The Office of the National Coordinator for
Health Information Technology

Guide to
Privacy and Security of Electronic Health Information

Version 2.0
April 2015

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
HealthIT.gov

Table of Contents

List of Acronyms **4**
Foreword **5**
Revised Guide to Privacy and Security of Electronic Health Information 5
Introduction and Purpose 5
Context 6
Actions and Programs 6
Federal Organizations 6
Chapter 1 ..... **8**
Why Do Privacy and Security Matter? 8
Increasing Patient Trust and Information Integrity Through Privacy and Security 8
Chapter 2 ..... **10**
Your Practice and the HIPAA Rules 10
Understanding Provider Responsibilities Under HIPAA 10
What Types of Information Does HIPAA Protect? 11
Who Must Comply with the HIPAA Rules? 11
The HIPAA Privacy Rule 13
HIPAA Privacy Rule Limits Uses and Disclosures of Patient Information 14
Chapter 3 ..... **22**
Understanding Patients' Health Information Rights 22
Patients' Rights and Your Responsibilities 22
Notice of Privacy Practices (NPP) 22
Patient Access to Information 23
Amending Patient Information 23
Accounting of Disclosures 24
Rights to Restrict Information 24
Right to Confidential Communications 24
Designated Record Set 25
Chapter 4 ..... **26**
Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity 26
The HIPAA Security Rule 26
How to Keep Your Patients' Health Information Secure with an EHR 28
Working with Your EHR and Health IT Developers 29
Cybersecurity 30
Chapter 5 ..... **32**
Medicare and Medicaid EHR Incentive Programs Meaningful Use Core Objectives that Address Privacy and Security 32
Meaningful Use 32
General Overview of Stage 1 and Stage 2 Meaningful Use 33

Chapter 6 ..... **35**
Sample Seven-Step Approach for Implementing a Security Management Process 35
Introduction 35
How to Get Started on Security 35
Sample Seven-Step Approach for Implementing a Security Management Process 37
Step 1: Lead Your Culture, Select Your Team, and Learn 37
Step 2: Document Your Process, Findings, and Actions 40
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis) 41
Step 4: Develop an Action Plan 43
Step 5: Manage and Mitigate Risks 46
Step 6: Attest for Meaningful Use Security-Related Objective 53
Step 7: Monitor, Audit, and Update Security on an Ongoing Basis 54
Chapter 7 ..... **56**
Breach Notification, HIPAA Enforcement, and Other Laws and Requirements 56
Civil Penalties 56
Criminal Penalties 56
The Breach Notification Rule: What to Do If You Have a Breach 57
Risk Assessment Process for Breaches 58
Reporting Breaches 59
Investigation and Enforcement of Potential HIPAA Rules Violations 60
Penalties for Violations 60
Other Laws and Requirements 61

Tables

Table 1: Overview of HHS Entities 7
Table 2: Examples of Potential Information Security Risks with Different Types of EHR Hosts 43
Table 3: Five Security Components for Risk Management 45
Table 4: Comparison of Secured and Unsecured PHI 58
Table 5: Overview of Penalties 60
Table 6: Overview of Other Laws and Requirements 61

List of Acronyms

AHIMA	American Health Information Management Association
AIDS	Acquired Immune Deficiency Syndrome
BA	Business Associate
BAA	Business Associate Agreement
CD	Compact Disc
CE	Covered Entity
CEHRT	Certified Electronic Health Record Technology
CFR	Code of Federal Regulations
CHPS	Certified in Healthcare Privacy and Security
CMS	Centers for Medicare and Medicaid Services
CPHIMS	Certified Professional in Healthcare Information and Management Systems
CPOE	Computerized Provider Order Entry
DVD	Digital Video Disc
EHR	Electronic Health Record
EP	Eligible Professional
ePHI	Electronic Protected Health Information
FAQ	Frequently Asked Questions
FERPA	Family Educational Rights and Privacy Act
FR	Federal Register
GINA	Genetic Information Nondiscrimination Act
Health IT	Health Information Technology
HHS	U.S. Department of Health and Human Services
HIE	Health Information Exchange
HIMSS	Healthcare Information and Management Systems Society
HIO	Health Information Organization
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HIV	Human Immunodeficiency Virus
IT	Information Technology
NIST	National Institute of Standards and Technology
NPP	Notice of Privacy Practices
NPRM	Notice of Proposed Rulemaking
OCR	Office for Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
PHR	Personal Health Record
REC	Regional Extension Center
SRA	Security Risk Assessment
USC	United States Code

Foreword

Revised Guide to Privacy and Security of Electronic Health Information

Introduction and Purpose

Everyone has a role to play in the privacy and security of electronic health information — it is truly a shared responsibility. The Office of the National Coordinator for Health Information Technology (ONC) provides resources to help you succeed in your privacy and security responsibilities. This Guide to Privacy and Security of Electronic Health Information (referred to as "Guide") is an example of just such a tool.

The intent of the Guide is to help health care providers — especially Health Insurance Portability and Accountability Act (HIPAA) Covered Entities (CEs) and Medicare Eligible Professionals (EPs)[1] from smaller organizations — better understand how to integrate federal health information privacy and security requirements into their practices. This new version of the Guide provides updated information about compliance with the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs' privacy and security requirements as well as the HIPAA Privacy, Security, and Breach Notification Rules.

The U.S. Department of Health and Human Services (HHS), via ONC, the Centers for Medicare and Medicaid Services (CMS), and the Office for Civil Rights (OCR), supports privacy and security through a variety of activities. These activities include the meaningful use of certified EHRs, the Medicare and Medicaid EHR Incentive Programs, enforcement of the HIPAA Rules, and the release of educational resources and tools to help providers and hospitals mitigate privacy and security risks in their practices.

[1] The following are considered "Eligible Professionals": doctors of medicine or osteopathy, doctors of dental surgery or dental medicine, doctors of podiatry, doctors of optometry, and chiropractors. (Source: http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf)

This Guide is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this Guide.

Context

This Guide is designed to help you work to comply with federal requirements and federal programs' requirements administered through HHS agencies and offices. These key programs and organizations involved in health information privacy and security are described below.

Actions and Programs

- The **HIPAA Privacy, Security, and Breach Notification Rules**, as updated by the HIPAA Omnibus Final Rule[2] in 2013, set forth how certain entities, including most health care providers, must protect and secure patient information. They also address the responsibilities of Business Associates (BAs), which include EHR developers working with health care providers.

- In 2011, CMS initiated the Medicare and Medicaid EHR Incentive Programs.[3,4] The programs are referred to as **"EHR Incentive Programs"** or **"Meaningful Use"** Programs throughout this Guide. Meaningful Use encourages health care organizations to adopt EHRs through a staged approach. Each stage contains core requirements that providers must meet; privacy and security are included in the requirements.

Federal Organizations

This Guide frequently refers to federal organizations within HHS that have a distinct health information technology (health IT) role. These organizations are summarized in Table 1.

[2] In January 2013, HHS issued a Final Rule that modified the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA). This Final Rule is often referred to as the HIPAA Omnibus Final Rule. These modifications are incorporated throughout this Guide. The Rule can be accessed at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
[3] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/
[4] In 2012, CMS finalized the Stage 2 Meaningful Use criteria that an EP must follow to continue to participate in the Medicare and Medicaid EHR Incentive Programs. Several Stage 2 criteria address privacy and security. The 2012 regulations also revised Stage 1 criteria that address privacy and security. The regulations can be accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf.

Table 1: Overview of HHS Entities

Federal Office/Agency	Health IT-Related Responsibilities	Website
Centers for Medicare and Medicaid Services (CMS)	• Oversees the Meaningful Use Programs	www.cms.gov
Office for Civil Rights (OCR)	• Administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules • Conducts HIPAA complaint investigations, compliance reviews, and audits	www.hhs.gov/ocr
Office of the National Coordinator for Health Information Technology (ONC)	• Provides support for the adoption and promotion of EHRs and health information exchange • Offers educational resources and tools to assist providers with keeping electronic health information private and secure	www.HealthIT.gov

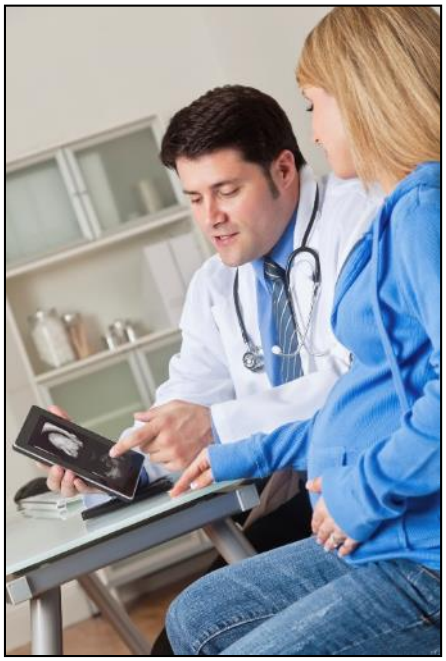
A fourth federal entity mentioned in this Guide is the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. NIST sets computer security standards for the federal government and publishes reports on topics related to information technology (IT) security. While the reports are intended for the federal government, they are available for public use and can provide valuable information to support a strong security program for your practice setting. To review NIST publications that are relevant to the HIPAA Security Rule, visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html[5] and scroll to the bottom of the page.

Other state and federal laws may require additional privacy and security actions that are not addressed in this Guide.

[5] Note that the NIST special publications on this website are provided as an informational resource and are not legally binding guidance for CEs to comply with the requirements of the HIPAA Security Rule.

Chapter 1
Why Do Privacy and Security Matter?

Increasing Patient Trust and Information Integrity Through Privacy and Security



To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. If your patients lack trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you.[6] Withholding their health information could have life-threatening consequences.

This is one reason why it's so important for you to ensure the privacy and security of health information. When patients trust you and health information technology (health IT) enough to share their health information, you will have a more complete picture of patients' overall health and together, you and your patient can make more-informed decisions.

In addition, when breaches of health information occur, they can have serious consequences for your organization, including reputational and financial harm or harm to your patients. Poor privacy and security practices heighten the vulnerability of patient information in your health information system, increasing the risk of successful cyber-attack.

To help cultivate patients' trust, you should:

- Maintain accurate information in patients' records
- Make sure patients have a way to request electronic access to their medical record and know how to do so

[6] http://www.healthit.gov/sites/default/files/022414_hit_attitudesaboutprivacydatabrief.pdf. See also Agaku, I.T., Adisa, A.O., Ayo-Yusuf, O.A., & Connolly, G.N. (2014, March-April). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association, 21*(2), 374-8. Abstract available at http://www.ncbi.nlm.nih.gov/pubmed/23975624.

- Carefully handle patients' health information to protect their privacy
- Ensure patients' health information is accessible to authorized representatives when needed

Protecting patients' privacy and securing their health information stored in an EHR is a core requirement of the Medicare and Medicaid EHR Incentive Programs.[7] (The EHR Incentive Programs are also referred to as the "Meaningful Use" Programs throughout this Guide.) **Your practice — not your EHR developer — is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR.**

Effective privacy and security measures help you meet Meaningful Use requirements while also helping your clinical practice meet requirements of the HIPAA Rules and avoid costly civil money penalties for violations,[8] as discussed in Chapter 7.

[7] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html
[8] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/

Chapter 2
Your Practice and the HIPAA Rules

Understanding Provider Responsibilities Under HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) Rules provide federal protections for patient health information held by Covered Entities (CEs) and Business Associates (BAs) and give patients an array of rights with respect to that information. This suite of regulations includes the **Privacy Rule**, which protects the privacy of individually identifiable health information; the **Security Rule**, which sets national standards for the security of electronic Protected Health Information (ePHI); and the **Breach Notification Rule**, which requires CEs and BAs to provide notification following a breach of unsecured Protected Health Information (PHI). CEs must comply with the HIPAA Privacy,[10] Security,[11] and Breach Notification[12] Rules. BAs must comply with the HIPAA Security Rule and Breach Notification Rule as well as certain provisions of the HIPAA Privacy Rule.

