The Office of the National Coordinator for
Health Information Technology

Guide to Privacy and Security of Health Information

Version 1.2 060112

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

Guide to Privacy and Security of Health Information

The Office of the National Coordinator for Health Information Technology

Contents

Contents

The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Chapter 1:

What Is Privacy & Security and Why Does It Matter?

Version 1.2 060112

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 1:

What Is Privacy & Security and Why Does It Matter?

In your medical practice, patients are unlikely to share sensitive information unless they trust that you will honor their confidentiality. As you know, patients who trust their health information will be kept private and secure will be more willing to discuss their symptoms, conditions, and past and present risk behaviors.

Why Does Privacy & Security Matter?

Your patients trust you. Trust is clinically important and a key business asset. How your practice handles patient information is an important aspect of this trust. To help cultivate patients' trust, you:

- Make sure patients can request access to their medical record;
- Carefully handle patients' health information to protect their privacy; and
- Keep the information in patients' individual records as accurate as possible.

> Good patient care means safe record-keeping practices. Do not forget that an EHR represents a unique and valuable human being: it is not just a collection of data that you are guarding – it's a life.

Protecting patients' privacy and securing their health information is a core requirement for the Medicare and Medicaid Electronic Health Record (EHRs) Programs[1]. The Medicare and Medicaid EHR Incentive Programs are referred to as the "Meaningful Use Programs" throughout this document. Further, effective privacy and security measures protect your clinical practice from civil and criminal penalties[2]. Currently, your practice may have some privacy and security measures in place, such as private exam rooms, a notice of privacy practices, or a secure way to transmit patient information for billing.

Ensuring privacy and security of health information, including information in electronic health records (EHR), is the key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.

> Adopting an EHR and electronically sharing patient health information with other providers creates both new risks and new ways to secure information.
>
> Updating your privacy and security practices can be manageable and affordable, but it will require a sustained effort.

Your practice, not your EHR vendor, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR and comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and CMS[3] Meaningful Use Requirements.

1 http://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf
2 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
3 http://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf

The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Chapter 2:

Privacy & Security and Meaningful Use

Version 1.1 022312

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[4] (MU) criteria make it virtually certain that eligible professional (EPs) need to have an Internet connection. The intent of this meaningful use discussion is to provide information pertaining to eligible professionals. Please see the CMS flow chart for assistance with determining if you are an eligible professional. For information about meaningful use requirements pertaining to eligible hospitals and critical access hospitals (CAH), please see the relevant CMS guidance.

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 health information in electronic health record (EHR) system, 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[5], eligible professionals 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 eligible professional 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[6]: 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[7]: 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 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its 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. This guide's references to HIPAA requirements pertain to pre-Health Information Technology for Economic and Clinical Health Act (HITECH) final rulemaking.

4 https://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf
5 https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp
6 http://www.cms.gov/EHRIncentivePrograms/Downloads/12ElectronicCopyofHealthInformation.pdf
7 http://www.cms.gov/EHRIncentivePrograms/Downloads/15_Core_ProtectElectronicHealthInformation.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 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.	Under the HIPAA Security Rule, you are required to implement policies and procedures to prevent, detect, contain, and correct security violations (45 CFR 164.308). Visit the Office for Civil Rights website for more information.

The Centers for Medicare & Medicaid Services has also launched a new comprehensive tool, An Introduction to the Medicare EHR Incentive Program for Eligible Professionals[8], to help guide eligible professional through all of the phases of the Medicare EHR Incentive Program—from eligibility and registration to attestation and payment.

Core Measure 12

Assure You Comply with MU Privacy Requirements

CMS operates the Meaningful Use Programs. Please refer to the official requirements for the Meaninguful Use Programs when structuring your compliance program. The information and tips below are some suggested ways of approaching these areas.

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[9] 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)[10] may also have some resources for you to use.

8 https://www.cms.gov/EHRIncentivePrograms/Downloads/Beginners_Guide.pdf
9 http://www.healthit.gov/providers-professionals/ehr-privacy-security/10-step-plan
10 http://www.healthit.gov/REC

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

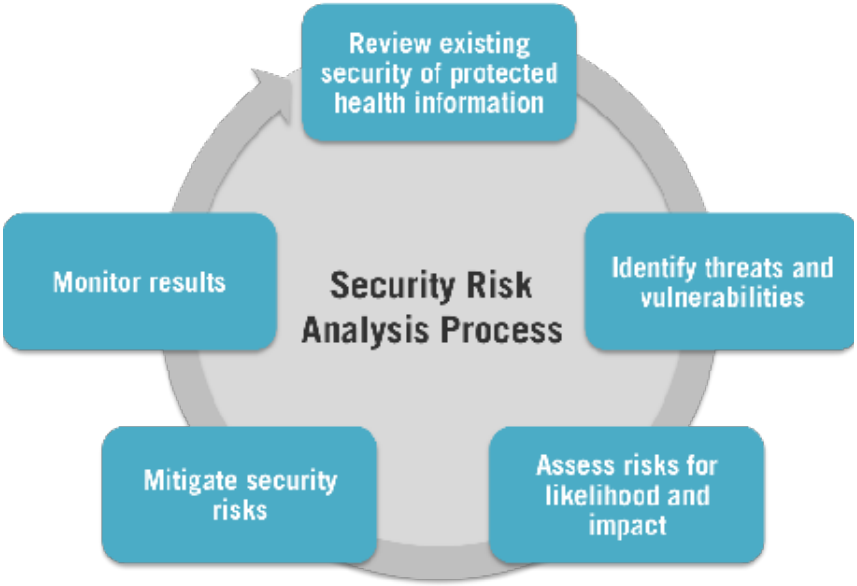
   Learn more about communicating with patients[11] about health information privacy.

Core Measure 15

Assure You Comply with MU Security Requirements

CMS operates the Meaningful Use Programs. Please refer to the official requirements for the Meaninguful Use Programs when structuring your compliance program. The information and tips below are some suggested ways of approaching these areas.

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

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

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 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[12].

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.

12 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. 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 the Reassessing Your Security Practice in a Health IT Environment.
Before I attest for an EHR incentive program, I must fully mitigate all risks.	**False.** The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.
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. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.

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

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[13] and the Cybersecurity Video[14].

For tools to assist you today, please visit the Privacy and Security Resources[15].

13 http://www.healthit.gov/providers-professionals/regional-extension-centers-recs
14 http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__cybersecurity/3696
15 http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

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[16] 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 was originally 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 in the document.

For more information on how to use this checklist, contact your local REC[17].

16 http://healthit.hhs.gov/pdf/cybersecurity/Basic-Security-for-the-Small-Healthcare-Practice-Checklists.pdf
17 http://www.healthit.gov/providers-professionals/regional-extension-centers-recs

The Office of the National Coordinator for Health Information Technology

Guide to

Privacy and Security of Health Information

Chapter 3:

10 Step Plan for Meeting Privacy and Security Portions of Meaningful Use

Version 1.2 060112

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 3:

10 Step Plan for Meeting Privacy and Security Portions of Meaningful Use

Before you get started, check with your local Regional Extension Center (REC)[18] about where you can get help beyond the resources in the Privacy and Security Resources[19] section of the website. Work with your electronic health record (EHR) vendor(s) letting them know that health information security is one of your major goals in adopting an EHR. Practice staff and any other partners that you have can also help you fulfill your Health Insurance Portability and Accountability Act of 1996 (HIPAA) responsibilities.

