The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Version 1.0 022112

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in HealthIT

www.HealthIT.gov

Chapter 2:

Privacy & Security and Meaningful Use

Meaningful Use[3](MU) criteria make it virtually certain that eligible providers (EPs) need to have an Internet connection. To facilitate electronic exchange of patient information, submit claims electronically, generate electronic records for patients' requests, or e-prescribe, an Internet connection is a necessity, not an option. Basic cyber security practices are needed to protect the confidentiality, integrity, and availability of electronic health record (EHR) systems, regardless of how they are delivered—whether installed in a provider's office or accessed over the Internet.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security requirements are embedded in the Medicare and Medicaid EHR Incentive Programs through the following meaningful use requirements. To fulfill requirements of Stage 1 of Meaningful Use[4], eligible providers need to "attest" that they have met certain measures or requirements regarding the use of the EHR for patient care. The attestation is effectively a confirmation or statement on the part of the provider that (s)he has met those requirements.

For privacy and security, the following are the requirements for Stage 1 of Meaningful Use:

- Core Objective & Measure 12[5]: Provide patients with an electronic copy of their health information, upon request.
  - More than 50 percent of all patients who request an electronic copy of their health information are provided it within three business days.
- Core Objective & Measure 15[6]: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
  - Conduct or review a security risk analysis in accordance with the requirements under the HIPAA Security Rule (45 CFR 164.308(a)(1) (ii) (A)) implement security updates as necessary and correct identified security deficiencies as part of the risk management process.

These Meaningful Use requirements are not intended to supersede or substitute for compliance required under HIPAA. If you are a covered entity, you are still required to comply with the HIPAA Privacy and Security Rules.

The Centers for Medicare & Medicaid Services has also launched a new comprehensive tool, An Introduction to the Medicare EHR Incentive Program for Eligible Professionals[7] , to help guide eligible providers through all of the phases of the Medicare EHR Incentive Program—from eligibility and registration to attestation and payment.

3 http://www.healthit.gov
4 https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp
5 http://www.cms.gov/EHRIncentivePrograms/Downloads/12ElectronicCopyofHealthInformation.pdf
6 http://www.cms.gov/EHRIncentivePrograms/Downloads/15_Core_ProtectElectronicHealthInformation.pdf
7 https://www.cms.gov/EHRIncentivePrograms/Downloads/Beginners_Guide.pdf

Stage 1 Objective	Stage 1 Measure	Description of HIPAA Requirement
#12. Provide patients with an electronic copy of their health information (including diagnostics test results, problem list, medication lists, medication allergies) upon request.	More than 50 percent of all patients who request an electronic copy of their health information are provided it within three business days.	Access. Under the HIPAA Privacy Rule, patients have a right to view and obtain a copy of their protected health information (PHI) in your designated record set, including information stored in your EHR.
#15. Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under the HIPAA Security Rule (45 CFR 164.308(a)(1)(ii)(A)) implement security updates as necessary and correct identified security deficiencies as part of the risk management process.	Under the HIPAA Security Rule, you are required to conduct a security risk analysis (45 CFR 164.308). Visit the Office for Civil Rights website for more information.

Core Measure 12

Assure You Comply with MU Privacy Requirements

As you adopt an EHR, make time to identify any gaps in how your practice fulfills its responsibilities for both the HIPAA Privacy Rule and other applicable laws. Privacy is the focus of the 4-step process discussed below, which complements the security risk analysis process that is emphasized in the 10-Step Plan for meeting Meaningful Use.

4-Step Privacy Process

1. Read about HIPAA Privacy Rule: Read about HIPAA Privacy Rule requirements. For example, does your Notice of Privacy Practices inform patients of their health information privacy rights?

2. Review Your State Privacy Laws: In many states, state agencies or professional associations have prepared an analysis of the interaction between state privacy law and the HIPAA Privacy Rule. This analysis is often referred to as a "HIPAA preemption analysis". You may want to contact your professional association to see whether such an analysis is available for your state.

3. Review Your Practice's Adherence to Federal and State Privacy Requirements: Please see the Privacy and Security Resources page for helpful information. Your Regional Extension Center (REC) may also have some resources for you to use.