Where Can I Get Help or More Information?
Regional Extension Centers (RECs)[9] across the nation can offer customized, on-the-ground assistance to providers who are implementing HIPAA privacy and security protections.

Whether patient health information is on a computer, in an Electronic Health Record (EHR), on paper, or in other media, providers have responsibilities for safeguarding the information by meeting the requirements of the Rules.

This chapter provides a broad overview of the HIPAA privacy and security requirements. You may also need to be aware of any additional applicable federal, state, and local laws governing the privacy and security of health information.[13]

[9] http://www.healthit.gov/providers-professionals/regional-extension-centers-recs
[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
[11] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[12] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[13] State laws that are more privacy-protective than HIPAA continue to apply.

What Types of Information Does HIPAA Protect?

The Privacy Rule protects most *individually identifiable health information* held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" or "PHI." Individually identifiable health information is information, including demographic information, that relates to:

- The individual's past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

In addition, individually identifiable health information *identifies the individual or there is a reasonable basis to believe it can be used to identify the individual.*

For example, a medical record, laboratory report, or hospital bill would be PHI if information contained therein includes a patient's name and/or other identifying information.

The HIPAA Rules do not apply to individually identifiable health information in your practice's employment records or in records covered by the Family Educational Rights and Privacy Act (FERPA), as amended.[14]

Who Must Comply with the HIPAA Rules?

CEs[15] and BAs must comply with the HIPAA Rules. CEs include:

- Health care providers who conduct certain standard administrative and financial transactions in electronic form, including doctors, clinics, hospitals, nursing homes, and pharmacies. Any health care provider who bills electronically (such as a current Medicare provider) is a CE.
- Health plans
- Health care clearinghouses

A BA is a person or entity, other than a workforce member[16] (e.g., a member of your office staff), who performs certain functions or activities on your behalf, or provides certain services to or for you, when the services involve the access to, or the use or disclosure of, PHI.[17] BA *functions or activities* include

[14] 20 United States Code (USC) 1232g; 45 Code of Federal Regulations (CFR) 160.103; http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
[15] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
[16] Workforce members are employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such covered entity, whether or not they are paid by the covered entity. 45 CFR 160.103.
[17] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html and 45 CFR 160.103.

claims processing, data analysis, quality assurance, certain patient safety activities, utilization review, and billing.

BA *services to a CE* can be legal, actuarial, accounting, consulting, data aggregation, information technology (IT) management, administrative, accreditation, or financial services.[18] Many contractors that perform services for a CE are not BAs because the services do not involve the use or disclosure of PHI.

Examples of BAs include:

- Health Information Organizations or Exchanges (HIOs/HIEs)
- E-prescribing gateways
- Other person who provides data transmission services (that involve routine access to PHI) to a CE
- A subcontractor to a BA that creates, receives, maintains, or transmits PHI on behalf of the BA
- An entity that a CE contracts with to provide patients with access to a Personal Health Record (PHR) on behalf of a CE

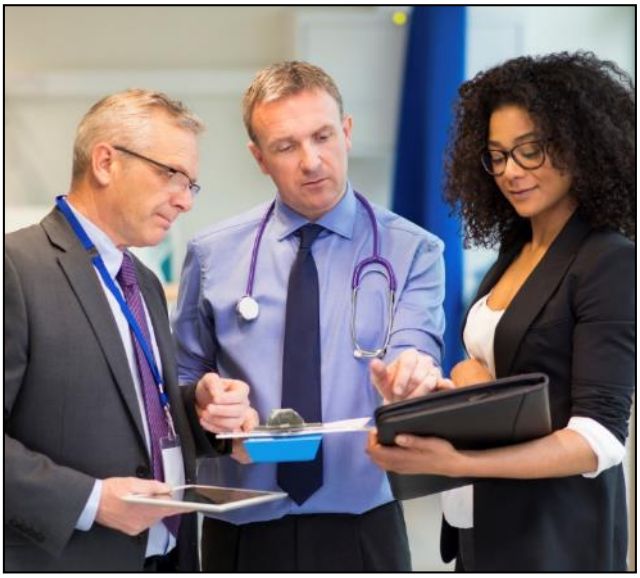
Following are some scenarios to help illustrate who is and who is not a BA. This is not an exhaustive list of examples.

- You hire a company to turn your accounting records from visits into coded claims for submission to an insurance company for payment; **the company is your BA for payment purposes**.[19]
- You hire a case management service to identify your diabetic and pre-diabetic patients at high risk of non-compliance and recommend optimal interventions to you for those patients. **The case management service is a BA** acting on your behalf by providing case management services to you.
- You hire a web designer to maintain your practice's website and improve its online access for patients seeking to view/download or transmit their health information. The designer must have regular access to patient records to ensure the site is working correctly. **The web designer is a BA.**
- **Not a BA:** You hire a web designer to maintain your practice's website. The designer installs the new electronic version of the Notice of Privacy Practices (NPP) and improves the look and feel of the general site. However, the designer has no access to PHI. **The web designer is not a BA.**
- **Not a BA:** You hire a janitorial company to clean your office nightly, including vacuuming your file room. **If the janitors do not have access to PHI, then the janitors are not BAs.**

[18] Ibid.
[19] Ibid.

When a CE discloses PHI to health plans for payment, there is no BA relationship because the health plan is not performing a function or activity for the CE. While the CE may have an agreement to accept discounted fees as reimbursement for services provided to health plan members, that agreement does not create a BA relationship because neither entity is acting on behalf of or providing a service to the other.[20]

A CE can be the BA of another CE when it performs the functions or activities for the CE. For example, if a hospital provides billing services for attending physicians, the hospital is a BA of the physicians for the purposes of preparing those bills. Other functions the hospital performs regarding the attending physicians, such as quality review of patient outcomes for hospital privileging purposes, do not create a BA relationship because the activities are not done on behalf of the physician. Finally, a health care provider is not a BA of another health care provider when it uses and discloses PHI for treatment purposes. So the attending physician and the hospital do not have a BA relationship as they share PHI to treat their mutual patients.



When a CE uses a contractor or other non-workforce member to perform BA services or activities, the Rules require that the CE include certain protections for the information in a BA agreement. In the agreement, a CE must impose specified written safeguards on the PHI accessed, used, or disclosed by the BA. Moreover, a CE may not contractually authorize its BA to make any use or disclosure of PHI that would violate the Rule.

BAs are directly liable for violating the HIPAA Security Rule and Breach Notification Rule as well as certain provisions of the Privacy Rule. Liability may attach to BAs, even in situations in which the BA has not entered into the required agreement with the CE.

Specific requirements for CEs and BAs are discussed below; also see Step 5D of Chapter 6.

The HIPAA Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used and shared, including rights to examine and obtain a copy of their health records as well as to request corrections.

[20] Ibid.

The imposition of civil and criminal penalties is possible for violations of HIPAA and the HIPAA Privacy Rule. Learn more about HIPAA enforcement on the Office for Civil Rights (OCR) website[21] and in Chapter 7. The Privacy Rule is discussed further on the Privacy Rule page of the OCR website.[22]

HIPAA Privacy Rule Limits Uses and Disclosures of Patient Information

This section provides examples of how the Privacy Rule may apply to your practice.

Do I Need to Inform My Patients about How I Use or Disclose Their Health Information?

Generally, yes, a CE must prominently post and distribute an NPP. The notice must describe the ways in which the CE may use and disclose PHI. The notice must state the CE's duties to protect privacy, provide an NPP, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to the U.S. Department of Health and Human Services (HHS) and to the CE if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the CE. CEs must act in accordance with their notices.

The Rule also contains specific distribution requirements for health care providers and health plans.

In addition to providing this notice to patients at the initial visit, your practice must make its NPP available to any patient upon request (discussed in Chapter 3). Chapter 6, Step 5C, provides an overview about new notification requirements resulting from the 2013 Privacy Rule modifications.

You may want to start with and personalize for your practice the model NPPs for providers[24] that were developed by OCR in collaboration with the Office of the National Coordinator for Health Information Technology (ONC). Your REC or medical association also may be able to suggest some NPP templates that comply with the updated requirements. Note that your state health information privacy law may require you to add other information to your notice.

Notice of Privacy Practices (NPP)

HHS provides model NPPs[23] that you can download and personalize for your practice's use. These model notices reflect the changes required by the HIPAA Omnibus Final Rule. You will notice that NPPs must include the following information:

- How the CE may use and disclose an individual's PHI
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the CE
- The CE's legal duties with respect to the information, including a statement that the CE is required by law to maintain the privacy of PHI
- Whom individuals can contact for further information about the CE's privacy policies

[21] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/
[22] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
[23] http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
[24] http://www.healthit.gov/providers-professionals/model-notices-privacy-practices

Do I Have to Get My Patients' Permission to Use or Disclose Their Health Information with Another Health Care Provider, Health Plan, or Business Associate?

In general, you as a CE may use and disclose PHI for your own treatment, payment, and health care operations activities — and other permissible or required purposes consistent with the HIPAA Privacy Rule — *without* obtaining a patient's written permission (e.g., consent or authorization).

A CE also may disclose PHI for:

- The treatment activities of another health care provider,
- The payment activities of another CE and of any health care provider, or
- The health care operations of another CE when:
    - Both CEs have or have had a relationship with the individual
    - The PHI pertains to the relationship
    - The data requested is the minimum necessary
    - The health care operations are:
        - Quality assessment or improvement activities
        - Review or assessment of the quality or competence of health professionals, or
        - Fraud and abuse detection or compliance.

An exception applies to most uses and disclosures of psychotherapy notes that may be kept by a provider from the EHR; a CE cannot disclose psychotherapy notes without an individual's written authorization.

Except for disclosures to other health care providers for treatment purposes, you must make reasonable efforts to use or disclose only the minimum amount of PHI needed to accomplish the intended purpose of the use or disclosure. This is called the minimum necessary standard.[25] When this minimum necessary standard applies to a use or disclosure, a CE may not use or disclose the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

When Are Patient Authorizations Not Required for Disclosure?

- **Information Sharing Needed for Treatment** – You may disclose, without a patient's authorization, PHI about the patient as necessary for treatment, payment, and health care operations purposes. Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to

[25] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

another. A disclosure of PHI by one CE for the treatment activities undertaken by another CE is fundamental to the nature of health care.

- **Disclosures to Family, Friends, and Others Involved in the Care of the Individual as well as for Notification Purposes** – To make disclosures to family and friends involved in the individual's care or for notification purposes, or to other persons whom the individual identifies, you must obtain informal permission by asking the individual outright, or by determining that the individual did not object in circumstances that clearly gave the individual the opportunity to agree, acquiesce, or object. For example, if a patient begins discussing health information while family or friends are present in the examining room, this is a "circumstance that clearly gave the individual the opportunity to agree, acquiesce, or object." You do not need a written authorization to continue the discussion.

  Where the individual is incapacitated, in an emergency situation, or not available, a CE generally may make such disclosures, if the provider determines through his/her professional judgment that such action is in the best interests of the individual.

