly defines the vendor responsibilities and assurances that the products are HIPAA compliant. • For more information on EMR vendor contracts, see the ***Medical Records: Electronic*** chapter.

Implement Physical Safeguards	
Implement facility access controls	• Implement policies and procedures that safeguard the facility and equipment from unauthorized physical access, tampering, and theft. Implement appropriate control measures (e.g., locked doors, signs restricting access, alarms, identification numbers, and security cables on computers).
Maintain maintenance records	• Document and maintain records of repairs and modifications related to the facility's physical security of its ePHI (e.g., hardware, walls, doors, locks).

Implement Physical Safeguards	
Protect workstations	• Develop policies and procedures that address the security measures to protect workstations with ePHI (e.g., privacy screens, password protected screen savers, automatic log offs).
Implement device and media controls and disposal	• Develop policies and procedures for controlling and disposing any devices, hardware, equipment, and media used in the practice.
Maintain inventories and logs	• Maintain a complete and current inventory of computers, servers, storage devices, office equipment, and medical devices that contain ePHI. Keep logs of devices and equipment that include serial number, location (on the network and in the facility), and purchase and upgrade dates.
Sanitize prior to disposal	• When taking equipment out of service, sanitize or destroy the internal memory and dispose of the equipment appropriately. ○ Refrain from storing old computers, drives, and servers prior to sanitation. ○ For high-capacity devices (e.g., servers, laptops, and external hard drives) use a vendor or professional for sanitization. Request a certificate of sanitization or other proof of sanitization and destruction. ○ For medical devices, contact the manufacturer to determine the most effective means to sanitize the memory. ○ For small portable media (e.g., CD, USB flash drives, memory cards, SIM cards), recognize that complete destruction, such as shredding or pulverizing, is the preferred method of destruction.[10] ○ Sanitize legacy magnetic storage devices (e.g., tapes and floppy discs) by degaussing. Consider using a professional for degaussing, as it requires specific equipment and skill. If you choose to destroy magnetic devices by incineration, use a licensed facility.

Implement Physical Safeguards	
Erase internal memory before equipment or medical device is removed	• Evaluate all office equipment and medical devices with internal memories for memory content and ePHI before they leave the practice. Ensure that an experienced IT professional erases the internal memory before equipment or device is returned to a vendor, discarded, sold, or donated.
Manage copiers	• Assign IT staff member(s) to manage and maintain digital copiers. Ensure network copiers are included in data loss prevention and intrusion detection strategies. Consider the following: ○ Encrypting and password protecting copiers. ○ Including or adding an overwriting capability when purchasing or leasing copiers, as overwriting renders the information residing in the hard drive/memory cache unusable. Recognize that overwriting is more secure than deleting, as information cannot be recovered after overwriting. ○ Overwriting the hard drive on a regular basis, e.g., monthly.[11] Identify and implement security measures to address vulnerabilities.
Sanitize smartphones	• For information on sanitizing smartphones, see the ***Communication: Electronic*** chapter or the NIST Draft Special Publication 800-88 Revision 1 Guidelines for Media Sanitation at http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf.

Implement Technological Safeguards	
Assign unique user identifier	• Assign a unique user identifier to each person that has been granted access to systems with ePHI. Ensure the identifier allows for tracking the user's activity within information systems. • Implement an automatic logoff feature that terminates an electronic session after a set time of inactivity to ensure unauthorized users do not access the workstation.

Implement Technological Safeguards	
Assign password to authenticate user	• Assign a password or PIN to each user to ensure the person seeking access is verified. • Monitor user access to ePHI. Ensure timely inactivation of users when terminated, and re-evaluate access needs when changes in position occur.
Protect ePHI being transmitted	• Encrypt all ePHI transmitted between your office and outside organizations. Depending on the size of the practice, use alternative methods such as password protecting documents or files containing ePHI or prohibiting ePHI transmission via email.
Protect integrity of data stored in the EHR	• Develop and implement measures to protect health record accuracy. At a minimum, policies and procedures should address: ○ Locking patient visit notes and progress notes no later than 48 hours after the date of service. ○ Ensuring authorship integrity of multiple authors, retaining all signatures so each entry is unambiguously identified. ○ Requiring amendments, addendums, and late entries to be clearly labeled as such and date stamped with the date actually made. ○ Avoiding using features that create cloned documentation, such as copy/paste, "make me the author," demo recall that copies forward data, replicating information from previous visits, or using smart phrases. • Install and update security systems and prevention measures for unauthorized access to patient information (e.g., anti-virus software). Prohibit the installation of any unapproved software.

References:

1. Beazley. *Beazley 2018 breach briefing*. p. 13. https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf
2. U.S. Department of Health & Human Services, Office of Civil Rights (OCR), The HIPAA Privacy and Security Rules, Summary of the HIPAA Security Rule, accessed 6/12/2018 https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
3. Ibid.
4. Richard Kissel, Andrew Regenscheid, Matthew Scholl and Kevin Stine, Guidelines for Media Sanitization, NIST Special Publication 800-88, Revision 1, December 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf,
5. Ibid.
6. Ibid, p. iv.
7. Ibid, pp. 27-40.
8. U.S. Department of Health & Human Services, Office of Civil Rights (OCR), The HIPAA Privacy and Security Rules, Summary of the HIPAA Security Rule, accessed 6/12/2018 https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
9. Beazley. Beazley 2017 breach briefing. p. 8. https://www.beazley.com/documents/Whitepapers/201707-beazley-breach-briefing.pdf
10. Richard Kissel, Andrew Regenscheid, Matthew Scholl and Kevin Stine, Guidelines for Media Sanitization, pp. 27-40.
11. Ibid.

Additional Resources:

U.S. Department of Health & Human Services, Office of Civil Rights (OCR), The HIPAA Privacy and Security Rules, *Frequently Asked Questions about the Disposal of Protected Health Information*, n.d., accessed 10/31/2018
https://www.hhs.gov/hipaa/for-professionals/faq/disposal-of-protected-health-information/index.html

U.S. Department of Health & Human Services, Office of Civil Rights (OCR), The HIPAA Privacy and Security Rules, *Security Rule Guidance Materials,* accessed 6/12/2018
https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html