An EP must meaningfully use certified EHR technology for an EHR reporting period, and then attest to CMS that he or she has met meaningful use for that period. Start your 10-step process at least 90 days before you begin the EHR reporting period.

This is not intended as a statement of meeting Meaningful Use (MU) standards; this is one suggested organized process to address the various components.

Privacy & Security 10-Step Plan for Meaningful Use

Step 1: Confirm You Are a "Covered Entity"

Most health care providers are covered entities, and thus, have HIPAA responsibilities for individually identifiable health information. The U.S. Department of Health and Human Services (HHS) tool can help you confirm if you are a covered entity[20].

Step 2: Provide Leadership

Your leadership—especially emphasizing the importance of protecting patient information—is vital to your privacy security activities. For example, HIPAA requires covered providers to designate both a privacy and a security officer on their staff. In a very small practice, you may have to assume both responsibilities.

18 http://healthit.gov/rec
19 http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
20 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

Your security officer should be able to work effectively with others to safeguard patient information. At various times, the officer will need to coordinate with your privacy officer (if a different person), practice manager, IT administrator or consultant, and your EHR vendor.

Subsequent actions are:

- Designate a privacy and security officer. This person will be responsible for developing and maintaining your privacy and security practices to meet HIPAA requirements. This person should be part of your EHR adoption team and be able to work effectively with others. In a very small practice, you may be the privacy and security officer or your practice manager may carry both roles. Be sure to:
  - Record the assignment in a new security documentation file, even if you are the officer.
  - Discuss your expectations and their accountability. Note that you, as a covered health care provider, retain ultimate responsibility for HIPAA compliance.
  - Enable your designated security person to develop a full understanding of the HIPAA Rules so (s)he can succeed in his/her role.
- Explore HIPAA security requirements with your EHR vendor. What security functions does the EHR/Health IT product offer? If you have implemented an EHR, what are the current settings of those functions? What is the vendor's pricing for training staff on those functions, developing relevant policies and procedures, and correcting security-setting deficiencies in the EHR system?
- Select a qualified professional to assist you with the security risk analysis. Your security risk analysis must be done well, or you will lack the information necessary to effectively protect patient information. Note that doing the analysis in-house may require an upfront investment developing a staff member's knowledge of HIPAA and electronic information security issues. Use this opportunity to have your staff learn as much as possible about health information security.

  You however, can conduct the risk analysis yourself. Just as you contract with professionals for accounting, taxes, and legal counsel, so, too, outsourcing the security risk analysis function can make sense. RECs often provide this direct support. Another source of assistance may be your state or local medical association, or other professional medical association.

  If you need to, outsource this to a professional, a qualified professional's expertise and focused attention will yield quicker and more reliable results than if your staff does it piecemeal over several months. The professional will suggest cost-effective ways to mitigate risks so you do not have to do the research yourself and evaluate options. You are still ultimately responsible for the security risk analysis even if you outsource this function.

  Talk to several sources of potential assistance. If you contract with a professional, ONC recommends that you use a professional who has relevant certification, and direct experience tailoring a risk analysis to medical practices with a similar size and complexity as yours.
- Use a checklist as a security risk preview. Have your security officer or security risk professional performing the risk analysis use a checklist to get a preliminary sense of potential shortcomings in how your practice protects patient information. A single checklist does not fulfill the security risk analysis requirement, but the checklist will help everyone get ready for needed improvements.

Keep the results as part of your documentation (see Step 3).

- Continue to refresh your knowledge base. Learn about HIPAA, state laws, and other privacy and security requirements that also require compliance.
- Promote culture of protecting patient privacy. "Culture" means creating an overall atmosphere in your office that is protective of patients' information. Culture sets the tone.
    - Constantly communicate through your actions as you comply with, implement, and enforce your privacy and security policies and procedures. Second, remind staff why securing patient information is important to patients and the medical practice.

Over time, protecting privacy will become ingrained into all aspects of your practice operations. Further, your patients will feel and sense that you are safeguarding their health information.

Where to Find Help

Your local REC may offer:

- Direct support with conducting the security risk analysis, training staff, and risk mitigation.
- Guidance, information resources, and tools.
- A list of professionals qualified to conduct security risk analyses.

Also, your REC or your membership associations may know of training resources. Training may be available through your local community college.

The Privacy and Security Resources page provides some useful education materials.

Certification in Health Information Security

Two examples of certification are:

- Certified in Healthcare Privacy and Security (CHPS)
- Certified Professional in Healthcare Information and Management Systems (CPHIMS)

Step 3: Document Your Process, Findings, and Actions

The Centers for Medicare & Medicaid Services (CMS) within HHS advise all providers that attest for the EHR incentive programs to retain all relevant records that support attestation. Thus, faithfully record all your practice decisions, findings, and actions related to safeguarding patient information. These records will be essential if you ever are audited for compliance with HIPAA[21] or an EHR incentive program.

Documentation shows why and where you have security measures in place, how you created them, and what you do to monitor them. Create a paper or electronic folder for your records.

The HHS Office for Civil Rights (OCR) and state attorneys general investigate HIPAA complaints; OCR conducts audits[22] for HIPAA privacy and security rule compliance. Providers in the CMS EHR incentive programs may also receive a random audit from CMS to determine if they actually conducted the security risk analysis and implemented adequate safeguards.

Records about how you did the security risk analysis and acted on the results would inform an audit.

Examples of Records for Your Privacy and Security Documentation Folder

Contents should include, but not be limited to:

- Completed checklists
- Security risk analysis report
- Risk management action plan
- Agreements for business associates
- Trainings for staff and any associated certificates
- EHR logs that show utilization of security features and monitor user actions
- Your policies and procedures

Also, this documentation should help you run your practice efficiently. You will eventually have a master record of security findings, decisions, and actions that your workforce can reference instead of trying to reconstruct from memory and scattered bits of information.

Step 4: Conduct Security Risk Analysis

Conduct a security risk analysis (or reassessment if you already conducted a risk analysis) that compares your current security measures to what is legally and pragmatically required to safeguard patient information. The risk analysis also identifies high priority threats and vulnerabilities.

OCR has issued Guidance on Risk Analysis[23]. The U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) has issued a security risk assessment tool[24] that offers a set of questions tailored to small practices that can help you get started on a risk analysis[25].
A security risk professional can plan and implement this process, but you will want to know what to expect.

21 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
22 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
23 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
24 http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures/protect-electronic-health-information
25 http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures/protect-electronic-health-information

The first time you conduct a risk analysis:

- Review the existing security infrastructure in your medical practice against legal requirements and industry best practices. An optional analysis is to assess how well your medical practice currently fulfills nationally accepted principles for data stewardship.
- Identify potential threats to patient privacy and security vulnerabilities and assesses the potential impact if that what-if occurred.
- Prioritize risks for action based on the likelihood of specific risks and their potential impacts on patients, the practice, and others.

Follow a specific process in conducting the risk analysis so that you consider all potential threats and vulnerabilities. The process does not need to be formal (e.g., that you used a specific tool), but it should be systematically approached so it covers all security risks.