After assessing, address any compliance gaps. For example,

- Consider other changes so your medical practice conforms to nationally accepted principles and state laws regarding patient privacy.

- Be aware that privacy and security requirements in the U.S. Department of Health and Human Services Office for Civil Right's (OCR's) forthcoming Health Information Technology for Economic and Clinical Health Act (HITECH) Modifications final rulemaking could change from the proposed requirements. Watch for the release of the final rule (sometime in 2012) via announcements from OCR, your associations, or in industry newsletters.

4. Anticipate and Address Patient Privacy Concerns: Be sure to anticipate the privacy concerns your patients may have as you digitize their health information. Reassure them that your EHR will help you safeguard their privacy. Patient relations on privacy and security issues should be an integral part of your overall patient engagement strategy

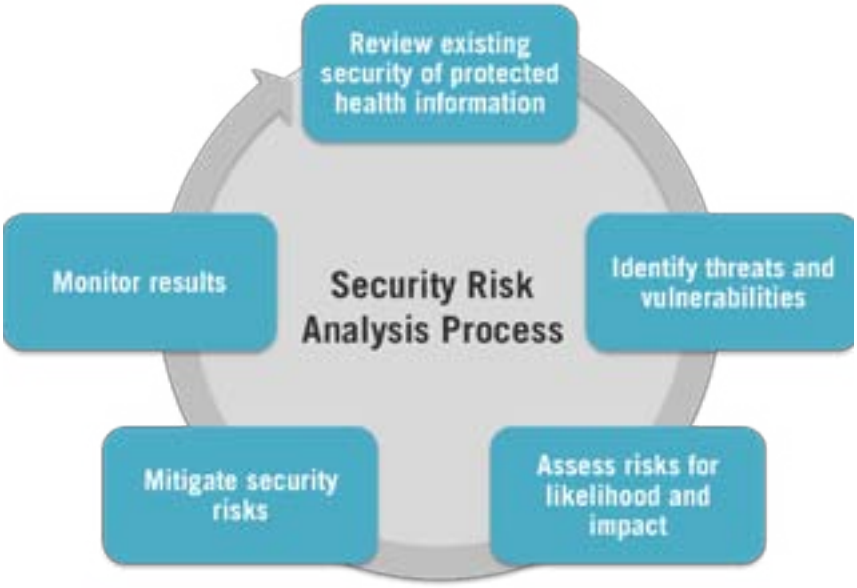
   Learn more about communicating with patients[8] about health information privacy.

Core Measure 15

Assure You Comply with MU Security Requirements

The figure to the right depicts a high-level security risk analysis process, the focus of the Meaningful Use Core Measure 15. The "risks" that you will be analyzing and managing refer to:

- Security vulnerabilities (e.g., user access controls are not properly configured, allowing staff to inappropriately view patient health information).
- Threats to protected health information (e.g., theft of portable device that stores or can access patient information).



This means that you must perform a security review of your electronic health care system and correct any practice that might make your patients' information vulnerable.

A security update could be updated software, changes in workflow processes or storage methods, new or updated policies and procedures, staff training, or any other necessary corrective action that needs to take place to eliminate security deficiency or deficiencies identified in the risk analysis.

Identify Risks to Your Medical Practice

Protecting patient information has two phases: initiation and maintenance. Initiating a set of safeguards requires a security risk analysis, which identifies and prioritizes risks so that a risk mitigation strategy can be formulated and applied. Afterward, the risk management strategy must be maintained through an ongoing, cyclical process of

8 http://www.healthit.gov/patients-families

reviewing existing security measures, identifying new risks and re-assessing previously identified risks, planning ways to mitigate risks, and monitoring and evaluating results.

To learn more about security risk analysis, download Chapter 3 of the full guide.

What Is a Security Risk Analysis?

To make a simplistic medical analogy, a security risk analysis is the examination and testing you do to assess clinical risk and diagnose a condition. Just as you use a diagnosis and other clinical data to plan treatment, you will use the risk analysis to create an action plan to make your practice better at protecting patient information. Further, privacy and security are like chronic diseases that require treatment, ongoing monitoring and evaluation, and periodic adjustment.

A security risk analysis is a systematic and ongoing process of both:

- Identifying and examining potential threats and vulnerabilities to protected health information in your medical practice.
- Implementing changes to make patient health information more secure than at present, then monitoring results (i.e., risk management).

