Patient's Guide to HIPAA

How to Use the Law to Guard your Health Privacy

WORLD **PRIVACY** FORUM

Version 2.0

Prepared by Robert Gellman for the World Privacy Forum, with assistance from Pam Dixon, executive director, World Privacy Forum. John Fanning, former privacy advocate, U.S. Department of Health and Human Services, and Dr. Lewis Lorton, health technology and privacy expert contributed to the first edition of the Guide. Robert Gellman and the World Privacy Forum take responsibility for the judgments and accuracy of information in this guide. Nothing in this guide constitutes legal advice.

Patient's Guide to HIPAA

World Privacy Forum
www.worldprivacyforum.org

Cover by John Emerson
Ebook/Digital: ISBN-13: 978-0-9914500-0-8

The World Privacy Forum is a globally recognized NGO working in privacy, identity, and emerging privacy/tech issues. We conduct respected research on the most important privacy and data protection issues of our time, and also offer consumers direct privacy support and assistance. Our work has broken new ground, provided the foundations for new consumer protection laws, and has changed privacy for the better. We rely on donations to make all of this happen, and we welcome your donation of any amount. We accept donations via credit/debit card, PayPal, Bitcoin/Ethereum, bank wire, and checks. Please visit https://www.worldprivacyforum.org/donate

How to Use This Guide

This guide is for patients. It offers a roadmap through the thicket of health privacy laws and rules that patients confront everyday. The purpose of this guide is to help patients understand how to make health privacy laws work to protect their privacy and recognize the limits of those laws.

The guide focuses mostly on the federal health privacy rule known as HIPAA. This federal privacy rule establishes a baseline of protection that applies to health care providers and health care insurers throughout the United States. The guide also discusses other federal laws that cover some health records. This guide does not offer detailed, technical explanations for every provision and every nuance of HIPAA. Instead, this guide concentrates on those parts of HIPAA that will are likely to be most helpful to real people. This guide does not review state law, and you need to know that a stronger state law can provide additional privacy protections.

If you work at a covered entity, this guide will still be useful to you, but it will not tell you everything you need to know to carry out your HIPAA responsibilities. It still offers a good introduction to the things that most patients care about.

You can read this guide cover-to-cover or you can use the index to Frequently Asked Questions (FAQs) to jump to the part of the guide that covers your particular question or problem. In some places, we include a sidebar to offer an illustration, explanation, or comment. From time to time, you will also find a "rule of thumb" offering a simple way to understand complex issues.

Quick Start

For a list of all FAQ questions, please see the complete list in the HIPAA Guide Index.

If you have general questions about HIPAA, jump to Part I, Learning about HIPAA.

If you have questions about the seven patient rights of privacy, jump to Part II, Basic Patient Rights.

If you have questions about signing consent forms and other forms at your doctor's office or at a hospital, jump to Part III, What You Should Know About Uses and Disclosures.

Navigation tips

You can navigate through the HIPAA Guide several ways.

- Use the HIPAA Guide Index as your starting page. This page lists all of the frequently asked questions about HIPAA that the Guide covers. To get to the information, click on any question you see in the index.

- At the top of each FAQ, you will find a link to the Index of FAQs so you can jump quickly through the guide.

Document History

The *Patients Guide to HIPAA* was originally published March, 2009. Since then, it has received two major updates.

Changes in the revised 2019 edition

This guide is up to date with the HIPAA health privacy rule as of January 1, 2019. Changes include minor updates and edits throughout; updating of Internet links, with additional links to HHS guidance; coverage of immunization registries; discussion of blocking robocalls; consideration of privacy and adult children covered under parental health insurance; and a discussion of the 21st Century Cures Act relating to mental health treatment of adults and communication with their caregivers.

Changes in the revised 2013 edition

This guide reflects the HIPAA health privacy rule in effect as of September 23, 2013. It includes the changes that the Department of Health and Human Services adopted early in 2013 and that took effect on September 23, 2013. These changes cover amendments made by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) and by the Genetic Information Nondiscrimination Act of 2008 (GINA). Notice the big gap between the dates of these laws and the effective date of the implementing regulation. It takes a long time to convert new laws into working rules. In December we updated FAQ 52, Pay Out of Pocket.

Index to Frequently Asked Questions (FAQs)

Introduction and Purpose

The purpose of this guide is to help you understand how to make health privacy laws work to protect your privacy and to recognize the limits of the law. We don't offer detailed technical explanations for every provision and every nuance. Instead, this guide concentrates on those parts of health privacy laws and rules that will be most helpful to real people. Even so, this guide is not short. We encourage you to use the summary and list of questions to find what you want. If you view this guide on the WPF web site, you can also use the menu to navigate to different parts of the guide.

The most important acronym we use here is HIPAA, which stands for the Health Insurance Portability and Accountability Act. HIPAA has several important parts, but the health privacy rule is the main focus here.