Make sure your risk analysis examines risks specific to your situation, including if your EHR is based in your office or Internet-based. The latter you may also know as "cloud computing" or "application service provider (ASP).

What to Expect

- Each step will require bringing your security team together and deciding who will be responsible for what component.
- You will finish the risk analysis, but then need to use the information to create and implement an action plan.
- Periodically – at least annually – you will need to return to the risk analysis report and reassess.
- The risk analysis can produce murky results. However, you will be able to see where you are meeting, not meeting, or exceeding HIPAA requirements.
- The risk analysis process is ongoing. There is no simple checklist that you can use to know that your security process is "done" or sufficient.
- Federal, state, and privacy and security requirements will continue to evolve.

Security Risks in Office-Based vs. Internet-Hosted EHRs

Both office-based (locally-hosted) and Internet-hosted (remotely-hosted) EHRs have features that enable your practice to better control access to and use of protected health information than was available with paper medical records. On the other hand, both EHR types also introduce new risks to your patients' information. The mix of security risks relates, in part, to your EHR type.

The table on the next page offers a few examples of different risks associated with office-based vs. Internet-hosted EHRs.

Examples of Potential Information Security Risks with Different EHR Hosts	
Office-Based EHRs	Internet-Hosted EHR
Natural disaster could greatly disrupt availability of, and even destroy, protected health information.	The vendor controls many security settings, the adequacy of which may be hard to assess.
The security features on your office-based EHR may be less sophisticated than an Internet-hosted EHR.	Your data may be stored outside the U.S. Other countries have different health information privacy & security laws that may apply to data mantained in such country.
You directly control the security settings.	You are more dependent on the reliability of your Internet connection.
When public and private information security requirements change, you have to figure out how to update your EHR to comply and work out any bugs.	In the future, the vendor might request extra fees to update your EHR for compliance as federal, state, and private information security requirements evolve

Free do-it-yourself tools for the security risk analysis are available on the Privacy and Security Resources[26] page, and some RECs[27] provide this service or can provide additional tools. Look for tools that are suitable to your practice in terms of scale and terminology. Some commercial security risk analysis products are now available; before buying one, seek out an independent review from a health information security expert. Be sure to involve your EHR vendor, beginning with some basic questions.

Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program. A risk analysis should also be done when a major change occurs to your practice or electronic system, such as your decision to participate in a health information exchange (HIE)[28]. Annual reassessments will take less time and effort than the original full risk analysis. Review and update the prior analysis for changes in risks. Reassessments will take less time and effort than the original full risk analysis. Review and update the prior analysis for changes in risks.

Step 5: Develop an Action Plan

Using your risk analysis results, discuss and develop an action plan to mitigate the identified risks. The plan should have five components: administrative, physical, and technical safeguards; policies and procedures; and organizational standards. Often, basic security measures can be highly effective and affordable.

Your action plan is informed by your risk analysis and should focus on high priority threats. Take advantage of the flexibility that you have to right-size security measures to your specific practice characteristics. It is important that your security be right-sized so the plan is feasible and affordable for your practice.

Your action plan should have at least any combination of the five required components, which are addressed in Steps 3 and 6-9. Although the steps are sequential, the security components are interrelated. Begin with identifying the easy actions that can reduce the greatest risks.

26 http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147
27 http://www.healthit.gov/rec
28 http://healthit.hhs.gov/portal/server.pt?open=512&objID=1488&mode=2

To develop your action plan, your staff that has been designated as being responsible for security should schedule time together to prioritize actions and structure into steps. Once the plan is written, your designated security staff will need to continue to meet periodically to coordinate actions, work through unexpected snags, and track progress. If your staff is unsure of how specific HIPAA requirements might apply to your specific practice, review OCR specific guidance or other materials in the Privacy and Security Resources[29]. Also, you could seek guidance from your legal counsel or a security risk professional.

Last but not least, reward your team as it achieves milestones. Also, understand that you will not be able to eliminate risk, but you will be able to lower it.

Step 6: Manage and Mitigate Risks

Begin implementing your action plan. Develop written and up-to-date policies and procedures about how your practice protects e-PHI. Retain outdated policies and procedures. Do not lose sight of basic security measures, some of which can be low-cost and highly effective

Your EHR vendor can help you use the security functions in your certified EHR[30].

This step is focused on implementing your action plan, especially three parts:

- Information security settings in your EHR
- Written policies and procedures
- Continuous monitoring of your security infrastructure

The goal is to protect patient information through ongoing efforts to identify, assess, and manage risks.

Above all, integrate information security into your practice routines and create a culture of continually safeguarding patient information.

Remember the Basics

- Is your server in a room only accessible by authorized staff? Do you keep the door locked?
- Are your passwords easily found (e.g., taped to a monitor)? Easy to guess?
- Do you have a fire extinguisher that works?
- Where, when, and how often do you back-up? Is at least one back-up kept offsite? Can your data be recovered from the back-ups?
- How often is your EHR server checked for viruses?
- Who has keys to your building? Any former employees or contractors?
- What is your plan for what to do if your server crashes and you cannot directly recover data? Do you have documentation about what kind of server it was, what software it used, etc.?

29 http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147
30 http://healthit.hhs.gov/CHPL

Information Security Settings in Your EHR

A certified EHR assures that your new system has a package of core technical security functions[31]. However:

- Certification does not guarantee performance or reliability of these security functions.
- The security functions may be "off" or the settings could be at a suboptimal level, either of which can create vulnerabilities.
- You and your staff should become familiar with the security settings in your EHR. Most of these are accessible to whoever has administrator privileges. Learning how to configure these settings, for example, will help when staff leave or join your practice. While nationally accepted standards on these configurations have not yet been developed, there are industry best practices. Your health information organization that facilitates electronic exchanges may have specific requirements.
- Your risk analysis should specifically examine the adequacy of your EHR security safeguards as it transmits, stores, and allows modifications to protected health information.
- You may need to contract with an information security expert at some point but you should first avail yourself of other sources, such as the REC for your area, Privacy & Security Resources, your EHR vendor, or your state or county medical association. These resources can assist you in assuring that your EHR security features are appropriately configured.

Written Policies and Procedures

Your policies and procedures guide how your practice operates on a day-to-day basis with respect to protecting patient information. HIPAA Privacy and Security Rules requires these to be written. Your REC consultant may have a sample manual.

To use as a guide, your medical practice policies and procedures should at least:

- Establish protocols for all of your security components (administrative, physical, and technical safeguards).
- Recognize individual privacy rights and specify processes for fulfilling these responsibilities.
- Instruct your workforce on what to do when something happens that impairs the availability, integrity, or confidentiality of protected health information. (Sometimes called incident response or management plans.)
- Specify a process and sanction policy for breach notification.
- Detail enforcement, starting with the use of your EHR security logs to monitor access to and use of protected health information. Your sanction policy must be applied equally and as written.

Once your written policies and procedures are in place, HIPAA requires that you:

- Train staff (see Step 7) on what is required and how to implement the policies and procedures. HIPAA requires that your workforce be specifically trained on your medical practice's policies and procedures for breach notification.

31 https://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf

- Consistently apply the policies and procedures when unauthorized access occurs. Staff members who do not comply with your breach notification policies and procedures must be sanctioned. Document your actions.
- Periodically review your policies and procedures and make sure they are still current and your practice is adhering to them.
- Update your policies and procedures when your internal or external environment changes, creating new risks.
- Retain policies and procedures for six years after you have updated or replaced them. State and private requirements may specify a longer time period.