  You must limit the PHI disclosed to what is directly relevant to that person's involvement in the individual's care or payment for care. Similarly, a CE may rely on an individual's informal permission to use or disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care, of the individual's location, general condition, or death.[26] OCR's website contains additional information about disclosures to family members and friends in fact sheets developed for consumers[27] and providers.[28]

- **Information Needed to Ensure Public Health and Safety** – You may disclose PHI without individual authorization in the following situations:
  - To send immunization records to schools. Immunization records about a student or prospective student of a school can be disclosed to the school without written authorization — as long as your practice has a parent or guardian's oral agreement if the student is a minor, or from the individual if the individual is an adult or emancipated

[26] 45 CFR 164.510(b). Also, search the HHS Frequently Asked Questions (FAQs) at http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html.
[27] http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf
[28] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf

minor. Your practice must document such oral agreement. Such disclosures can only be made in instances where state law requires the school to have such information before admitting the student. In addition, the PHI disclosed in such an instance must be limited to proof of immunization.[29]

- To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.[30]
- To a foreign government agency (at the direction of a public health authority) that is acting in collaboration with the public health authority.[31]
- To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the CE to notify such individuals as necessary to prevent or control the spread of the disease.[32]

- **Information Needed to Prevent or Lessen Imminent Danger** – You may disclose PHI that you believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone you believe can prevent or lessen the threat (including the target of the threat). CEs may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[33]
- **Disclosures in Facility Directories** – In health care facilities where a directory of patient contact information is maintained, a CE may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility. The CE may then disclose the individual's condition and location in the facility to anyone asking for the individual by name and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

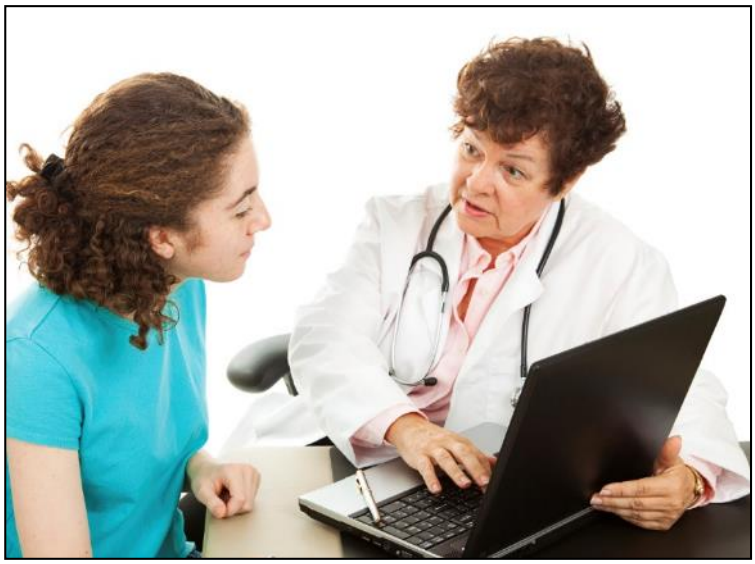
  Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, CEs generally may make such uses and disclosures if, in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.
- **Note:** Health information of an individual that has been deceased for more than 50 years is not PHI and therefore not subject to the Privacy Rule use and disclosure standards. You may use and disclose the information without patient authorization.

[29] 45 CFR 164.512(b)(1)(vi).
[30] 45 CFR 164.501 and 164.512(b)(1)(i).
[31] 45 CFR 164.512(b)(1)(i).
[32] 45 CFR 164.512(b)(1)(iv).
[33] 45 CFR 164.512(j).

For more information on disclosures for public health purposes and circumstances that permit the disclosure of PHI without a patient authorization, visit the Health Information Privacy Public Health web page.[34]

When Are Patient Authorizations Required for Disclosure?

A CE must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. A CE may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.



An authorization must be written in specific terms. It may allow use and disclosure of PHI by the CE seeking the authorization or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

Specific purposes that require an individual's written authorization include:

- **Psychotherapy Notes** – Your practice and your BA must obtain an individual's authorization to use or disclose psychotherapy notes[35] with the following exceptions:
    - The CE who originated the notes may use them for treatment.
    - A CE may use or disclose, without an individual's authorization, the psychotherapy notes for its own training; to defend itself in legal proceedings brought by the individual; for HHS to investigate or determine the CE's compliance with the Privacy Rules; to avert a

[34] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html

[35] 42 CFR 164.501: "*Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical test, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

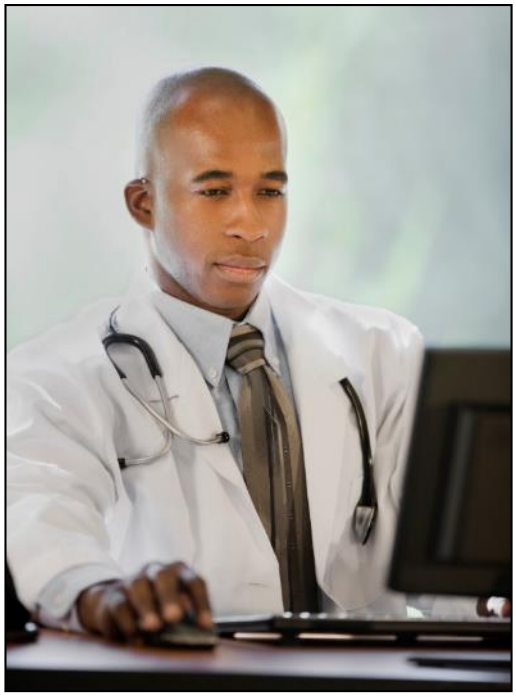
serious and imminent threat to public health or safety; to a health oversight agency for lawful oversight of the originator of the psychotherapy notes; for the lawful activities of a coroner or medical examiner; or as required by law.

- **Marketing Activities** – Your practice and your BA must obtain a patient's authorization prior to using or disclosing PHI for marketing activities. Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. If you are being paid for such use or disclosure in marketing, the authorization must state that payment is involved. However, the Privacy Rule carves out some health-related activities from this definition of marketing. *Activities not considered to be marketing, and therefore not subject to the marketing authorization requirements, are*:
    - Communications for treatment of the individual; and
    - Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual if there is no compensation involved for making the communication. For example:
        - You contract with a health coach to provide case management and to coordinate the care you provide for your patients with other physicians.
        - An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.
        - A hospital social worker shares medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home.
- **PHI Sales and Licensing** – Your practice and your BA may not sell PHI without patient authorization (including the licensing of PHI). A sale is a disclosure of PHI in which your practice or your BA directly or indirectly receives payment from the recipient of the PHI.
    - The following are examples of actions that do not constitute "sale of PHI" and therefore do not require patient authorization:
        - Public health reporting activities
        - Research, if the remuneration is reasonable and cost-based
        - Treatment and payment
        - Sale or merger of your practice
        - Due diligence
        - A payment you make to a BA for services the BA supplied

- **Research** – Special rules apply with regard to clinical research, bio-specimen banking, and all other forms of research not involving psychotherapy notes. In some circumstances, patient authorization is required. You may want to obtain specific guidance on these requirements from sources like the main OCR Health Information Privacy Research web page[36] and the National Institutes of Health HIPAA Privacy Rule Information for Researchers web page.[37]

What is De-Identified PHI?

The Privacy Rule does not restrict the use or disclosure of *de-identified health information*. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. If data is de-identified in the manner prescribed by HIPAA, it is not PHI. Increasingly researchers are seeking and using de-identified clinical data for health system improvement activities.



The Privacy Rule permits a CE or its BA to create and freely use and disclose information that is not individually identifiable by following the Privacy Rule's de-identification requirements. These provisions allow the entity to use and disclose information that neither identifies nor provides a reasonable basis to identify an individual. The Rule provides two de-identification methods: 1) a formal determination by a qualified expert; or 2) the removal of 18 specified individual identifiers as well as absence of actual knowledge by the CE that the remaining information could be used alone or in combination with other information to identify the individual. You may use a BA to de-identify the PHI.

Note that just removing the identifiers specified in the Privacy Rule may NOT make information de-identified.[38] However, once PHI is de-identified in accordance with the Privacy Rule, it is no longer PHI, and thus may be used and disclosed by your practice or your BA for any purpose (subject to any other applicable laws).

What About Patient Information Pertaining to Behavioral Health or Substance Abuse?

The HIPAA Rules apply equally to all PHI, including individually identifiable behavioral health or substance abuse information that your practice collects or maintains in a patients' record. Thus, for HIPAA Rule compliance purposes, you would protect such behavioral health or substance abuse information that your practice collects in the same way that you protect other PHI.[39] However,

[36] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/
[37] http://privacyruleandresearch.nih.gov/pr_02.asp
[38] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html
[39] Learn more about the HIPAA Privacy Rule and sharing information related to mental health at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html.

remember that the Privacy Rule restricts sharing of psychotherapy notes without patient authorization. In addition, other federal regulations govern health information related to substance abuse and mental health services. Also, state privacy laws may be more stringent than the HIPAA Rules regarding information about individuals' behavioral health and substance abuse; please review your specific state's laws.

The HIPAA Privacy Rule allows you to share a patient's health information, except for psychotherapy notes, with another CE for treatment, payment, and health care operations without a patient's authorization, as long as no other state law applies. For additional guidance on the HIPAA Privacy Rule and sharing information related to mental health, please see OCR's Guidance at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html.

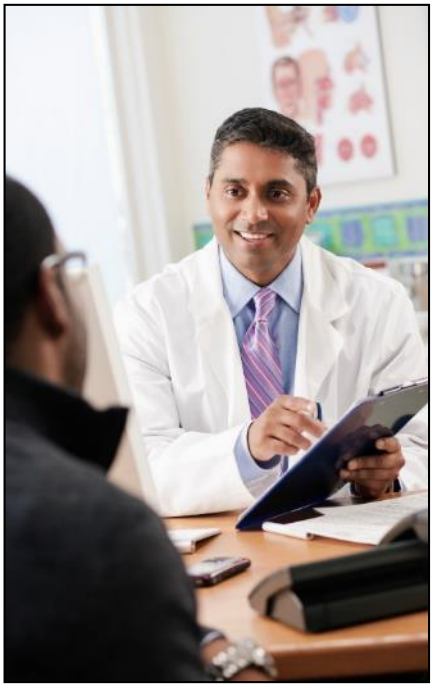
Federal and State Privacy Laws — Which Prevail?

The HIPAA Rules provide a floor of federal protections for PHI. However, the Rules are not the only laws that address the protection of health information. In some instances, a more protective state law may forbid a disclosure or require you to get an individual's written authorization to disclose health information where HIPAA would otherwise permit you to disclose the information without the individual's permission. The HIPAA Rules do not override such state laws that do not conflict with the Rules and offer *greater* privacy protections. If a state law is *less* protective than the HIPAA Rules but a CE or BA could comply with both, both apply — such as when a state law permits disclosure without an authorization and the Privacy Rule requires an authorization, the entity could comply by obtaining authorization.

This Guide is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this Guide.

Chapter 3
Understanding Patients' Health Information Rights

Patients' Rights and Your Responsibilities



The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule standards address the use and disclosure of individuals' Protected Health Information (PHI) by organizations subject to the Privacy Rule. The Rule also addresses standards for individuals' privacy rights so that patients can understand and control how their health information is used and disclosed. The Office for Civil Rights (OCR) explains these rights and other requirements more fully on its website, including in its Summary of the HIPAA Privacy Rule,[40] its Frequently Asked Questions (FAQs),[41] and its Understanding Health Information Privacy page.[42]

As a health care provider, you have responsibilities to patients under the HIPAA Privacy Rule, including providing them with a Notice of Privacy Practices (NPP) and responding to their requests for access, amendments, accounting of disclosures, restrictions on uses and disclosures of their health information, and confidential communications.

The Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (also known as "Meaningful Use" Programs) add new rights for patients who want their health care providers to transmit their electronic PHI (ePHI) to themselves or other caregivers.

Notice of Privacy Practices (NPP)

If you are a Covered Entity (CE), you must provide your patients with a notice of your privacy practices. Your notice must contain certain elements, including:

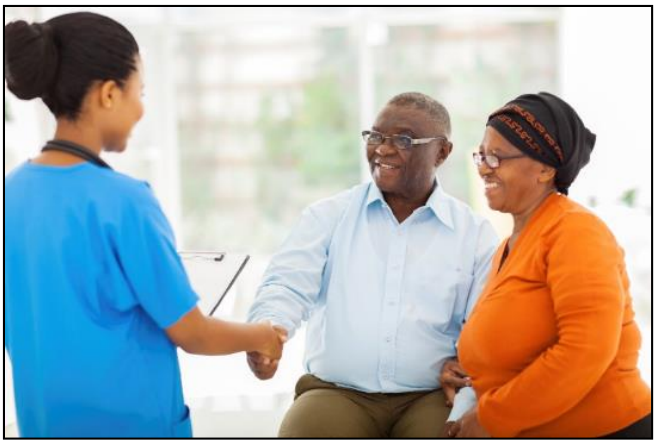
- Description of how your practice may use or disclose (share) an individual's PHI
- Specification of individuals' rights, including the right to complain to the U.S. Department of Health and Human Services (HHS) and to your practice if they believe their privacy rights have been violated (many of these rights are described below)

[40] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[41] http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
[42] http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

- Details of your practice's duties to protect privacy, provide an NPP, and abide by the terms of the notice (OCR provides extensive information for providers, including customizable model notices, on its website. Visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html for requirements and http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html for model notices.)