The federal Department of Health and Human Services issued the HIPAA rules. The health privacy rule establishes a minimum set of health privacy practices for physicians and health plans. We will remind you repeatedly that other state and federal laws that provide stronger privacy protections remain in effect. The HIPAA rule may not be the only place to look.

There are other HIPAA rules beyond the privacy rule. One covers security requirements, and is called the **HIPAA security rule**. (http://www.hhs.gov/hipaa/for-professionals/security/index.html)

One covers reporting of data breaches to the Secretary of HHS by HIPAA-covered entities, which is called the **HIPAA breach notification rule**: (http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html)

Another HIPAA rule covers enforcement procedures, the **HIPAA enforcement rule**: (http://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html)

This guide focuses on the **HIPAA privacy rule**: (https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html). Because the other rules are of less interest to individuals, we don't explain them here in detail.

In this guide, we talk about laws, rules, regulations, act, and statutes. Lawyers can find real and technical differences between these terms, but the differences don't matter much to patients. For our purposes, the terms are generally interchangeable references to legally binding policies or obligations.

In order to keep this guide streamlined, we mostly avoid lengthy explanation of minutiae, unless absolutely necessary. This means that some sections may not

describe every possible detail of a rule. One way to tell that we have streamlined a discussion is use of the word generally. That word signals that there are more details, exceptions, explanations, etc., in the text of the rule or elsewhere.

When we can, we offer a rule of thumb that cuts through the legalisms. Our rules of thumb are correct but may not be complete. They may leave out details, exceptions, and special cases not of great importance to the majority of people. We also look outside the formal rules and suggest other ways to accomplish reasonable privacy goals.

You can always read the full rule itself to find out what we left out. You can find the full HIPAA privacy rule here: (http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html). However, those who aren't used to "bureaucratese" may find the rule daunting. Everyone will find it to be long.

There's a "redline" version of the HIPAA privacy rule with the 2013 changes posted by a law firm; this is available at: (http://www.jdsupra.com/legalnews/be-prepared-redline-version-of-the-hipa-44999/). The redline shows the changes from the previous version of the rule. Another website has the current version of the privacy rule without any marking of the 2013 changes, and this may be easier for some to use. (http://www.hipaasurvivalguide.com/hipaa-regulations/164-501.php)

Feel free to look around the HHS website at (http://www.hhs.gov/ocr/privacy/).for other helpful materials. HHS has its own FAQ on HIPAA at (http://www.hhs.gov/hipaa/for-professionals/faq). Many of the questions there provide answers for those who have responsibility for implementing the law, but patients may learn something useful as well. There are also useful guidance materials at (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html).

1. What is the World Privacy Forum?

The World Privacy Forum is a nonprofit, non-partisan, 501(c)(3), public interest research group. The WPF focuses on privacy, and health privacy is one of our key areas of work. You can find out more about our work at: (https://www.worldprivacyforum.org). The World Privacy Forum provides a wide variety of consumer and policy advice as well as resources relating to privacy matters.

The WPF wrote the first report ever done on medical identity theft, a subset of identity theft, coining the term and bringing the problem to public attention. Medical identity theft occurs when someone uses an individual's name and sometimes other parts of their identity – such as insurance information – without the individual's knowledge or consent to obtain medical services or goods. Another variation of medical identity theft occurs when someone uses an individual's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous information in existing health records, often in the name of the victim. Harms to victims include wrongful medical treatment because of the incorrect information and the use of health insurance benefits by someone not entitled to them.

If you want to learn more about medical identity theft, go to (https://www.worldprivacyforum.org/category/med-id-theft/).If you think you were a victim of medical identity theft, see the *FAQ for Victims of Medical ID Theft at* (http://www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html). The answers there specifically address the needs of identity theft victims. This same page also links to consumer tips for medical ID theft and other resources.

2. Where Else Can I Find Help?

If you want the official view – as well as the text of the federal health rule known as HIPAA and related materials – go to the website of the Office of Civil Rights (you will often see this office referred to as its acronym, OCR) of the federal Department of Health and Human Services (HHS) at (http://www.hhs.gov/hipaa/index.html or http://www.hhs.gov/hipaa/for-individuals/index.html). The website offers fact sheets, FAQs (http://www.hhs.gov/hipaa/for-individuals/faq/index.html), formal summaries of the HIPAA privacy rule, and more. If you are a covered entity looking for guidance on implementing HIPAA, HHS has webpages for you as well. Start at (http://www.hhs.gov/hipaa/for-professionals/index.html).

The official materials are formal and even useful at times, but there is a lot to wade through. We seek to tell it like it is. The Office of Civil Rights tells it like it is supposed to be. Both views have relevance.