Continuous Monitoring of Your Security Infrastructure

In the security risk analysis illustration (see Chapter 3, or download the entire guide here) the "monitor results" is the process of reviewing how well your security infrastructure works. The security risk analysis provides feedback that your practice needs for continuous improvement, documentation, and your annual analysis of security risks.

Monitoring results also relates to a HIPAA Security Rule requirement that you have audit controls and the capability to audit. Your audit controls and capabilities should be in scale with the size of your practice. (Note: in this context, "audit" is what you do to monitor the adequacy and effectiveness of your security infrastructure and make needed changes.)

Your certified EHR has a function to generate audit logs. This means it can record how protected health information is accessed, by whom, what the individual did, when, and for what purposes. Your EHR also can produce reports. Audit logs are useful tools for both holding your workforce accountable for protecting patient information and for learning about unexpected or improper modifications to patient information.

Have your security officer, IT administrator, and EHR vendor work together so your audit function is active and configured to your needs. They may want you to:

- Decide whether you will conduct the audits in-house, by an information security consultant, or a combination of the two.
- Determine what to audit and how the audit process will occur.
- Identify trigger indicators—or signs that protected health information could have been compromised and further investigation is needed.
- Establish a schedule for routine audits and guidelines for random audits.

Step 7: Prevent with Education and Training

To safeguard patient information, your workforce must know how to implement your policies, procedures, and security audits. HIPAA requires you as a covered provider to train your workforce (employees, volunteers, trainees, and contractors serving on your workforce) on your policies and procedures. Your staff must receive formal training on breach notification.

Reinforce workforce training with reminders. Lead by example in adhering to your policies and procedures.

Workforce education and training—plus a culture that values patients' privacy—are a necessary part of risk management.

Workforce Education and Training

You need your staff to adhere to your security policies and procedures and understand their roles and the potential consequences of not adhering to them. Your staff may need focused training to develop the requisite skills to perform the steps required.

Breach notification is a training component that HIPAA Privacy Rule specifically requires.

How Often?

Your practice may formally educate and train your workforce at least once a year and when your practice changes policies or procedures. It is particularly important that your staff be trained on how to respond to security incidents or an unauthorized disclosure of protected health information (PHI).

Make Protecting Patient Information Part of Your Routine

Deliberately create an operational culture that emphasizes patient confidentiality. Lead by example by complying with your practice policies and procedures. Speak often about the importance of trust in the patient-provider relationship and that patients expect your practice to be a good steward of their health information. Also:

- Continually remind staff to safeguard patient confidentiality and the security of protected health information.
- Make sure your staff has a copy of your policies and procedures for easy reference.
- Address staff questions.
- Reassess each workforce member's job functions and enable him/her to access only the minimum necessary health information as appropriate.

Step 8: Communicate with Patients

Your patients may be concerned about confidentiality and security of their health information in an EHR. Emphasize the benefits of EHRs to them as patients, perhaps using consumer education handouts that others have developed. Reassure them that you have a system to proactively protect their health information privacy. Good patient relations also mean you have policies and procedures for communicating with patients and caregivers if a breach[32] of unsecured protected health information (PHI) occurs.

Most patients trust their providers to keep their health information confidential, but some patients may worry about their privacy being compromised in EHRs and electronic sharing of their health information.

Don't surprise patients with your EHR adoption; instead, develop a four-part effort to:

- Communicate with patients about the security and confidentiality of their health information. This includes, but goes beyond your Notice of Privacy Practices[33].
- Address their individual health information rights, especially the right to access a copy of their electronic medical record.

32 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
33 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

- Educate patients about how their health information is used and may be shared outside your practice. In some cases, depending on state law and the nature of information you are sharing, you may need to obtain a patient's authorization or permission prior to exchanging their health information.
- Notify patients and caregivers when a breach of unsecured PHI has occurred (this is referred to as a breach notification), following your previously developed policies and procedures.

Patient relations on privacy and security issues should be an integral part of your overall patient engagement strategy[34].

Consumer communications should be culturally appropriate. Consider language, communication needs, and the level of trust that seems to exist between different patient populations and health care providers. If a population has some distrust of the medical establishment, then take extra steps to reassure them that you are safeguarding their information.

For concerned patients and their caregivers, be ready to guide them through the change. For ideas, see the Privacy & Security Informational Resources[35], which provides other materials for you and your patients.

Fulfill Your Responsibilities for Patients' Health Information Rights

In the future, expect more patients to ask how you handle their electronic health information. More patients will ask for their medical records, and some will want changes to their records.

To prepare for patient requests, ask your EHR vendor and REC consultant about ways to use your system to help you fulfill individual patient rights. A good place to start is focusing on the EHR incentive program objective of giving patients a copy of their electronic health information upon request. For example, walk through the steps of saving a patient's record on a mobile device such as a disc or jump/USB drive (which should be password protected or encrypted) as well as how to print out a patient's record. Ask your vendor to provide step-by-step instructions that include screen shots on how to perform these actions.

Once you have established a process and procedure on how patients can get a copy of their EHR, develop procedures for patients to ask you to modify their health information, restrict disclosure, and obtain a report about prior disclosures. (Patients' Individual Rights and Your Responsibilities section in Chapter 4 explains these legal rights.)

Online Communications with Patients

If you plan to interact with patients via online platforms (e.g., e-mail, a patient portal for your EHR, or social media) adhere to HIPAA requirements for protected health information. Check the Privacy & Security Resources[36] page for more information.

Step 9: Update Business Associate Agreements

Make sure your business associate[37] agreements require compliance with HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification requirements. This will require your business associates to safeguard protected health information they get from your practice, train their workforce, and adhere to breach notification requirements. OCR offers a sample business associate contract provisions[38].

34 http://www.healthit.gov/patients-families
35 http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
36 http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
37 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
38 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Health information organizations (HIOs) that facilitate the electronic exchange of individual patient information may also be considered business associates. Please see OCR's guidance pertaining to HIO[39].

If you electronically exchange protected health information with others, be sure your agreement with your health information organization is also up to date.

Organizational standards are a required HIPAA security component. First, make sure your written policies require all business associates that routinely access protected health information to comply with HIPAA and HITECH, including breach notification. These policies should also state how business associates are accountable. Next, update your agreements with your business associates to be compliant with existing and new standards.

Step 10: Attest for the Security Risk Analysis MU Objective

Providers can register for the EHR Incentive Programs anytime, but they can only attest after they have met the meaningful use requirements for an EHR reporting period. Only attest for an EHR incentive program, after you have fulfilled the security risk analysis requirement and have documented your efforts.

Do not attest for an EHR Incentive program[40] until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis. Document these changes.

When you attest to meaningful use, it is a legal statement that you have met specific standards, including that you protect electronic health information. Providers participating in the EHR Incentive Program can be audited.

If you attest prior to actually meeting the meaningful use security requirement, you could increase your business liability for federal law violations and making a false claim. From this perspective, consider implementing multiple security measures as feasible, prior to attesting. The priority would be mitigating high-impact and high-likelihood risks.