The HIPAA Security Rule requires covered entities to conduct a risk analysis to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk analysis is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk analysis guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk analysis is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]."

Providers should develop a risk analysis that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

For more information, view OCR's guidance on risk analysis.[9]

As a covered health care provider, you ultimately retain responsibility for HIPAA compliance, including the security risk analysis. You have several options for completing your risk analysis, including enlisting the assistance of REC staff, hiring an outside professional, or doing it yourself, but whichever method you choose, you can expect that the security risk analysis will require your direct involvement.

To learn more, visit the Privacy and Security Resources page for more information.

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

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 MU 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.
I have to outsource the security risk analysis.	False. It is possible for small practices to do risk analysis themselves using self-help tools such as the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's (ONC) risk analysis tool. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
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.
There is a specific risk analysis method that I must follow.	False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.
My security risk analysis only needs to look at my EHR.	False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.
I only need to do a risk analysis once.	False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173.
Before I attest for an EHR incentive program, I must fully mitigate all risks.	False. The EHR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period.
Each year, I'll have to completely redo my security risk analysis.	False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks.

Mitigate Risks to Your Medical Practice

Risk Management Entails Five Security Components

Your security infrastructure should have five components, whereby, the HIPAA Security Rule outlines specific requirements. The following table briefly outlines each component and provides examples.

5 Security Components for Risk Management		
Security Components	**Examples**	**Examples of 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 assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Breach notification and associated policies • Business associate agreements	• Agreement review and updates

For any single risk, a combination of safeguards may be necessary because there are multiple potential triggers. For example, assuring continuous access to patient information may require adding a power surge protection strip, putting the server in a locked room, and being meticulous about backups.

Learn more about these requirements through the HHS HIPAA Security Rule Educational Paper Series[10] and the Cybersecurity Video

For tools to assist you today, please visit the ONC Privacy and Security Resources

10 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Health Information Security Quick Tips

Some good practices that can help you meet your security requirements include:

- Prevent Unauthorized or Inappropriate Access: Issue unique user names and passwords to everyone who will use the EHR (if accessed this way) to help prevent unauthorized or inappropriate access to patient information and system controls. If your EHR has the capability, associate access levels with specific roles (e.g., "attending physician", "medical assistant").
- Use Encryption Technology: Whether an EHR is locally installed or accessed over the Internet, encryption technology can protect patient health information from being read by unauthorized parties when it is transmitted, or stored on any device, including mobile devices. Encrypting PHI puts information in a coded form that can only be read by an authorized user who has a "key."
- Backup Your System: To keep information available when and where it is needed, plan for backing up your EHR system and recover the system in the event of an incident, such as fire, cyber-attack, or natural disaster.

The Threat of Cyber-Attacks

Most everyone has seen news reports of cyber-attacks against, for example, nationwide utility infrastructures or the information networks of the Pentagon. Health care providers may believe that if they are small and low profile, they will escape the attention of the "bad guys" who are running these attacks. Yet, everyday there are new attacks aimed specifically at small to mid-size organizations because they are low profile and less likely to have fully protected themselves. Criminals have been highly successful at penetrating these smaller organizations, carrying out their activities while their unfortunate victims are unaware until it is too late.

Our Own Worst Enemy

Even though cyber-attacks from hackers and other criminals are popular news stories, research indicates that often times, well-meaning computer users can be their own worst enemies because they fail to follow basic safety principles. This might be due to lack of training, time pressures, or any of a range of reasons.

ONC's CyberSecurity Checklist[11] shows you 10 simple best-practices that can be taken to reduce the most important threats to the safety of EHRs. This core set of best practices was developed by a team of cybersecurity and health care subject matter experts to address the unique needs of small health care practices. They are based on a compilation and distillation of cybersecurity best practices for smaller organizations.

- The information contained in this checklist is not intended to serve as legal advice nor should it substitute for legal counsel. The material in is designed to provide information regarding best practices and assistance to REC staff in the performance of technical support and implementation assistance. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

For more information on how to use this checklist, contact your local REC[12].

11 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
12 http://healthit.hhs.gov/cybersecurity