Patient Access to Information

Patients have the right to inspect and receive a copy of their PHI in a *designated record set*, which includes information about them in your medical and billing records. (Designated record sets are explained at the end of this chapter.) Generally, a CE must grant or deny the request for access within 30 days of receipt of the request. If the health information is held in electronic format and the patient requests to receive it in a specific electronic format, a CE must provide it in the electronic format requested by the patient if it is readily producible. If the format is not available, the CE must provide the health information in an electronic format agreed to by the patient and CE.



Under the Meaningful Use requirements, additional rights apply as well. For example, as your practice gains the capability to demonstrate Stage 2 Meaningful Use, you will be required to respond to any requests from your patients to transmit an electronic copy of PHI directly to persons or entities they designate. An individual may request that you transmit PHI in your records to his or her Personal Health Record (PHR) or to another physician. Your EHR developers, as your BAs, must cooperate in this obligation.

Amending Patient Information

Under the HIPAA Rules, patients have the right to request that your practice amend their PHI in a designated record set. Generally, a CE must honor the request unless it has determined that the information is accurate and complete. The CE must act on an individual's request for an amendment no later than 60 days after the receipt of the request. If you accept an amendment request, your practice must make the appropriate amendment by identifying the records in the designated record set that are affected by the amendment and providing a link to the location of the amendment. If you refuse the request, additional requirements, including the patient's right to file a statement of disagreement that stays with the health record, apply.

Accounting of Disclosures

Individuals have a right to receive an accounting of disclosures[43] of their PHI made by your practice to a person or organization outside of your practice. An accounting of disclosures is a listing of the:

- Names of the person or entity to whom the PHI was disclosed
- Date on which the PHI was disclosed
- Description of the PHI disclosed
- Purpose of the disclosure

This right to an accounting is limited, as the Rule does not require you to include disclosures made for treatment, payment, heath care operations, and several other purposes and situations.

Your practice is required to provide an accounting of disclosures for the six years prior to the date on which the accounting was requested.

Rights to Restrict Information

Individuals have the right to request that your practice restrict certain:

- Uses and disclosures of PHI for treatment, payment, and health care operations
- Disclosures to persons involved in the individual's health care or payment for health care
- Disclosures to notify family members or others about the individual's general condition, location, or death

If your patient (or another person on behalf of the individual) has fully paid out-of-pocket for a service or item and also requests that the PHI not be disclosed to his/her health plan, your practice cannot disclose the PHI to a health plan for payment or health care operations.[44] You should implement policies and procedures that ensure this directive can be carried out.

Right to Confidential Communications

Your practice must accommodate reasonable requests by your patients to receive communications from you by the means or at the locations they specify. For example, they may request that appointment reminders be left on their work voicemail rather than home phone voicemail.

[43] OCR has issued a Notice of Proposed Rulemaking (NPRM) proposing changes to the right to accounting provisions in the Privacy Rule pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. Learn more at http://blog.cms.gov/2015/01/29/cms-intends-to-modify-requirements-for-meaningful-use/.

[44] 45 Code of Federal Regulations (CFR) 164.522(a)(1)(vi).

Designated Record Set

Given that the HIPAA rights of access and amendment are specific to a CE's designated record set, review your practice's policy about your designated record set to confirm that the policy specifies that EHRs are a component of the set.

A designated record set is a group of records that your practice or your Business Associate (BA) (if applicable) maintains to make decisions about individuals. For health care providers, the designated record set includes (but is not limited to) a patient's medical records and billing records. CEs are responsible for determining what records should be included as part of the designated record set.

For more information about designated record sets, review OCR's guidance on the HIPAA Privacy Rule's Right of Access and Health Information Technology.[45]

[45] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf

Chapter 4

Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity

To support patient care, providers store electronic Protected Health Information (ePHI) in a variety of electronic systems, not just Electronic Health Records (EHRs). Knowing this, providers must remember that all electronic systems are vulnerable to cyber-attacks and must consider in their security efforts all of their systems and technologies that maintain ePHI.[46] (See Chapter 6 for more information about security risk analysis.)

While a discussion of ePHI security goes far beyond EHRs, this chapter focuses on EHR security in particular.

The HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule[47] establishes a national set of minimum security standards for protecting all ePHI that a Covered Entity (CE) and Business Associate (BA) create, receive, maintain, or transmit. The Security Rule contains the administrative, physical, and technical safeguards that CEs and BAs must put in place to secure ePHI.

Resources

- HIPAA Requirements,[48] in detail
- HIPAA Privacy Rule,[49] in detail
- HIPAA Security Rule,[50] in detail
- Privacy and Security Resources[51]

[46] Refer to the booklet "Partners in Integrity" at http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/understand-prevent-provider-idtheft.pdf for more information about medical identity theft and fraud prevention.
[47] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[48] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
[49] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
[50] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[51] http://healthit.gov/providers-professionals/ehr-privacy-security/resources

These Security Rule safeguards can help health care providers avoid some of the common security gaps that could lead to cyber-attack intrusions and data loss. Safeguards can protect the people, information, technology, and facilities that health care providers depend on to carry out their primary mission: caring for their patients.

The Security Rule has several types of safeguards and requirements which you must apply:

1. **Administrative Safeguards**[52] – Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to ePHI and then implement security measures to reduce the identified risks.
2. **Physical Safeguards**[53] – These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.[54] These safeguards are the technology and the policies and procedures for its use that protect ePHI and control access to it.
3. **Organizational Standards**[55] – These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's ePHI. The standards provide the specific criteria required for written contracts or other arrangements.
4. **Policies and Procedures**[56] – These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.

Visit the Office for Civil Rights (OCR) website[57] for a full overview of security standards and required protections for ePHI under the Security Rule.

[52] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
[53] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf
[54] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
[55] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf
[56] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf
[57] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

How to Keep Your Patients' Health Information Secure with an EHR

Your practice is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of ePHI maintained in your EHR.

Having an EHR affects the types and combinations of safeguards you will need to keep your patients' health information confidential. EHRs also bring new responsibilities for safeguarding your patients' health information in an electronic form.

To uphold patient trust as your practice continues to adopt and use an EHR or other electronic technology for collection and use of ePHI, and to comply with HIPAA Security Rule and Meaningful Use requirements, your practice must conduct a security risk analysis (sometimes called "security risk assessment"). (See Chapter 6 for more discussion on security risk analysis.) The risk analysis process will guide you through a systematic examination of many aspects of your health care practice to identify potential security weaknesses and flaws.

Many health care providers will need to make changes to reduce risks and to comply with the HIPAA Rules and Meaningful Use requirements. Fortunately, properly configured and certified EHRs[58] can provide more protection to ePHI than paper files provided. (See Step 5A in Chapter 6 for more information about using electronic capabilities to help safeguard patients' information.)

Your EHR Software and Hardware

Most EHRs and related equipment have security features built in or provided as part of a service, but they are not always configured or enabled properly.

As the guardian of ePHI, it is up to you — along with your designated staff members — to learn about these basic features and ensure they are functioning and are updated when necessary. **You and your staff must keep up-to-date with software upgrades and available patches.**

Remember, security risk analysis and mitigation is an ongoing responsibility for your practice. Vigilance should be part of your practice's ongoing activities.

Encryption 101

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text. For more information about encryption, review the National Institute of Standards and Technology (NIST) *Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices*.[59]

[58] http://oncchpl.force.com/ehrcert
[59] http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Working with Your EHR and Health IT Developers

When working with your EHR and health information technology (health IT) developers, you may want to ask the following questions to help understand the privacy and security practices they put in place.[60]

- When my health IT developer installs its software for my practice, does its implementation process address the security features listed below for my practice environment?
    - ePHI encryption
    - Auditing functions
    - Backup and recovery routines
    - Unique user IDs and strong passwords
    - Role- or user-based access controls
    - Auto time-out
    - Emergency access
    - Amendments and accounting of disclosures
- Will the health IT developer train my staff on the above features so my team can update and configure these features as needed?
- How much of my health IT developer's training covers privacy and security awareness, requirements, and functions?
- How does my backup and recovery system work?
    - Where is the documentation?
    - Where are the backups stored?
    - How often do I test this recovery system?
- When my staff is trying to communicate with the health IT developer's staff, how will each party authenticate its identity? For example, how will my staff know that an individual who contacts them is the health IT developer representative and not a hacker trying to pose as such?
- How much remote access will the health IT developer have to my system to provide support and other services? How will this remote access be secured?
- If I want to securely email with my patients, will this system enable me to do that as required by the Security Rule?

[60] For additional information about questions to ask health IT developers, see the Questions for EHR Developers document at http://bit.ly/EHRdevqs.

Cybersecurity

An Internet connection is a necessity to conduct the many online activities that can be part of EHR and ePHI use. Exchanging patient information electronically, submitting claims electronically, generating electronic records for patients' requests, and e-prescribing are all examples of online activities that rely on cybersecurity practices to safeguard systems and information.

The Threat of Cyber-Attacks

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

Cybersecurity refers to ways to prevent, detect, and respond to attacks against or unauthorized access against a computer system and its information. Cybersecurity protects your information or any form of digital asset stored in your computer or in any digital memory device.

It is important to have strong cybersecurity practices in place to protect patient information, organizational assets, your practice operations, and your personnel, and of course to comply with the HIPAA Security Rule.[61] Cybersecurity is needed whether you have your EHR locally installed in your office or access it over the Internet from a cloud service provider.

The Office of the National Coordinator for Health Information Technology (ONC) offers online Cybersecurity information,[62] including the Top 10 Tips for Cybersecurity in Health Care, to help you reduce your risk. For a full overview of security standards and required protections for ePHI under the HIPAA Security Rule, visit OCR's HIPAA Security Rule web page.[63]

Mobile Devices

The U.S. Department of Health and Human Services (HHS) has put together a collection of tips and information[64] to help you protect and secure health information that you may access, receive, and store on mobile devices such as smartphones, laptops, and tablets.

[61] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[62] http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility
[63] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[64] http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Email and Texting

Consumers increasingly want to communicate electronically with their providers through email or texting. The Security Rule requires that when you send ePHI to your patient, you send it through a secure method and that you have a reasonable belief that it will be delivered to the intended recipient. The Security Rule, however, does not apply to the patient. A patient may send health information to you using email or texting that is not secure. That health information becomes protected by the HIPAA Rules when you receive it.

In this environment of more online access and great demand by consumers for near real-time communications, you should be careful to use a communications mechanism that allows you to implement the appropriate Security Rule safeguards, such as an email system that encrypts messages or requires patient login, as with a patient portal. If you use an EHR system that is certified under ONC's 2014 Certification Rule, your EHR should have the capability of allowing your patients to communicate with your office through the office's secure patient portal.[65]

If you attest to Meaningful Use and use a certified EHR system, you should be able to communicate online with your patients. The EHR system should have the appropriate mechanisms in place to support compliance with the Security Rule. You might want to avoid other types of online or electronic communication (e.g., texting) unless you first confirm that the communication method meets, or is exempt from, the Security Rule.[66]

[65] 45 CFR 170.315(e)(3).
[66] 45 CFR 164.312(e)(1).