39 http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf
40 http://www.cms.gov/EHRIncentivePrograms/Downloads/15ProtectElectronicHealthInformation.pdf

The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Chapter 4:

Integrating Privacy and Security into Your Practice

Version 1.2 060112

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 4:

Integrating Privacy and Security into Your Practice

Understanding Patients' Health Information Rights and Provider Responsibilities

Ensuring privacy and security of electronic health information is a key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to individually identifiable health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules protect the privacy and security of individually identifiable health information. Whether the information is on a computer, paper, or other media, you have responsibilities for safeguarding health information. The HIPAA Privacy Rule covers protected health information (PHI) in any medium, while the HIPAA Security Rule covers electronic protected health information (e-PHI). HIPAA Rules have detailed requirements regarding both privacy and security.

Your practice, not your electronic health record (EHR) vendor, is responsible for taking the steps needed to comply with HIPAA privacy, security standards, and the Centers for Medicare & Medicaid Services' (CMS') Meaningful Use requirements.

Read up on laws governing the privacy and security of health information. You must comply with all applicable federal, state, and local laws.

The HIPAA Privacy Rule

The HIPAA Privacy Rule[41] establishes a set of national standards for the use and disclosure of individually identifiable health information – often referred to as protected health information – by covered entities, as well as standards for providing individuals with privacy rights and helping individuals understand and control how their health information is used. HIPAA Privacy Rule requirements:

- Apply to most health care providers, including those who do not have EHRs or do not participate in a CMS EHR incentive program;
- Set a federal floor for protecting individually identifiable health information across all mediums (electronic, paper, and oral);
- Limit how covered entities may use and disclose individually identifiable health information they receive or create;
- Give individuals rights with respect to their protected health information, including a right to examine and obtain a copy of information in their medical records, and the right to ask covered entities to amend their medical record if information is inaccurate or incomplete;
- Impose administrative requirements for covered entities, such as training of employees with regard to the Privacy Rule; and
- Establish civil and criminal penalties.

41 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

Violations of the Privacy Rule may be enforced through imposition of civil and criminal penalties. Learn more about HIPAA enforcement[42].

Several central tenets of the Privacy Rule are:

- In general, you may use or disclose protected health information for treatment, payment, and health care operations without obtaining a patient's written permission. For other purposes, such as marketing, you may need to obtain an individual's authorization to use or disclose the patient's protected health information.
- Your agreements with business associates must explicitly require them to comply with HIPAA, including breach notification requirements.
- Generally, you and your business associates must limit your access to, use of, and disclosure of protected health information to the minimum necessary to carry out an action. This is called the "minimum necessary rule." There are several exceptions to this rule. For example, generally, you do not have to limit the disclosure of protected health information to the minimum amount necessary when you are disclosing the information for treatment of the individual.

Related Topics

- Complying with Privacy & Security Requirements

Resources

- HIPAA Requirements in detail (OCR)
- The Privacy Rule, in detail (OCR)
- The Security Rule, in detail (OCR)
- Customized, on-the-ground assistance to providers
- Privacy and Security Resources

Patients' Rights and Your Responsibilities

Under HIPAA, patients have legal, individual rights to access their health information and learn about disclosures of their health information. As their health care provider, you are responsible for respecting these rights.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) explains these rights and other requirements in its Summary of the HIPAA Privacy Rule[43].

As a covered entity, you have responsibilities to patients under the HIPAA Privacy Rule, including:

- Notice of Privacy Practices: Under the HIPAA Privacy Rule, covered entities must provide patients with full information on how their protected health information is used and disclosed. This is accomplished by giving patients a Notice of Privacy Practices that describes how an individual's information may be used or shared, specifies an individual's legal rights with respect to their protected health information held by the covered entity (many of which are described below), and the covered entity's legal duties.

42 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
43 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

- Patient access to their information: Patients have the right to inspect, review, and receive a copy of health information about themselves held by covered entities or business associates in a designated record set, which includes a health care provider's medical and billing records. Generally, these health plans and providers have to comply with requests for access within 30 days.
- Amending patient information: Patients have the right to request that covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendments to persons identified by the individual as having received the original information and in need of the amendment(s) as well as those entities that the covered entity itself identified as having received the original information who would be in need of the amendments due to their prior or foreseeable reliance on the original information to the detriment of the individual. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record.
- Accounting of disclosures: Individuals have a right to receive an accounting of disclosures, which is a listing of when a HIPAA covered entity has shared the individual's PHI with a person or organization outside of the entity. Accounting is only required for certain disclosure purposes. A covered entity must provide an accounting of disclosures made during the accounting period, which is six years immediately preceding the accounting request, but a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.
- Rights to restrict information: Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions; however, a covered entity must have a procedure to evaluate all requests. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Designated Record Set

A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

For more information about what a designated record set is, please see OCR's Health IT Guidance on Access[44].

HIPAA Limits on Using & Disclosing Patient Information

What types of information does HIPAA protect?

The Privacy Rule applies to all PHI[45] , which includes, when held or transmitted by a covered entity, information that:

- Relates to the individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and

44 http://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_access_medical_records/311.html
45 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

- Identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

Protected health information can be in any form—electronic, paper, or oral—and includes financial and demographic information collected from patients.

Is there any information that is not restricted by HIPAA?

HIPAA Rules do not govern the use or disclosure of health information that does not identify an individual (known as "de-identified" PHI). Once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or health information organization for any purpose (subject to any other applicable laws). You can share de-identified PHI, but just removing name, address, and social security number may NOT make information "de-identified[46]". The Privacy Rule designates two processes through which a covered entity can determine that protected health information is de-identified.

Also, the HIPAA Rules do not apply to a covered entity's own employment records, or to education-related and certain other records covered by the Family Educational Rights and Privacy Act (FERPA)[47].

What about patient information pertaining to behavioral health or substance abuse?

The HIPAA Privacy Rule protects individually identifiable behavioral health or substance abuse information that a covered entity collects or maintains in a medical record in the same way that it protects other PHI.

HIPAA is not the only federal law that impacts the disclosure of health information. In some instances, a more protective law may require an individual's permission to disclose health information where HIPAA would permit the informationto be disclosed without the individual's authorization. In addition, HIPAA permits State laws that offer greater privacy protection and are not contrary to continue to be applicable. State laws that are not more protective are pre-empted by HIPAA.

Do I need to inform my patients about how I use or disclose their health information?

Under the HIPAA Privacy Rule, covered entities must provide patients with a Notice of Privacy Practices[48] that specifies an individual's legal rights and the covered entity's legal duties with respect to the use and disclosure of PHI.

In addition to providing this notice to patients at the initial visit, a covered provider must make its notice available to any patient upon request.

Your practice has likely been using a Notice of Privacy Practices for several years now. If you need a template of an acceptable privacy practice, your REC or state or county medical association may be able to suggest some templates that comply with HIPAA requirements. Note that state and private sector requirements may necessitate adding other information to your notice. Plan to reassess your notice once OCR issues the final rule for the Health Information Technology for Economic and Clinical Health Act (HITECH) changes to HIPAA.

Please refer to OCR's website to learn more about the notice[49].

---

46 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html
47 http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
48 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html
49 http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html

How to Keep Your Patients' Health Information Secure

A new EHR alters the mix of security needed to keep patient health information confidential. A new EHR also brings new responsibilities for safeguarding your patients' health information in an electronic form.

