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

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

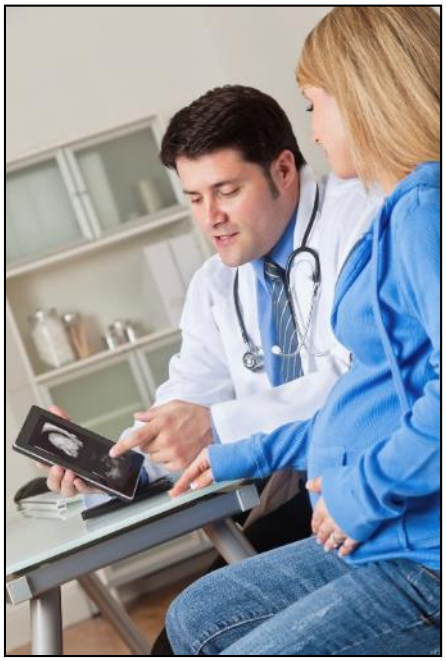
A fourth federal entity mentioned in this Guide is the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. NIST sets computer security standards for the federal government and publishes reports on topics related to information technology (IT) security. 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

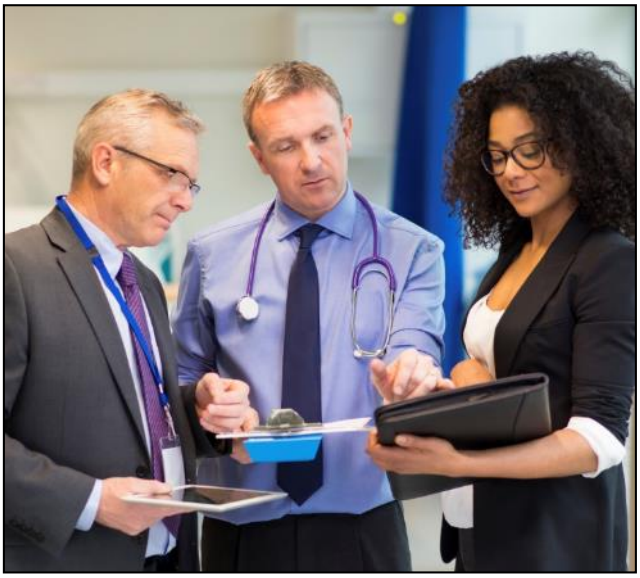
Following are some scenarios to help illustrate who is and who is not a BA. This is not an exhaustive list of examples.

- 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."

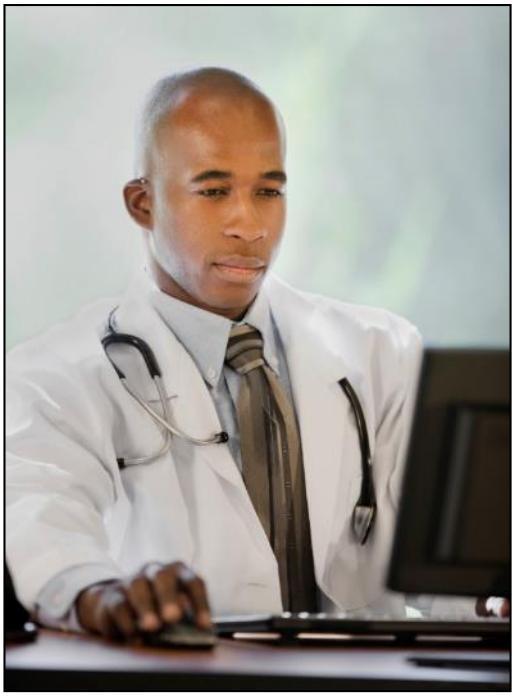
serious and imminent threat to public health or safety; to a health oversight agency for lawful oversight of the originator of the psychotherapy notes; for the lawful activities of a coroner or medical examiner; or as required by law.

- **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.

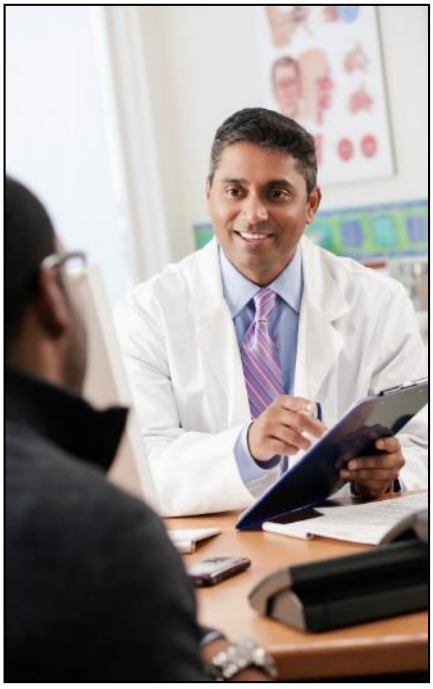
Federal and State Privacy Laws — Which Prevail?

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:

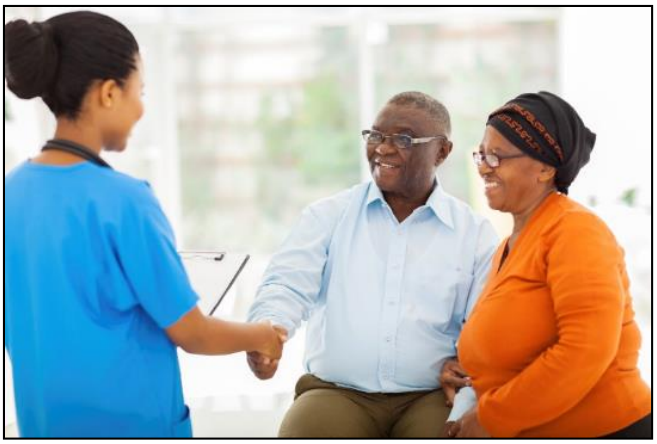
- Description of how your practice may use or disclose (share) an individual's PHI
- Specification of individuals' rights, including the right to complain to the U.S. Department of Health and Human Services (HHS) and to your practice if they believe their privacy rights have been violated (many of these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