Chapter 5

Medicare and Medicaid EHR Incentive Programs Meaningful Use Core Objectives that Address Privacy and Security

Meaningful Use

In the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (also called "Meaningful Use" Programs), the Centers for Medicare and Medicaid Services (CMS) set staged requirements for providers to demonstrate progressively more integrated use of EHRs and receive incentive payments for such use.

The first version (1.2) of this Guide discussed two of the Stage 1 core objectives that relate to privacy and security requirements. This updated Guide focuses on Stage 1 and Stage 2 core objectives that address privacy and security, but it does not address menu objectives, clinical quality measures, or Stage 3. Visit the CMS Medicare and Medicaid EHR Incentive Programs web page[68] for information about incentive payment year requirements.

Privacy in Meaningful Use

Simply stated, Meaningful Use privacy requirements address patients' rights both to:

1. Have their health information protected from unauthorized access; and
2. Access their health information.

Security in Meaningful Use

The Meaningful Use security requirements protect Protected Health Information (PHI) against unauthorized access. The program requires Stage 1 and 2 core objectives that can be found on the CMS website.[67]

[67] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/
[68] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/

General Overview of Stage 1 and Stage 2 Meaningful Use

Meaningful Use[69] must be demonstrated by:

- Using the capabilities of Certified EHR Technology (CEHRT) adopted by the U.S. Department of Health and Human Services (HHS) as standards, implementation specifications, and certification criteria (in the Office of the National Coordinator for Health Information Technology's Standards and Certification Criteria regulations),[70] and
- Meeting CMS-defined criteria through a phased approach based on anticipated technology and capabilities development.

To define meaningful use, CMS sought to balance the sometimes competing considerations of improving health care quality, encouraging widespread EHR adoption, promoting innovation, and avoiding imposing excessive or unnecessary burdens on health care providers.[71]

The Stage 1 Meaningful Use criteria, consistent with other provisions of Medicare and Medicaid law, focuses on:

- Electronically capturing health information in a structured format;
- Using that information to track key clinical conditions and communicating that information for care coordination purposes (whether that information is structured or unstructured, but in structured format whenever feasible);
- Implementing clinical decision support tools to facilitate disease and medication management;
- Using EHRs to engage patients and families; and
- Reporting clinical quality measures and public health information.[72]

The Stage 2 Meaningful Use criteria, consistent with other provisions of Medicare and Medicaid law, expanded upon the Stage 1 criteria to encourage the use of health information technology (health IT) for continuous quality improvement at the point of care and the exchange of information in the most structured format possible. Examples of such use include the electronic transmission of orders entered using Computerized Provider Order Entry (CPOE) and the electronic transmission of diagnostic test results (such as blood tests, microbiology, urinalysis, pathology tests, radiology, cardiac imaging, nuclear medicine tests, pulmonary function tests, genetic tests, genomic tests and other such data needed to diagnose and treat disease).[73]

---

[69] http://www.healthit.gov/policy-researchers-implementers/meaningful-use
[70] 79 Federal Register (FR) 54429. See also the "ONC Fact Sheet: 2015 Edition Health IT Certification Criteria, Base EHR Definition, and ONC Health IT Certification Program Modifications Proposed Rule" at http://www.healthit.gov/sites/default/files/ONC-Certification-Program-2015-Edition-Fact-Sheet.pdf.
[71] 75 FR 44321.
[72] 75 FR 44321.
[73] 77 FR 64755.

To demonstrate Meaningful Use, providers must meet measures and report the use of their practices' EHRs to CMS via attestation. The Meaningful Use Programs define Eligible Professionals (EPs) as doctors of medicine or osteopathy, dental surgery or dental medicine, podiatric medicine, optometry, and chiropractic medicine.[74] Review the CMS flow chart[75] for assistance with determining if you are an EP and to determine whether to select Medicare or Medicaid to demonstrate Meaningful Use.

Both Meaningful Use Stage 1[76] and Stage 2[77] require participating providers to "attest" that they have met certain objectives and measures regarding the use of the EHRs for patient care. The attestation is effectively your confirmation or statement that your practice has met those requirements.

In the Medicare and Medicaid EHR Incentive Programs, specific Meaningful Use requirements incorporate many HIPAA privacy and security requirements for electronic PHI (ePHI). Basic cybersecurity practices are needed to protect the confidentiality, integrity, and availability of health information in the EHR system. These protections are essential whether the EHR is installed on a server in your office or hosted on your behalf by a developer over the Internet.

[74] EPs may *not* be hospital-based. Hospital-based EPs are any provider who furnishes 90% or more of their services in a hospital setting (inpatient or emergency room).
[75] http://cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/eligibility_flow_chart.pdf
[76] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html
[77] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html

Chapter 6

Sample Seven-Step Approach for Implementing a Security Management Process

Introduction

This chapter describes a sample seven-step approach that could be used to implement a security management process in your organization and includes help for addressing security-related requirements of Meaningful Use for the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs. The Meaningful Use requirements for privacy and security (discussed in Chapter 5) are grounded in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This approach does not cover all the requirements of Meaningful Use and the HIPAA Rules, but following this approach may help you fulfill your compliance responsibilities. This is a sample approach for security management, although occasionally we note related privacy activities.

How to Get Started on Security

Before you start, ask your local Regional Extension Center (REC)[78] where you can get help. In addition:

- Check the Office of the National Coordinator for Health Information Technology (ONC) Health IT Privacy and Security Resources web page.[79]
- Review the Office for Civil Rights (OCR) Security Rule Guidance Material.[80]
- Look at the OCR audit protocols.[81]
- Let your EHR developer(s) know that health information security is one of your major goals in adopting an EHR.
- Check with your membership associations to see if they have training resource lists or suggestions.

[78] http://healthit.gov/rec
[79] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[80] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[81] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

- Check to see if your local community college[82] offers any applicable training.
- Discuss with your practice staff, and any other partners you have, how they can help you fulfill your HIPAA Rules responsibilities.

To implement a security management process in your organization, an organized approach to privacy and security is necessary (see Step 2 later in this chapter).

The security management process standard is a requirement in the HIPAA Security Rule. Conducting a risk analysis is one of the requirements that provides instructions to implement the security management process standard. ONC worked with OCR to create a Security Risk Assessment (SRA) Tool[83] to help guide health care providers (from small practices) through the risk assessment process. Use of this tool is not required by the HIPAA Security Rule but is meant to provide helpful assistance.

Before discussing the sample seven-step approach to help providers implement a security management process, one clarification must be emphasized. The scope of a risk analysis for the EHR Incentive Programs security requirements is much narrower than the scope of a risk analysis for the HIPAA Security Rule security management process standard.

The risk analysis requirement in the HIPAA Security Rule is much more expansive. It requires you to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic Protected Health Information (ePHI) that an organization creates, receives, maintains, or transmits — not just the ePHI maintained in Certified EHR Technology (CEHRT). This includes ePHI in other electronic systems and all forms of electronic media, such as hard drives, floppy disks, compact discs (CDs), digital video discs (DVDs), smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.[84] In addition, you will need to periodically review your risk analysis to assess whether changes in your environment necessitate updates to your security measures.

Under the HIPAA Security Rule, the frequency of reviews will vary among providers. Some providers may perform these reviews annually or as needed depending on circumstances of their environment. Under the EHR Incentive Programs, the reviews are required for each EHR reporting period. For Eligible Professionals (EPs), the EHR reporting period will be 90 days or a full calendar year, depending on the provider's year of participation in the program.

[82] http://www.healthit.gov/policy-researchers-implementers/community-college-consortia
[83] http://healthit.gov/providers-professionals/security-risk-assessment-tool
[84] It's not just the ePHI in EHRs but also in practice management systems, claim processing systems, billing, patient flow (bed management), care and case management, document scanning, clinical portals, and dozens of other ancillary systems that don't meet the definition of CEHRT.

Sample Seven-Step Approach for Implementing a Security Management Process

The sample seven steps which will be discussed here are:

Step 1: Lead Your Culture, Select Your Team, and Learn
Step 2: Document Your Process, Findings, and Actions
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)
Step 4: Develop an Action Plan
Step 5: Manage and Mitigate Risks
Step 6: Attest for Meaningful Use Security-Related Objective
Step 7: Monitor, Audit, and Update Security on an Ongoing Basis

Step 1: Lead Your Culture, Select Your Team, and Learn

Your leadership — especially your emphasis on the importance of protecting patient information — is vital to your practice's privacy and security activities. Your commitment to an organized plan and approach to integrating privacy and security into your practice is important.

This first step in your seven-step approach presents six actions that you should take to set the stage for implementing an effective security management process for your organization. Each of these six actions is discussed below.

1A. Designate a Security Officer(s)
1B. Discuss HIPAA Security Requirements with Your EHR Developer
1C. Consider Using a Qualified Professional to Assist with Your Security Risk Analysis
1D. Use Tools to Preview Your Security Risk Analysis
1E. Refresh Your Knowledge Base of the HIPAA Rules
1F. Promote a Culture of Protecting Patient Privacy and Securing Patient Information

Step 1A: Designate a Security Officer(s)

Your security officer will be responsible for developing and maintaining your security practices to meet HIPAA requirements. This person could be part of your EHR adoption team and should be able to work effectively with others.

A security officer is responsible for protecting your patients' ePHI from unauthorized access by working 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, information technology (IT) administrator or consultant, your EHR developer, and legal counsel.

When you designate your officer(s), be sure to:

- Record all officer assignments in a permanent documentation file (this file should focus on HIPAA compliance efforts), even if you are the officer(s).
- Discuss your expectations for the officer and his/her accountability. Note that you, as a Covered Entity (CE), retain ultimate responsibility for HIPAA compliance.
- Enable your designated officer(s) to develop a full understanding of the HIPAA Rules so they can succeed in their roles. For example, allow them time to participate in privacy and security presentations, seminars, and webinars and to read and review the Final Rules and the analysis and summaries on the ONC Health IT Privacy and Security Resources web page,[85] including the helpful OCR audit protocols.[86] Have them use the ONC Cybersecure training games[87] as a useful training tool.

Step 1B: Discuss HIPAA Security Requirements with Your EHR Developer

As you prepare for the security risk analysis, meet with your EHR developer to understand how your system can be implemented in a manner consistent with the HIPAA requirements and those for demonstrating Stage 1 and Stage 2 Meaningful Use (see Chapters 4 and 5).

- Before you purchase an EHR, perform your due diligence by discussing and confirming privacy and security compliance requirements and product capabilities. Refer to the listing of CEHRT developers[88] as you proceed.
- If you have implemented an EHR, confirm your practice's understanding of the overall functions that your EHR product offers and then assess your current security settings.
- You would want to make sure that the EHR system can be configured to your policies and procedures and that the EHR will sign a Business Associate Agreement (BAA) that reflects your expectations. Confirm any planned additional capabilities that you need or that your EHR developer is responsible for providing, especially if any are required to demonstrate Meaningful Use. Ask the developer for its pricing for training staff on those functions, developing relevant policies and procedures, and correcting security-setting deficiencies in the EHR system.

Step 1C: Consider Using a Qualified Professional to Assist with Your Security Risk Analysis

Your security risk analysis must be conducted in a manner consistent with the HIPAA Security Rule, or you will lack the information necessary to effectively protect ePHI. Note that doing the analysis in-house

[85] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[86] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
[87] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[88] http://oncchpl.force.com/ehrcert?q=chpl

may require an upfront investment of your time and a staff member's time to understand and address electronic information security issues and the HIPAA Security Rule.

- A qualified professional's expertise and focused attention can often yield quicker and more reliable results than if your staff does an in-house risk analysis in a piecemeal process spread over several months. Certification (see box at right) can be one indicator of qualifications. The professional will suggest ways to mitigate risks so you can avoid the need to research and evaluate options yourself.
- 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.

You are still ultimately responsible for the security risk analysis even if you hire a professional for this activity. Further, the security risk analysis will require your direct oversight and ongoing involvement.

The security risk analysis process is an opportunity to learn as much as possible about health information security. See Step 3 in this chapter for more discussion about security risk analyses.