To uphold patient trust as your practice adopts an EHR, and to comply with HIPAA and meaningful use requirements, covered providers must conduct a security risk analysis. The risk analysis process will lead you to systematically examine many aspects of your medical practice:

- Your EHR software and hardware
- Adequacy of your practice protocols
- Physical setting and environment
- Staff education and training
- EHR access controls
- Contracts with your business associates
- Patient relations and communications

If you do not generally use e-PHI, you will likely need to make changes in the above areas to comply with HIPAA and Meaningful Use requirements. Fortunately, properly configured, certified EHRs[50] can provide more protection to patient health information than that provided by paper:

- Unique passwords and user names help prevent unauthorized access to the system.
- User and role based access controls prevent inappropriate or unauthorized access to both patient information and system controls.
- Backup and recovery is essential to ensuring availability of patient information to providing consistency in care.
- Encryption protects patient health information in transmission and on mobile devices, and is often a limit on liability for breach purposes under HIPAA.
- Appropriate and properly installed wireless capability provides firewalls and encryption functionality to keep your practice network secure.

The HIPAA Security Rule

The HIPAA Security Rule[51] establishes national standards to protect individuals' electronic protected health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The HIPAA Security Rule requires providers to implement security measures, which help protect patients' privacy by creating the conditions for patient health information to be available, but not be improperly used or disclosed. These requirements apply only to e-PHI.

All health care providers considered "Covered Entities" under HIPAA (most are) are responsible for complying with the

50 http://healthit.hhs.gov/CHPL
51 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

two related rules of HIPAA: Privacy[52] and Security[53]. The HIPAA Security Rule sets out specific protections that all covered providers must follow to protect health information. These practices include administrative, technical, and physical safeguards. These safeguards, when applied well, can help practices avoid some of the common security gaps that lead to cyber-attack or data loss. They can protect the people, information, technology, and facilities that health care providers depend on to carry out their primary mission: helping their patients.

The HIPAA Security Rule requires three kinds of safeguards: administrative, physical, and technical.

Administrative safeguards

These safeguards establish standards and specifications for your health information security program that include the following:

- Security management processes to identify and analyze risks to e-PHI and implementing security measures to reduce risks
- Staff training to ensure knowledge of and compliance with your policies and procedures
- Information access management to limit access to electronic health records to protect health information, including the information in EHRs
- Contingency plan to respond to emergencies or restore lost data

Physical safeguards

These safeguards control physical access to your office and computer systems. Examples of required physical safeguards include:

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users
- Workstation use policies to ensure proper access to and use of workstations

52 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
53 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

Technical safeguards

These safeguards include hardware, software, and other technology that limits access to e-PHI. Examples of required technical safeguards include the following:

- Access controls to restrict access to PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper e-PHI alteration or destruction
- Transmission security measures to protect e-PHI when transmitted over an electronic network

Please visit the OCR website for a full overview of security standards and required protections for e-PHI under the HIPAA Security Rule.

Working with Your EHR and Health IT Vendors

When working with your EHR and Health IT vendors, you may want to ask some of the following questions to help you ascertain some of the issues you need to address in your particular practice:

- Are the security features listed below in my certified EHR and my practice environment addressed in your implementation process? Will you train my staff on these features so they can update and configure as necessary?
  - Encryption
  - Auditing function
  - Firewalls and encryption on computer, software, and router
  - Backup and recovery
  - Unique IDs and passwords, biometric if available
  - Role based or user based access controls
  - Anti-virus and anti-spyware
- How does my backup and recovery system work, where is the documentation and how do I test this recovery system?
- How much of your EHR training covers privacy and security functions?
- Communications regarding updates, for example how will you know when valid EHR vendor staff are contacting your practice so that staff do not fall victim to social hacking?

Your EHR Software and Hardware

Most EHRs and the related equipment have these security features built into or provided as part of a service, although they are not always configured or enabled properly. As the guardian of patient health information, it is up to you to learn these basic features and along with your staff, ensure they are functioning and are updated when necessary. Remember, security risk analysis and mitigation is an ongoing responsibility for your practice. This should be part of your practice's ongoing activities and a full security risk analysis should be conducted at least once a year.

Cybersecurity

To exchange patient information, submit claims electronically, generate electronic records for patients' requests, or e-prescribe, an Internet connection is a necessity.

Strong cybersecurity practices are important in order to protect patient information, organizational assets, operations, personnel, and for compliance with the HIPAA Security Rule. Basic cybersecurity practices are needed to protect the confidentiality, integrity, and availability of electronic health record systems, regardless of how they are delivered—whether installed in a physician's office or accessed over the Internet.

Definition of Cybersecurity

Cybersecurity: The protection of information and systems that connect to the Internet. It is in fact protecting your personal information or any form of digital asset stored in your computer or in any digital memory device. It includes detection and response to a variety of cyber (online) attacks.

The U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's (ONC's) Cybersecurity Checklist[54] shows you 10 simple best practices that should be taken to reduce the most important threats to the safety of EHRs.

For a full overview of security standards and required protections for e-PHI under the HIPAA Security Rule[55], visit OCR's website.

Definition of e-PHI

Electronic Protected Health Information (e-PHI): The HIPAA Security Rule protects a subset of information covered by the HIPAA Privacy Rule. This subset of information is referred to as e-PHI. e-PHI is all PHI a covered entity maintains or transmits in electronic form. The Security Rule does not apply to PHI transmitted orally or in writing.

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI). PHI includes information:

- That relates to the individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and
- That identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

54 http://healthit.hhs.gov/pdf/cybersecurity/Basic-Security-for-the-Small-Healthcare-Practice-Checklists.pdf
55 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

What to Do in Case of a Breach of Unsecured PHI?

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

The Breach Notification Rule

The Breach Notification Rule[56] requires HIPAA covered entities to notify individuals and the Secretary of U.S. Department of Health and Human Services (HHS) of the loss, theft, or certain other impermissible uses or disclosures of unsecured protected health information. In particular, health care providers must promptly notify the Secretary of HHS if there is any breach of unsecured protected health information that affects 500 or more individuals, and notify the media if the breach affects more than 500 residents of a State or jurisdiction. If a breach affects fewer than 500 individuals, the covered entity must notify the Secretary and affected individuals. The covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- Significant breaches are investigated by OCR and penalties may be imposed for failure to comply with the HIPAA Rules. Breaches that affect 500 or more patients are publicly reported on the OCR website[57].
- Similar breach notification provisions implemented and enforced by the Federal Trade Commission[58], apply to vendors of personal health records and their third party service providers.

Your Practice and the HIPAA Rules

Who Must Comply with HIPAA Rules?

"Covered entities[59]" must comply with the HIPAA Privacy and Security Rules:

- Health care providers, including doctors, clinics, hospitals, nursing homes, and pharmacies that electronically transmit any health information in connection with a transaction for which HHS has adopted a standard pursant to HIPAA administrative simplification, also known as transaction standard;
- Health plans; and
- Health care clearinghouses.

Where can I get help or more information?

Sixty-two Regional Extension Centers across the nation are prepared to offer customized, on-the-ground assistance to providers who are implementing HIPAA privacy and security protections.