Why does responsibility for the federal health privacy rule rest with the Office of Civil Rights? The Department had to put the health privacy function somewhere, and it chose the Office of Civil Rights. The Office of Civil Rights also enforces violations of the HIPAA privacy rule. Some complained that the Office of Civil Rights was not focused on health privacy. It didn't bring enforcement actions for years after the health care world had to comply with health privacy rule. However, enforcement by OCR became much more aggressive in recent years, and you have a reasonable chance that your complaint will receive appropriate attention. In fact, there's a much greater chance that a health privacy complaint at OCR will result in an investigation than a similar privacy complaint will result in action by the Federal Trade Commission.

You can find other guides to HIPAA on the Internet. However most of them are for health care providers like hospitals and doctors trying to comply with the law. Hospitals and health plans sometimes offer patient-oriented privacy materials. Overall, we were surprised at how few free, detailed patient-oriented materials are available.

The Privacy Rights Clearinghouse (https://www.privacyrights.org) has a wealth of useful materials on privacy in general as well as some facts sheets on medical privacy (https://www.privacyrights.org/topics/health-medical). The Center on Medical Record Rights and Privacy at Georgetown University's Health Policy Institute had a good website focused on patient access rights. But it is out of date. You might find something relevant under the medical privacy tab at (http://hpi.georgetown.edu/papers.html).

The Center for Law, Ethics, and Applied Research in Health Information at Indiana University also has a variety of useful materials on health privacy at (https://medicine.iu.edu/research/centers-institutes/bioethics/research/health-information/).

Consumer Action has materials on health privacy for California patients. (http://www.consumer-action.org/english/articles/health_records_privacy_in_california). That information is also available in Spanish. (http://www.consumer-action.org/spanish/articles/health_records_privacy_in_california_sp). Consumer Action has other health privacy resources as well. (http://www.privacy-information.org/publications/P0/topics/medical).

The federal HIPAA rule may not be the only health privacy law relevant to you. The HIPAA rule establishes a "floor" of privacy protection. If state law or another federal law gives you more rights, greater access to your health records, more limits on disclosure, or lower fees for copies of your health records, then those other laws supersede HIPAA. This can be very important at times.

The National Conference of State Legislators has a site dedicated to HIPAA impacts and actions by states: (http://www.ncsl.org/research/health/hipaa-a-state-related-overview.aspx). Your state health department may also have useful information on its website. So might a state hospital association. After you have the citations, you have to look to find the laws. Knowing where to look is half the battle, however. Always, look carefully to see if the information on these websites is current. It may be hard to tell.

Be aware that state laws change, and the information on any state law website can be outdated. Pay attention to the dates of any discussion of state laws.

If the Privacy Act of 1974, a law applicable to federal agencies like Medicare and the Department of Veterans Affairs, is relevant to you, you can find a guide at (https://www.fas.org/sgp/foia/citizen.html). Federal agencies subject to HIPAA and the Privacy Act of 1974 must give you the best of both laws.

3. What Federal Laws Are Relevant to Health Privacy?

HIPAA is the most important federal health privacy law for almost everybody in the United States. Most of this guide explains what you should know about HIPAA.

We also highlight some other federal laws that may be relevant to your health privacy. There are five federal laws beyond HIPAA we think you should know about. Each of these touches on privacy in a slightly different way.

They are:

- Privacy Act of 1974
- Confidentiality of Alcohol and Drug Abuse Patient Records Regulations
- Family Educational Rights and Privacy Act (FERPA)
- Americans with Disabilities Act (ADA)
- Genetic Information Nondiscrimination Act (GINA)

We discuss each of these other laws briefly below.

Privacy Act of 1974

An important general purpose federal privacy law is the Privacy Act of 1974 (http://www.law.cornell.edu/uscode/text/5/552a). The Privacy Act of 1974 covers nearly all personal records (not just health records) maintained by federal agencies and some federal contractors. It applies to military health records, veterans' records, Indian Health Service records, Medicare records, and health records of other federal agencies. HIPAA also applies to most of those same federal records. So if a federal agency has health information about you, you are entitled to the best protections in both laws. HIPAA is sometimes better, but rights under the Privacy Act of 1974 are often better than HIPAA.

You can learn more about the Privacy Act of 1974 from a detailed guide published by the Department of Justice (http://www.justice.gov/opcl/1974privacyact-overview.htm). Warning: The Privacy Act of 1974 is just as complicated as HIPAA, and maybe even more so because there have been decades of litigation under the Privacy Act of 1974 (and very little under HIPAA). Remember that the Privacy Act of 1974 does not apply to most hospitals, clinics, or physicians. The Privacy Act of 1974 does not apply to them even though they may receive federal funds or are tax-exempt. Remember, the Act applies to federal agencies, not federal funds recipients.