Certification in Health Information Security

Some professionals have a certification in health information. For example, the Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA) are two organizations that offer certifications upon successful completion of an exam.

Certified in Healthcare Privacy and Security (CHPS)

This credential is designated to professionals who are responsible for safeguarding patient information. This credential signifies expertise in planning, executing, and administering privacy and security protection programs in health care organizations and competence in a specialized skill set in the privacy and security aspects of health information management.

Certified Professional in Healthcare Information and Management Systems (CPHIMS)

CPHIMS is a professional certification program for health care information and management systems professionals.

Step 1D: Use Tools to Preview Your Security Risk Analysis

Have your security officer or security risk professional consultant use tools available on the ONC and OCR websites to get a preliminary sense of potential shortcomings in how your practice protects patient information. A single listing of areas of focus or a checklist does not fulfill the security risk analysis requirement, but these types of tools will help everyone get ready for needed

improvements. Keep the results as part of your documentation (see Step 2). Consider the SRA Tool[89] and OCR Guidance on Risk Analysis[90] for more thorough guidance in evaluating your level of risk.

Step 1E: Refresh Your Knowledge Base of the HIPAA Rules

Learn about the HIPAA Rules, state laws, and other privacy and security requirements that also require compliance.

Step 1F: Promote a Culture of Protecting Patient Privacy and Securing Patient Information

Privacy and security are best achieved when the overall atmosphere in your office emphasizes confidentiality and protecting of patient information. Culture sets the tone that will:

- Consistently communicate your expectations that all members of your workforce protect patients' health information
- Guide your workforce's efforts to comply with, implement, and enforce your privacy and security policies and procedures
- Remind staff why securing patient information is important to patients and the medical practice

Step 2: Document Your Process, Findings, and Actions

Documentation of a risk analysis and HIPAA-related policies, procedures, reports, and activities is a requirement under the HIPAA Security Rule. Also, the Centers for Medicare and Medicaid Services (CMS) advise all providers who attest for the EHR Incentive Programs to retain all relevant records that support attestation.

Documentation shows how you did the security risk analysis and implemented safeguards to address the risks identified in your risk analysis. (See the box at right for additional items to include in your documentation folder.)

Over time, your security documentation folder will become a tool that helps your security procedures be more

Examples of Records to Retain

Contents should include, but not be limited to, the following:

- Your policies and procedures
- Completed security checklists
- Training materials presented to staff and volunteers; any associated certificates of completion
- Updated BA agreements
- Security risk analysis report
- EHR audit logs that show both utilization of security features and efforts to monitor users' actions
- Risk management action plan or other documentation (that shows appropriate safeguards are in place throughout your organization), implementation timetables, and implementation notes
- Security incident and breach information

[89] http://healthit.gov/providers-professionals/security-risk-assessment-tool
[90] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

efficient. Your workforce will be able to reference this master file of security findings, decisions, and actions. Further, the information will be more accurate than if your workforce tries to reconstruct past decisions and actions. These records will be essential if you are ever audited for compliance with the HIPAA Rules[91] or an EHR Incentive Program.

Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)

The risk analysis process assesses potential threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The findings from this analysis inform your risk mitigation strategy.

Before you start, these recommended resources can provide guidance on your security risk analysis:

- OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule[92]
- OCR Security Rule Frequently Asked Questions (FAQs)[93]
- SRA Tool,[94] which helps small practices conduct an extensive, systematic risk analysis
- National Institute of Standards and Technology (NIST) HIPAA Security Rule Toolkit[95]

If you want additional support, a security risk professional can plan and implement this analysis, but you will need to oversee the process. Some commercial security risk analysis products are available, but before you buy, seek out an independent review from a health information security expert.

Your first comprehensive security risk analysis should follow a systematic approach that covers all security risks. It should:

- Identify where ePHI exists in your practice and how it is created, received, maintained, and transmitted, including in your EHR. Types of risks to the ePHI maintained in your EHR will vary depending on whether your EHR is based in your office or hosted on the Internet (e.g., cloud-based or Application Service Provider).
- Identify potential threats and vulnerabilities to ePHI. Potential threats include human threats, such as cyber-attack, theft, or workforce member error; natural threats, such as earthquake,

Tips for a Better Security Risk Analysis

- Educate staff about the iterative and ongoing nature of the security risk analysis process.
- Make security a high priority in your workplace culture.
- Have an action plan that clearly assigns responsibilities for each risk analysis component.
- Involve your EHR developer in the process.
- Ensure that the risk analysis is specific to your situation.

[91] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
[92] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
[93] http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/index.html
[94] http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
[95] http://scap.nist.gov/hipaa/

fire, or tornado; and environmental threats, such as pollution or power loss. Vulnerabilities are flaws or weaknesses that if exploited by a threat could result in a security incident or a violation of policies and procedures.

- Identify risks and their associated levels (e.g., high, medium, low). This is done by assessing the likelihood that threats will exploit vulnerabilities under the safeguards currently in place and by assessing the potential impacts to confidentiality, integrity, and availability of ePHI.

A risk analysis can produce results that may fall into "gray" areas. However, you will be able to see where you are meeting, not meeting, or exceeding HIPAA requirements at a given point in time.

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

All types of EHRs outperform paper medical records when it comes to providing better access to and use of ePHI. On the other hand, EHRs also introduce new risks to ePHI. The mix of security risks is affected, in part, by the type of EHR hosting you have: office-based (local host) or Internet-hosted (remote host). Table 2 offers a few examples of different risks associated with office-based vs. Internet-hosted EHRs.

Table 2: Examples of Potential Information Security Risks with Different Types of EHR Hosts

Host Type	Risk	Examples of Mitigation Steps
Office-Based EHRs	Natural disaster could greatly disrupt the availability of, and even destroy, ePHI.	Always store routine backups offsite.
Office-Based EHRs	You directly control the security settings.	Regardless of your practice size, follow best practices on policies and procedures about access to ePHI. For example, use password controls and automatic logout features.
Office-Based EHRs	The security features on your office-based EHR may not be as up-to-date and sophisticated as an Internet-hosted EHR.	Maintain ongoing communication with your EHR developer about new features and their criticality to the security of the EHR.
Office-Based EHRs	When public and private information security requirements change, you have to figure out how to update your EHR and work out any bugs.	Routinely monitor for changes in federal, state, or private-sector information security requirements and adjust settings as needed.
Internet-Hosted (Cloud-Based) EHRs	You are more dependent on the reliability of your Internet connection. Your data may be stored outside the U.S., and other countries may have different health information privacy and security laws that may apply to such offshore data.	Confirm that your EHR host follows U.S. security standards and requirements.
Internet-Hosted (Cloud-Based) EHRs	The developer may control many security settings.	The adequacy of these settings may be hard to assess, but ask for specific information.
Internet-Hosted (Cloud-Based) EHRs	In the future, the developer might request extra fees to update your EHR for compliance as federal, state, and private-sector information security requirements evolve.	Ensure your EHR stays compliant. Before you buy, it is OK to ask your developer about fees it may charge for security updates.

Step 4: Develop an Action Plan

Using the results from your risk analysis, discuss and develop an action plan to mitigate the identified risks. Your action plan is informed by your risk analysis and should focus on high priority threats and vulnerabilities. Take advantage of the flexibility that the HIPAA Security Rule provides, which allows you to achieve compliance while taking into account the characteristics of your organization and its

environment. It is important that your security plan is feasible and affordable for your practice. Often, basic security measures can be highly effective and affordable (see box below).

Action Plan Components

The plan should have five components:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational standards
- Policies and procedures

These components correspond with the security components specified in the table on the next page. Table 3 briefly outlines each component and provides examples.

Low-Cost, Highly Effective Safeguards

- Say "no" to staff requests to take home laptops containing unencrypted ePHI.
- Remove hard drives from old computers before you get rid of them.
- Do not email ePHI unless you know the data is encrypted.
- Make sure your server is in a room accessible only to authorized staff, and keep the door locked.
- Make sure the entire office understands that passwords should not be shared or easy to guess.
- Notify your office staff that you are required to monitor their access randomly.
- Maintain a working fire extinguisher in case of fire.
- Check your EHR server often for viruses and malware.

Table 3: Five Security Components for Risk Management

Security Component	Examples of Vulnerabilities	Examples of Security Mitigation Strategies
Administrative Safeguards	• No security officer is designated. • Workforce is not trained or is unaware of privacy and security issues. • Periodic security assessment and	• Security officer is designated and publicized. • Workforce training begins at hire and is conducted on a regular and frequent basis. • Security risk analysis is performed periodically and when a change occurs in the practice or the technology.
Physical Safeguards	• Facility has insufficient locks and other barriers to patient data access. • Computer equipment is easily accessible by the public. • Portable devices are not tracked or not locked up when not in use.	• Building alarm systems are installed. • Offices are locked. • Screens are shielded from secondary viewers.
Technical Safeguards	• Poor controls allow inappropriate access to EHR. • Audit logs are not used enough to monitor users and other EHR activities. • No measures are in place to keep electronic patient data from improper changes. • No contingency plan exists. • Electronic exchanges of patient information are not encrypted or otherwise secured.	• Secure user IDs, passwords, and appropriate role-based access are used. • Routine audits of access and changes to EHR are conducted. • Anti-hacking and anti-malware software is installed. • Contingency plans and data backup plans are in place. • Data is encrypted.
Organizational Standards	• No breach notification and associated policies exist. • Business Associate (BA) agreements have not been updated in several years.	• Regular reviews of agreements are conducted and updates made accordingly.
Policies and Procedures	• Generic written policies and procedures to ensure HIPAA security compliance were purchased but not followed. • The manager performs ad hoc security measures.	• Written policies and procedures are implemented and staff is trained. • Security team conducts monthly review of user activities. • Routine updates are made to document security measures.

For any single risk, a combination of safeguards may be necessary because there are multiple potential vulnerabilities. For example, ensuring appropriate and continuous access to patient information may require something as simple as a physical safeguard of adding a power surge protection strip, putting the server in a locked room, and being meticulous about backups. Your action plan should have multiple combinations of the five required components. Although the steps are sequential, the security components are interrelated.

Learn more about these requirements through the HIPAA Security Rule Educational Paper Series,[96] the ONC Cybersecurity web pages,[97] and the Cybersecure training games.[98]

Process for Developing the Plan

Your security officer (see Step 1A) will need to convene the team to develop the security action plan. Begin by identifying the simple actions that can reduce the greatest risks.

If your staff is unsure how specific HIPAA requirements might apply to your specific practice, review OCR Security Rule Guidance[99] or other materials on ONC's Health IT Privacy and Security Resources web page.[100] Ask your security risk professional or legal counsel for help as needed.

Once the plan is written, your designated security team should meet periodically to coordinate actions, work through unexpected snags, and track progress. Reward your team as it achieves milestones. Understand that you will not be able to eliminate risk, but you will be able to lower it by implementing safeguards that reduce risk and vulnerabilities. More about implementing the action plan is in Step 5 below.

Step 5: Manage and Mitigate Risks

Once you have an action plan, follow it to reduce security risks and better protect ePHI. This step has four parts, each of which is discussed below.

Key Questions to Ask as You Plan

Who has keys to your practice?

Establish and follow a policy regarding keys and passwords. Ensure that access keys are returned before employees or contractors leave your practice. If any former employees and contractors have keys, change the locks. Do not forget about "virtual" keys like administrator accounts to your EHR or database — be sure to change these passwords periodically.

Where, when, and how often do you back up? Do you have at least one backup kept offsite? Can your data be recovered from the backups?

Periodically test your backup system to confirm you can retrieve your data backups when needed.

What is your contingency/ disaster plan when/if your server crashes and you cannot directly recover data?

Always maintain developer documentation that provides contact information and the serial numbers of your server and other hardware and software used, etc. Keep one copy offsite in a secure place.