If you are a covered entity and you have a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity, the person or

56 The Breach Notification Rule is an interim final rule and subject to future final rulemaking. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
57 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
58 http://www2.ftc.gov/opa/2009/08/hbn.shtm
59 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

entity is considered a "business associate[60]."

As a covered entity, it is your responsibility to obtain a written contract or agreement that the business associate will appropriately safeguard the PHI[61] created or received on your behalf.

Failure to Comply with HIPAA

Failure to comply with HIPAA can result in civil and criminal penalties.

Civil Penalties

OCR is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules and conducts complaint investigations, compliance reviews, and audits. Penalties may be imposed for failure to comply with the HIPAA Rules.

The civil penalties, especially for intentional disclosure of PHI are substantial, which makes compliance with the HIPAA Privacy and Security Rules essential.

State attorneys general may also enforce provisions of the HIPAA Rules.

Learn more about OCR's HIPAA enforcement[62], the HIPAA Privacy & Security Audit Program[63], or the HIPAA Enforcement Rule[64].

Oversight

The Office for Civil Rights, within the U.S. Department of Health and Human Services (HHS) administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules. State attorneys general may also enforce provisions of the HIPAA Rules. The Centers for Medicare and Medicaid Services within HHS oversees the EHR incentive programs. The Office of the National Coordinator for Health Information Technology provides support for the adoption and promotion of EHR and health information exchange (HIE) to improve health care in the United States.

Breach notification rule and reporting

Criminal Penalties

The U.S. Department of Justice prosecutes criminal violations of HIPAA. Under the HIPAA statute, criminal penalties can be imposed for the knowing misuse of unique health identifiers, and for knowingly and impermissibly obtaining or disclosing individually identifiable health information. The HIPAA identifier regulations specify the appropriate use of identifiers, and the HIPAA Privacy Rule identifies what is an impermissible obtaining or disclosing of individually identifiable health information.The Department of Justice investigates and prosecutes HIPAA criminal cases, and criminal penalties are applied upon conviction.

Public Reporting of Breach Incidents

Breaches of unsecured PHI that affect 500 or more individuals are publicly reported on the OCR website[65].

Find out more about the Breach Notification Rule and reporting requirements[66].

60 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
61 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
62 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
63 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
64 http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html
65 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
66 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

Compliance with Other Laws and Requirements

Besides HIPAA, HITECH, and Meaningful Use privacy and security-related requirements, your medical practice may also need to comply with additional privacy and security laws and requirements. To learn more about these other requirements, view the table below.

The table below provides a snapshot of these domains. Your state board of medicine and your state associations may also have guidance. Privacy and security requirements will continue to evolve. Stay abreast of them and integrate them into your medical practice.

Laws/ Requirements	Key Points
Sensitive Health Information	• Some laws and frameworks recognize that particular health conditions may put individuals at a higher risk for discrimination or harm based on that condition. Federal and some state laws require special treatment and handling of information relating to alcohol and drug abuse, genetics, domestic violence, mental health, and HIV/AIDs. • Federal laws: - 42 CFR Pt. 2: Confidentiality of Alcohol and Drug Abuse [67] - Family Education Rights and Privacy Act (FERPA)[68] - Genetic Information Nondiscrimination Act (GINA)[69] - Title X of Public Health Service Act - Confidentiality[70]
Minors' Health Information	• State and federal laws generally authorize parent or guardian access to minors' health information. • Depending on age and health condition (e.g., reproductive health, child abuse, mental health), and applicable state law, minors also have privacy protections related to their ability to consent for certain services under federal or state law. • Federal laws: - Family Education Rights and Privacy Act - Genetic Information Nondiscrimination Act - Title X of Public Health Service Act
Private-Sector Requirements	• A contracting health plan or payer may require additional confidentiality or safeguards.

67 http://www.samhsa.gov/healthPrivacy
68 http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
69 http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&node=29:4.1.4.1.21.0.26.9&idno=29%20and%20http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&
70 http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ce18bb9053f3b026e8983fd8ac27170c&rgn=div8&view=text&node=42:1.0.1.4.43.1.19.11&idno=42

Essential HIPAA Terms to Know

Understanding your HIPAA responsibilities requires being familiar with the following terms:

- Covered entities include health plans, health care clearinghouses, and most health care providers. Most providers are covered entities because they transmit electronic health information in connection with a standard transaction adopted pursuant to HIPAA administrative simplification rules (e.g., billing electronically). Transmission also includes electronic faxes and electronic submissions through an EHR or computer portal. Therefore, most provider practices will be covered entities under HIPAA.
- Business associates are individuals and organizations that perform services for or on behalf of your practice that entail routine access to protected health information. Examples: claims processing or administration. Also, there are situations in which a person or organization may transport information but may act merely as a conduit for protected health information (PHI) and not be considered a business associate. OCR provides more information about conduits of PHI.
- Individually identifiable health information ("IIHI"): Under HIPAA, IIHI is a subset of health information, and

  (a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse;

  (b) Relates to past, present, or future health or condition of an individual, provision or care, or payment; and

  (c) Identifies the individual or there is a reasonable basis to believe that the information could be used to identify the individual.
- Protected health information (PHI) refers to individually identifiable health information, that is:

  (a) Transmitted by electronic media;

  (b) Maintained in electronic media; or

  (c) Transmitted or maintained in any other form or medium.

HIPAA does not provide protections for all health information. HIPAA applies only to PHI.

- De-Identified Health Information is health information that does not identify an individual, and for which there is no reasonable basis to believe that it can be used to identify an individual. Once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI, or subject to the HIPAA Rules, and, thus, may be used and disclosed by the covered entity or business associate for any purpose without restriction by HIPAA (but remains subject to any other applicable laws). The Privacy Rule designates two ways whereby a covered entity can create de-identified health information[71].

- Breach Notification. A "breach" is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the unsecured protected health information[72], such that the use or disclosure poses a significant financial risk or financial, reputational, or other harm to the affected individual. The Breach Notification Rule[73] specifies what is considered a breach, how and when these breaches must be disclosed, and what the penalties are. For instance, health care providers and their contractors must notify the patient, HHS, and the media in certain circumstances.

71 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html
72 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
73 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Chapter 5:
Privacy and Security Resources

Version 1.2 060112

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 5:
Privacy and Security Resources

Get started today! The U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR), and other HHS agencies have developed and issued a number of guidance, tools, and educational materials designed to help you better integrate privacy and security into your practice. A brief description of each resource is provided, along with a direct link.

Technical Assistance

Regional extension centers (RECs) offer competent technical assistance with expertise in directly assisting providers in solo or small practice with all phases of adopting an electronic health record (EHR).

Find your local REC, or your state or county medical association and other professional associations for additional assistance. You can also look up the closest REC by zip code.

Regulatory & Guidance Information

HIPAA

- Health Information Privacy. U.S. Department of Health and Human Services. Guidance for covered entities on understanding your Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
    - OCR's Summary of the HIPAA Privacy Rule. Summary of key elements of the Privacy Rule, including who is covered, what information is protected, and how information can be used and disclosed. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
    - OCR's Summary of the HIPAA Security Rule. Summary of key elements of the Security Rule, including who is covered, what information is protected, and what safeguards must be in place. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
    - "Are You a Covered Entity?" The Office for Civil Rights describes to whom the Administrative Simplification standards adopted by HHS under HIPAA apply. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
    - Breach Notification Rule. U.S. Department of Health and Human Services. (2009) Describes the interim final breach notification regulations, issued in August 2009, implementing section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
- OCR's Guidance on the HIPAA Privacy Rule and Health IT Toolkit. These guidance documents discuss the HIPAA Privacy Rule and how it can facilitate the electronic exchange of health information. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/
- OCR's Guidance on Risk Analysis under the HIPAA Security Rule. This guidance clarifies OCR's expectations for organizations working to meet the risk analysis requirements of the HIPAA Security Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

- OCR's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals. This guidance explains the circumstances under which personal health information is considered unusable, unreadable, or indecipherable for the purposes of HIPAA compliance. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
- OCR's Remote Use Guidance. This guidance provides information on how a covered entity may protect electronic personal health information (e-PHI) when it is accessed or used outside of the organization's physical space. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf
- OCR's HIPAA Frequently Asked Questions (FAQs) Database. This searchable database provides information on a variety of topics related to HIPAA. Available at: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
- OCR's Sample Business Associate Contract Provisions. This document provides sample business associate contract language to help covered entities more easily comply with the HIPAA Privacy Rule. Available at:http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- OCR's HIPAA Privacy & Security Audit Program. This website provides an overview of the HIPAA Privacy and Security Audit Program. Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/
- The Nationwide Privacy & Security Framework for Electronic Exchange of Individually Identifiable Health Information. This document outlines a privacy and security policy framework for electronic health information exchange and an approach for addressing privacy and security challenges. Available at: http://www.hhs.gov/healthit/documents/NationwidePS_Framework.pdf

Meaningful Use – Privacy & Security

- Core Measure 12: Centers for Medicare & Medicaid Services. *Eligible Professional Meaningful Use Core Measures*. Measure 12 of 15. (Nov. 7, 2010.) This document provides definitions, attestation requirements, and other information related to Meaningful Use Core Measure 12, providing an electronic copy of health information to patients. Available at: http://www.cms.gov/EHRIncentivePrograms/Downloads/12ElectronicCopyofHealthInformation.pdf
- Core Measure 15: Centers for Medicare & Medicaid Services. *Eligible Professional Meaningful Use Core Measures*. Measure 15 of 15. (Nov. 7, 2010.) This document provides definitions, attestation requirements, and other information related to Meaningful Use Core Measure 15, protecting electronic health information. Available at: http://www.cms.gov/EHRIncentivePrograms/Downloads/15_Core_ProtectElectronicHealthInformation.pdf
- Centers for Medicare & Medicaid Services. Eligible Professional Meaningful Use Table of Contents Core and Menu Set Objectives. This document provides a listing of and links to Meaningful Use Core Objectives and Menu Objectives for Eligible Professionals. Available at: https://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf
- Meaningful Use Grid – Stage 1. ONC. This grid provides a quick reference for meaningful use objectives and measures, as well as standards and certification criteria. Available at: http://healthit.hhs.gov/media/MU/n508/MU_SCC_CombinedGrid.pdf

Tools

- Security Risk Assessment Tool. This tool can be used to help your practice conduct a security risk assessment. Available at: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- ONC's Reassessing Your Security Practices in a Health IT Environment. A Guide for Small Health Care Practices. This guide provides information to help small health care practices learn about security measures they may need to consider as they use health information technology. Available at: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1173&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true
- ONC's 10 Best Practices for the Small Health Care Environment. This guide provides information to help small health care practices learn about security measures they may need to consider as they use health information technology. Available at: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1173&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true
- ONC's Cybersecurity Checklist. This checklist provides 10 simple best practices that should be taken to reduce the most important threats to the safety of EHRs. Available at: http://healthit.hhs.gov/pdf/cybersecurity/Basic-Security-for-the-Small-Healthcare-Practice-Checklists.pdf
- HRSA Health IT Adoption Toolbox. HHS' Health Resources and Services Administration (HRSA) compiled planning, implementation, and evaluation resources to help health centers, safety net providers, and ambulatory care providers implement health IT applications in their facilities to meet administrative, IT, and clinical quality objectives. The Health Information Technology Toolbox is available at: http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/index.html
- HRSA Health IT Adoption Toolbox, Privacy, and Security. Privacy and Security information in the toolbox is available at: http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/index.html

Education & Training Materials

- HIPAA Privacy Rule Training Materials. To find educational materials to help you learn more about the HIPAA Privacy Rule, visit the OCR HIPAA Training Materials page.
- HIPAA Security Rule Training Materials. To find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic personal health information, visit the OCR Security Rule Guidance page.
- Uses & Disclosures: A Provider's Privacy Guide. Uses and disclosures of health information, a two-page fact sheet about when protected health information can be used or shared without a patient's express permission. Available at: http://www.cms.gov/MLNProducts/downloads/SE0726FactSheet.pdf
- Data Segmentation in Electronic Health Information - ONC Whitepaper: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950145_0_0_18/gwu-data-segmentation-final.pdf
- Consumer Consent Options – ONC Whitepaper: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1147
- Building Trust in Health Information Exchange. (2011) This document provides a statement on privacy and security by ONC and OCR and describes efforts by HHS to ensure electronic health information is protected. Available at: http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaceID=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPage.

- Health Information Security and Privacy Collaboration (HISPC). A series of products created by HISPC to address the privacy and security challenges presented by electronic health information exchange through multi-state collaboration. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__hispc/1240

Brochures, Fact Sheets, & Videos

- ONC Cybersecurity Video. A short video on cybersecurity emphasizing the importance of keeping electronic health information safe and secure. Available at: http://www.youtube.com/watch?v=BxSFS9faxI4&feature=player_embedded

Patient Relations & Health Information Privacy and Security

- A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others involved in the Patient's Care. OCR's guide provides information for health care providers regarding when a provider is allowed to share a patient's information under HIPAA. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf
- Health Information Privacy for Consumers & Patients. This OCR material provides information on health information privacy for consumers, including information on the HIPAA Privacy Rule and Security Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html
- What Patients Need to Know about EHRs. This ONC document provides patients with information about electronic health records. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_12811_953735_0_0_18/What_Patients_Need_to_Know_about_EHRs.pdf
- HealthIT.gov portal for patients and families. This portal provides information on health information technology specifically designed for patients and their families, including information on protecting the privacy and security of their health information. Available at: http://www.healthit.gov/patients-families

Other Federal & State-Level Privacy and Security Resources

- National Institute of Standards and Technology (NIST) HIPAA Security Rule Toolkit Application. The toolkit is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Available at: http://scap.nist.gov/hipaa/
- National Governors Association (NGA) produced a report on state consent laws and health information exchange. Available at: http://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-health-publications/col2-content/main-content-list/state-and-federal-consent-laws-a.html; http://www.nga.org/Files/pdf/1103HIECONSENTLAWSREPORT.PDF
- Center on Medical Record Rights and Privacy. This website has information developed for consumers/patients summarizing medical record privacy laws in each state. Available at: http://ihcrp.georgetown.edu/privacy/records.html
- Federal Privacy and Security Law Table. (February 2010) This table provides a table summarizing federal laws and regulations addressing privacy and security. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911059_0_0_18/Federal%20Privacy%20Laws%20Table%202%2026%2010%20Final.pdf