[96] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[97] http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility
[98] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[99] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[100] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

5A. Implement Your Action Plan (which includes using applicable EHR security settings and updating your HIPAA-related policies and procedures)
5B. Prevent Breaches by Educating and Training Your Workforce
5C. Communicate with Patients
5D. Update Your BA Contracts

Throughout this process, continue your efforts to build a culture that values patients' health information and actively protects it. One easy way is to give your staff time to play ONC's Cybersecure training games.[101] The games are a fun and engaging way to provide answers to many of the everyday questions around safeguarding PHI.

Step 5A: Implement Your Action Plan

The goal of following your security risk action plan is to protect patient ePHI through ongoing efforts to identify, assess, and manage risks. As discussed in Step 4, your action plan, regardless of how it is organized, should address all five HIPAA security components:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational standards
- Policies and procedures

This section focuses on technical safeguards and policies and procedures. Chapter 4 and Chapter 6 (Steps 1, 4, and 5D) provide additional information about these five components.

Information Security Settings in Your EHR

If an EHR is certified,[102] it has a package of core technical security functions, such as the ability to authenticate users with valid accounts. However:

- Use of CEHRT does not mean that your practice is "HIPAA compliant."
- Certification does not guarantee performance or reliability of security functions in CEHRT, especially if you turn off functions that are important to Privacy and Security Rule compliance.
- The security functions of the CEHRT may be "off," or the settings could be at a suboptimal level — both can create vulnerabilities.

[101] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[102] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html

It is vital that your practice learns about the security settings in your EHR, and your assigned EHR administrator(s) must have access to these settings. Your Health Information Exchange (HIE) may have specific requirements for security settings.

Your risk analysis should specifically examine the adequacy of your EHR security safeguards as your system transmits, stores, and allows modifications to ePHI.

Information Security: Encryption

Per the HIPAA Security Rule, a CE, such as a health care provider, must use encryption if, after implementing its security management process, it determines that encryption is a reasonable and appropriate safeguard in its practice environment to safeguard the confidentiality, integrity, and availability of ePHI.

Need assistance with appropriately configuring your EHR security features? In addition to working with an information security expert, gather information from sources such as:

- ONC's Health IT Privacy and Security Resources web page[103]
- Your EHR developer
- Your state or county medical association

Written Policies and Procedures

With respect to protecting patient information, your policies and procedures guide how your practice operates on a day-to-day basis. Your medical practice policies and procedures should accomplish the following, at minimum:

- Establish protocols for all five security components (administrative, physical, and technical safeguards; organizational standards; and policies and procedures).
- Commit to a HIPAA training program for all new staff when they are hired and on a regular basis for the entire workforce.
- Instruct your workforce on what to do when something happens that impairs the availability, integrity, or confidentiality of ePHI. (Sometimes these instructions are labeled as "incident response" or "breach notification and management" plans.)
- Specify a sanction policy for violations of the Privacy, Security, or Breach Notification Rules or your policies and procedures. Your sanction policy must be applied consistently as written.
- Detail enforcement, starting with the use of your EHR security audit logs to monitor access, use, and disclosure of ePHI.
- Specify the need for written agreements with BAs that detail their specific responsibility to comply with privacy and security.

[103] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

As you make the updates, retain outdated policies and procedures in your security documentation folder as described in Step 2.

Once your written policies and procedures are in place, the HIPAA Rules require that you do the following:

- Train your workforce (see Step 5B) on what is required and how to implement the policies and procedures. HIPAA requires that your workforce be specifically trained on these policies and procedures, including breach notification. Your workforce will need periodic refresher training on new aspects of your security program.
- Confirm that you have identified all your BAs. Contact them and confirm through written agreements that they understand their responsibilities to carry out HIPAA Rules requirements and to inform you of any breaches.
- Consistently apply your policies and procedures when unauthorized access to PHI occurs. Whenever a member of your workforce does not comply with your policies and procedures, he or she must be sanctioned. You must have a sanctions policy in place to ensure all members of the workforce are treated fairly. Document your actions.
- Periodically review your policies and procedures to make sure they are current and your practice adheres to them.
- Update your policies and procedures when changes in your internal or external environment create new risks.
- Retain policies and procedures in your documentation folder for at least six years after you have updated or replaced them (see Step 2). State and private-sector requirements may specify a longer time period for retention.

Step 5B: Prevent Breaches by Educating and Training Your Workforce

Workforce education and training — plus a culture that values patients' privacy — are a necessary part of risk management. All of your workforce members — employees, volunteers, trainees, and contractors supporting your office — need to know how to safeguard patient information in your practice. Your training program should prepare your workforce to carry out:

- Their roles and responsibilities in safeguarding patients' health information and complying with the HIPAA Rules
- Your HIPAA-related policies
- Your procedures, including processes to monitor security and steps for breach notifications

Your workforce may need focused training to develop the requisite skills to perform the steps you require. ONC's Cybersecure training games[104] and mobile device training videos[105] are highly recommended resources.

Reinforce workforce training with reminders. Above all, lead by example by adhering to your policies and procedures.

Frequency of Workforce Training

Your practice must educate and train individual workforce members at the time each person is hired or contracted. Industry best practices suggest that the entire workforce should be trained at least once every year and any time your practice changes its policies or procedures, systems, location, infrastructure, etc. It is particularly important that your workforce be trained on how to respond immediately to any potential security incidents or an unauthorized disclosure of ePHI because these situations may be breaches.

Making Protecting Patient Information Part of Your Routine

Deliberately create a culture that emphasizes PHI confidentiality. You can do this in a number of ways, which include:

- Speaking often about the importance of trust in the patient-provider relationship. Remind your workforce that patients expect your practice to be a good steward of their health information.
- Continually reminding staff to safeguard patient confidentiality and the security of ePHI.
- Making sure your staff has a copy of your policies and procedures for easy reference. Remind them to comply with those policies and procedures.
- Addressing staff questions, and getting outside resources to help if you feel you need additional expertise with message delivery.
- Reassessing each workforce member's job functions and enabling him/her to access only the minimum necessary health information as appropriate.

Step 5C: Communicate with Patients

Your patients may be concerned about the confidentiality and security of their health information in an EHR. Don't wait for them to ask. Instead, provide them with information about EHRs, especially the

[104] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[105] http://www.healthit.gov/providers-professionals/worried-about-using-mobile-device-work-heres-what-do-video

benefits EHRs can bring to them as patients. Reassure patients that you have a system to proactively protect the privacy and security of their health information. Your staff should be able to speak to the confidentiality and security of your EHR as well.

To preserve good patient relations, follow your policies and procedures for communicating with patients and caregivers if a breach of unencrypted ePHI ever occurs. As explained in Chapter 7, OCR and most state attorneys general strictly enforce breach procedures.

A multi-faceted communications plan will help you avert patient concerns about EHRs and privacy.

- Inform patients that you place a priority on maintaining the security and confidentiality of their health information. ONC and other federal agencies have developed consumer education handouts[106] that you may want to use or adapt.
- Address patients' individual health information rights, which include the right to access or obtain a copy of their electronic health record in an electronic form.
- 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 permission (consent or authorization) prior to exchanging his/her health information.
- Notify affected patients and caregivers when a breach of unsecured PHI has occurred, in accordance with your updated policies and procedures.

Patient relations on security issues should be an integral part of your overall patient engagement strategy.[107]

Consumer communications should be culturally appropriate. Consider the various languages, communication needs, and trust levels of different patient populations. If a particular group has some distrust of the medical establishment, take extra steps to reassure them that you are safeguarding their information.

Be prepared to discuss and answer the questions that concerned patients and their caregivers may have. For ideas, visit the ONC Health IT Privacy and Security Resources web page,[108] which provides other materials for you and your patients.

[106] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[107] http://www.healthit.gov/patients-families/protecting-your-privacy-security and http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf
[108] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

Fulfill Your Responsibilities for Patients' Health Information Rights[109]

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 made in their records. As part of the HIPAA Rules and Stage 2 Meaningful Use, you must respond to these patient requests. In particular:

- Patients can request copies of and access to their PHI in paper or electronic format, including from your EHR. Meaningful Use Core Objectives indicate that such ePHI held in the EHR should be made available to patients, upon request, **within four business days** of it being available to the provider (see Chapter 3).
- Patients can request corrections and amendments to the PHI in their records; this is called a "right to amend" and has always been part of the HIPAA Rules. Now Stage 2 Meaningful Use Objective 9 **requires you to respond to patients' requests to amend their ePHI that is in your EHR**.
- Under the Privacy Rule, a patient, or another person on a patient's behalf, can ask his/her provider to restrict submission of his/her PHI to the patient's health plan **when the patient has paid in full** for the health care service or item — and the provider must honor that request.

To prepare for patient requests, ask your EHR developer about ways to use your system to help you fulfill individual patient rights. For example, confirm what EHR capabilities are currently available and when additional capabilities will be available (such as amendments to and copies of their ePHI). Your developer or other expert consultant may also be able to assist you in implementing these features both in your EHR and your practice workflow. Ask your EHR developer to provide step-by-step instructions or best practice guidelines that include screen shots on how to perform these actions.

Once you have established a process and procedure on how to provide patients with a copy of their medical information from your EHR, develop an understanding of and procedures for what to do when patients ask you to modify or to amend their health information, restrict disclosure, or obtain a report about prior disclosures. (See Chapter 2.)

Online Communications with Patients

If you plan to interact with patients via online platforms (e.g., email, texting, a patient portal for your EHR, or social media), you must meet the Security Rule and Meaningful Use standards for the secure messaging of ePHI.

[109] OCR's patient access memo may be a helpful resource regarding patients' health information rights: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf

Remember that a provider who is emailing and texting patients and/or other providers is creating a security risk for the ePHI unless the transmission is encrypted. See the sidebar "Email and Texting" in Chapter 4 and visit the ONC website for information about the risks of emailing via mobile devices[110] and texting health information.[111] Read the Stage 2 EP Meaningful Use Core and Menu Measures Table of Contents.[112] If you have continued questions, obtain guidance from appropriate legal counsel.

Step 5D: Update Your BA Contracts

Be sure to update all your BA agreements to comply with the HIPAA Privacy, Security, and Breach Notification Rules.[113] (Refer to Chapter 2 for a refresher on the definition of a BA.) Such agreements should require your BAs to:

- Fully comply with relevant safeguards for PHI that they get from your practice
- Train their workforce
- Adhere to additional requirements for patient rights and breach notification

OCR offers sample BA contract provisions.[114]

Developers Supporting Health Information Exchange Are Often Considered BAs

Developers that support your practices through cloud computing/storage or secure physical storage facilities are most likely among your practice's BAs.

Step 6: Attest for Meaningful Use Security-Related Objective

The EHR Incentive Programs provide incentive payments to EPs as they demonstrate adoption, implementation, upgrading, and meaningful use of CEHRT. These Meaningful Use Programs are designed to support providers with the health information technology (health IT) transition and instill the use of EHRs to improve the quality, safety, and efficiency of patient health care.

Providers can register for the EHR Incentive Programs[115] anytime, but attesting requires you to have met the Meaningful Use requirements for an EHR reporting period. So, only attest for an EHR Incentive Program after you have fulfilled the security risk analysis requirement and have documented your efforts. Specifically, you should not attest until you have conducted your security risk analysis (or reassessment) *and* corrected any deficiencies identified during the risk analysis. Document these changes.

[110] http://www.healthit.gov/providers-professionals/faqs/can-you-use-email-send-health-information-using-your-mobile-device
[111] http://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p
[112] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_MeaningfulUseSpecSheet_TableContents_EPs.pdf
[113] Modifications to the Rules expand the types of entities considered BAs and place more obligations on BAs to strictly follow the HIPAA Security Rule.
[114] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
[115] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html

When you attest[116] 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 Programs can be audited.

If you attest prior to actually meeting the Meaningful Use security requirement, it is possible you could increase your business liability for violating federal law and making a false claim. Consult with appropriate legal counsel for further guidance. From this perspective, consider implementing multiple security measures prior to attesting. The priority would be to mitigate high-impact and high-likelihood risks.

Step 7: Monitor, Audit, and Update Security on an Ongoing Basis

Step 7 relates to the HIPAA Security Rule requirements that you have audit controls in place and have the capability to audit. HIPAA uses the term "audit" in two ways. In the first context, audit is what you *do* to monitor the adequacy and effectiveness of your security infrastructure and make needed changes.

- Have your security officer, IT administrator, and EHR developer work together so your system's monitoring/audit functions are active and configured to your needs. They may want you to:
    - Decide whether you will conduct the audits in-house, use an information security consultant, or have a combination of the two
    - Determine what to audit and how the audit process will occur
    - Identify trigger indicators — or signs that ePHI could have been compromised and further investigation is needed
    - Establish a schedule for routine audits and guidelines for random audits

In the second context, audit refers to an effort to *examine* what happened. This means your EHR must be set up to maintain retrospective documentation (i.e., an "audit log") on who, what, when, where, and how your patients' ePHI has been accessed. Such audits (i.e., the auditing process, which would examine logs) are required security technical capabilities that would be part of your Stage 1 and 2 Meaningful Use demonstrations. These capabilities include auditable events and tamper resistance, audit logs, access control and authorizations, automatic logoff, and emergency access (see Stage 2 Meaningful Use Core Measure 9[117] for more description).

Your audit controls and capabilities should be scaled to your practice's size. For example, your certified EHR has a function to generate audit logs. This means it can record when, where (e.g., which laptop), and how ePHI is accessed; by whom; what the individual did; and for what purposes. Your EHR can then produce reports using these data. Such audit logs are useful tools for both holding your workforce

[116] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html
[117] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_9_ProtectElectronicHealthInfo.pdf

accountable for protecting ePHI and for learning about unexpected or improper modifications to patient information.

Medical Record Retention

As you know, state law requires you to store medical records for a specified number of years. Your obligations and the length of time to maintain patient medical records recorded in an EHR are usually also a matter of your state's medical record retention laws. These laws are often found in a state's licensing laws.

If one of your BAs is an HIE, your written agreement with the HIE should require it to return or securely dispose of the ePHI it creates, receives, maintains, or transmits on behalf of your practice (the CE).

This Guide is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this Guide.

Chapter 7

Breach Notification, HIPAA Enforcement, and Other Laws and Requirements

Covered Entities (CEs) and Business Associates (BAs) that fail to comply with Health Insurance Portability and Accountability Act (HIPAA) Rules can receive civil and criminal penalties.

Civil Penalties

The Office for Civil Rights (OCR) is able to impose civil penalties for organizations that fail to comply with the HIPAA Rules. The potential civil penalties are substantial. Your good faith effort to be in compliance with the HIPAA Rules is essential.

State attorneys general also may bring civil actions and obtain damages on behalf of state residents for violations of the HIPAA Rules.[118] Learn more about OCR's HIPAA enforcement;[119] HIPAA Privacy, Security, and Breach Notification Audit Program;[120] and HIPAA Enforcement Rule.[121]

Criminal Penalties

The U.S. Department of Justice investigates and prosecutes criminal violations of HIPAA. Under HIPAA, the Justice Department can impose criminal penalties for:

Oversight

OCR, within the U.S. Department of Health and Human Services (HHS), administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules. OCR conducts complaint investigations, compliance reviews, and audits. OCR may impose penalties for failure to comply with the HIPAA Rules.

The Centers for Medicare and Medicaid Services (CMS) within HHS oversees the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs.

The Office of the National Coordinator for Health Information Technology (ONC) provides support for the adoption and promotion of health information technology (health IT) and Health Information Exchanges (HIEs) to improve health care in the United States.

[118] This authority was granted to state attorneys general in the Health Information Technology for Economic and Clinical Health (HITECH) Act.
[119] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
[120] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
[121] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html

- Knowing misuse of unique health identifiers[122]
- Knowing and unpermitted acquisition or disclosure of Protected Health Information (PHI)[123]

The Breach Notification Rule: What to Do If You Have a Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of unsecured PHI is presumed to be a breach unless the CE or BA demonstrates (based on a risk assessment) that there is a low probability that the PHI has been compromised.[124] When a breach of unsecured PHI occurs, the Rules require your practice to notify affected individuals, the Secretary of HHS, and, in some cases, the media.[125]

The Breach Notification Rule requires HIPAA CEs to notify individuals and the Secretary of HHS of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI. In particular, health care providers must promptly notify the Secretary of HHS if there is any breach of unsecured PHI that affects 500 or more individuals, and they must 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 CE must notify the Secretary and affected individuals. 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.[126]

- Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to Personal Health Record (PHR) developers and their third-party service providers.

If you can demonstrate through a risk assessment that there is a low probability that the use or disclosure compromised unsecured PHI, then breach notification is not necessary. (Please note that this breach-related risk assessment is different from the periodic security risk analysis required by the Security Rule).

And, if you encrypt your data in accordance with the OCR guidance regarding rendering data unusable, unreadable, or indecipherable, you may avoid reporting what would otherwise have been a reportable

[122] HIPAA regulations specify the appropriate use of identifiers.
[123] The HIPAA Privacy Rule establishes what is an impermissible obtainment or disclosure of PHI.
[124] http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
[125] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[126] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

breach. Remember, encryption depends on the encryption key being kept highly confidential, so do not store it with the data or in a location that would compromise it.[127]

Table 4 compares secured and unsecured PHI.

Table 4: Comparison of Secured and Unsecured PHI

Secured PHI	Unsecured PHI
An unauthorized person cannot use, read, or decipher any PHI that he/she obtains because your practice: • Encrypts the information; or • Clears, purges, or destroys media (e.g., data storage devices, film, laptops) that stored or recorded PHI; • Shreds or otherwise destroys paper PHI. (These operations must meet applicable federal standards.[128])	An unauthorized person may use, read, and decipher PHI that he/she obtains because your practice: • Does not encrypt or destroy the PHI; or • Encrypts PHI, but the decryption key has also been breached.

Risk Assessment Process for Breaches

When you suspect a breach of unsecured PHI has occurred, first conduct a risk assessment[129] in order to examine the likelihood that the PHI has been compromised. For you to demonstrate that a breach has not compromised PHI, your practice must conduct the risk assessment in good faith and by thoroughly assessing at least the four required elements[130] listed below.

- The nature and extent of the PHI involved in the use or disclosure, including the types of identifiers and the likelihood that PHI could be re-identified
    - As noted above, if your practice has a breach of encrypted data — and if you had followed standard encryption specifications — it would not be considered a breach of unsecured data, and you would not have to report it.
- The unauthorized person who used the PHI or to whom the disclosure was made (e.g., a sibling or a journalist)

[127] Federal Register (FR). (24 August, 2009). Rules and Regulations. II.A. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (Vol. 74, No. 162). Paragraph 3, pp. 42741-42.
[128] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
[129] 45 Code of Federal Regulations (CFR) 164.402(2); http://www.ecfr.gov/cgi-bin/text-idx?SID=938e08839465e82e2c30c3bd4a359ce2&node=pt45.1.164&rgn=div5#se45.1.164_1402
[130] The four elements are taken from the "Definition of Breach" section at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/.

- The likelihood that any PHI was actually acquired or viewed (e.g., an audit trail would provide insights)
- The extent to which the risk to the PHI has been mitigated (e.g., promptly changed encryption key)

When performing this assessment, you should address each element separately and then analyze the combined four elements to determine the overall probability that PHI has been compromised. The conclusions from your assessment must be reasonable. You have the burden of demonstrating that a use or disclosure of unsecured PHI did not constitute a breach. If this assessment indicates that there is:

- Low probability of compromised PHI, then the use or disclosure is not considered to be a breach and no notification is necessary.
- Probability of compromised PHI, breach notification is required.

Reporting Breaches

If you choose not to conduct the risk assessment, or if, after performing the risk assessment outlined above, you determine that breach notification is required, there are three types of notification to be made to individuals, to the Secretary of HHS, and, in some cases, to the media. The number of individuals that are affected by the breach of unsecured PHI determines your notification requirements. Visit the OCR Breach Notification Rule web page[131] for more information on notifying individuals, the Secretary, and the media.

If you determine that breach notification is required, you should also visit the OCR website for instructions[132] on how to submit the breach notification form[133] to the Secretary of HHS. Once notified, HHS publicly reports, on the OCR website,[134] breaches that affect 500 or more individuals. OCR opens a compliance review of all reported breaches that affect 500 or more individuals and many breaches affecting fewer than 500. (Note that similar breach notification provisions, which are implemented and

[131] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
[132] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[133] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[134] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html

enforced by the Federal Trade Commission,[135] apply to developers of PHRs that are *not* providing this service for a CE.)

Investigation and Enforcement of Potential HIPAA Rules Violations

OCR initiates investigations upon receipt of complaints,[136] breach reports, information provided by other agencies, and the media. The HIPAA Enforcement Rule provides different penalties for each of four levels of culpability:

- Violations that the entity did not know about and would not have known about by exercising reasonable diligence
- Violations due to "reasonable cause"
- Violations due to "willful neglect" that are corrected within 30 days
- Violations due to "willful neglect" that are not corrected within 30 days[137]

Penalties for Violations

Table 5 provides an overview of the penalty amounts for HIPAA violations. Contact your legal counsel for specific guidance.

Table 5: Overview of Penalties

Intent	Minimum Per Incident	Annual Cap for All Violations
Did Not Know or Could Not Have Known	$100 – $50,000	$1.5 million
Reasonable Cause and Not Willful Neglect	$1,000 – $50,000	$1.5 million
Willful Neglect, but Corrected Within 30 Days	$10,000 – $50,000	$1.5 million
Willful Neglect and Not Corrected Within 30 Days	$50,000	$1.5 million

In addition to investigations that OCR conducts for potential violations of the HIPAA Rules, the HITECH Act authorizes and requires HHS to conduct periodic audits to ensure that CEs and BAs comply with the HIPAA Rules.[138] Audits are not initiated because of any particular event or incident, but rather due to application of a set of objective criteria. HHS uses these audits as a way to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews.

[135] http://www.consumer.ftc.gov/
[136] http://www.hhs.gov/ocr/privacy/hipaa/complaints/
[137] 45 CFR 160.404.
[138] HITECH Act, Section 13411.

Other Laws and Requirements

Besides HIPAA Rules, 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. Table 6 provides a snapshot of these domains. Your state, state board of medicine, state associations, Regional Extension Center (REC), and HIE initiatives also may have guidance.

Table 6: Overview of Other Laws and Requirements

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 Human Immunodeficiency Virus (HIV)/Acquired Immune Deficiency Syndrome (AIDS).
	• Applicable federal laws:
	  ○ 42 CFR Part 2: Confidentiality of Alcohol and Drug Abuse
	  ○ Family Educational Rights and Privacy Act (FERPA)
	  ○ Title X of Public Health Service Act — Confidentiality

Adolescent/Minors' Health Information	• State and federal laws generally authorize parent or guardian access.
	• 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.
	• Applicable federal laws:
	  ○ FERPA
	  ○ Genetic Information Nondiscrimination Act (GINA)
	  ○ Title X of Public Health Service Act
	Note: The HIPAA Omnibus Rule clarified that CEs may release student immunization records to schools without authorization if state law requires schools to have immunization records and written or oral agreements (must be documented).

Private Sector	A contracting health plan or payer may require additional confidentiality or safeguards.

A good place to start privacy- and security-related compliance implementation within your practice is to:

- Stay abreast of privacy and security updates. Sign up for OCR's privacy and security listservs[139] to receive updates, and contact your local association to learn about available assistance sources.
- Integrate privacy and security updates into your policies and procedures.
- Identify and monitor violations and demonstrate good faith efforts to promptly cure any violation that may occur.

[139] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html

- Keep your workforce training materials up-to-date and conduct regular training sessions.
- Continually raise your practice's level of awareness about how to minimize the likelihood of privacy and security breaches.

This Guide is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this Guide.