The National Institutes of Health – part of the Department of Health and Human Services – may be one of the few major health care institutions in the United States not covered by HIPAA. However, the Privacy Act of 1974 still applies to the NIH. More at (https://oma.od.nih.gov/forms/Privacy Documents/Documents/NIH Privacy FAQs March 2013.pdf).

Confidentiality of Alcohol and Drug Abuse Patient Records Regulations

The Confidentiality of Alcohol and Drug Abuse Patient Records Regulations (42 Code of Federal Regulations Part 2) are an important set of federal rules for some health records. These rules provide privacy protections for records of federally funded substance abuse (alcohol and drug abuse) health care providers. You can find more information at (https://www.samhsa.gov/laws-regulations-guidelines/medical-records-privacy-confidentiality). The actual rules are also at (https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=b7e8d29be4a2b815c404988e29c06a3e&rgn=div5&view=text&node=42:1.0.1.1.2&idno=42). HHS updated the Part 2 rules in 2017. See https://www.federalregister.gov/documents/2017/01/18/2017-00719/confidentiality-of-substance-use-disorder-patient-records.

RULE OF THUMB

The alcohol and drug abuse rules contain the strictest privacy protections of just about any law. The rules allow many fewer disclosures than HIPAA, and the restrictions generally follow the records. That means that if a record is subject to the rules, the record remains subject to the rules if the record is disclosed to anyone. That is an unusual but very privacy protective policy.

The Substance Abuse and Mental Health Services Administration (SAMHSA) administers the alcohol and drug abuse rules. SAMHSA is part of the Department of Health and Human Services. You can find a document that discusses how HIPAA and the substance abuse privacy rule relate at (http://www.samhsa.gov/sites/default/files/part2-hipaa-comparison2004.pdf).

Family Educational Rights and Privacy Act (FERPA)

Health records at most schools and colleges (at least those receiving federal funds) are not covered by HIPAA but by the Family Educational Rights and Privacy Act (FERPA). You will find more information about FERPA and a link later in this guide. (See FAQ 9.) In general, FERPA's protections are better than HIPAA in some ways and not as good in others. There's a simple Q&A on FERPA and HIPAA at (https://www.hhs.gov/hipaa/for-professionals/faq/ferpa-and-hipaa/index.html), and a more detailed guide at (http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf) and at (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf). Be warned that the interplay between HIPAA and FERPA is very complex.

Americans with Disabilities Act (ADA)

The Americans with Disabilities Act (ADA) provides employees with disabilities some protections against discrimination in the workplace. The law includes limited workplace privacy protections as well. You can learn more about the ADA at the Equal Employment Opportunity Commission's website. (http://www.eeoc.gov/laws/types/disability.cfm).

Genetic Information Nondiscrimination Act (GINA)

The Genetic Information Nondiscrimination Act provides some federal protection from genetic discrimination in health insurance and employment. Genetic discrimination occurs when people are treated differently by their employer or insurance company because they have a genetic change that causes or increases the risk of an inherited disorder. GINA is a federal law designed to protect people in the United States from this form of discrimination. Most states have similar laws.

Title I of GINA makes it illegal for health insurance providers to use or require genetic information to make decisions about a person's health insurance eligibility or coverage. This part of the law went into effect on May 21, 2009. Title II makes it illegal for employers to use a person's genetic information when making decisions about hiring, promotion, and several other terms of employment. This part of the law went into effect on November 21, 2009.

For more on GINA, see: (https://ghr.nlm.nih.gov/primer/testing/discrimination). GINA has been controversial in some respects. Some think that the protections of GINA are not all that useful. We discuss the privacy provisions of GINA briefly in FAQ 56.

Some other federal privacy laws may apply at times to health records held by some records keepers (e.g., banks and credit bureaus). We don't think that these laws are relevant enough to most people to explain here. There are other general privacy resources at the World Privacy Forum website (https://www.worldprivacyforum.org) and at the website of the Privacy Rights Clearinghouse (https://www.privacyrights.org) .

Part I: Learning About HIPAA

4. What is HIPAA and Why Should You Care?

You can't get very far into health privacy without running across the acronym HIPAA. HIPAA stands for the Health Insurance Portability and Accountability Act, a 1996 US federal statute. Although many people associate HIPAA just with health privacy, the Act actually covers many topics unrelated to privacy. The part of the Act relevant to privacy directed the Department of Health and Human Services to write a health privacy rule. The rule originally took effect on April 14, 2003. Some refer to it as the health privacy rule, the HIPAA rule, or just plain HIPAA.

Other HIPAA rules also exist, but they don't relate to health privacy. When we say HIPAA in this document, it means the HIPAA health privacy rule unless we state otherwise. There is a HIPAA security rule for health records, a breach notification rule, and an enforcement rule. These rules all relate to health privacy in some way. Other HIPAA rules also exist, but most address topics unrelated to health privacy.

HIPPA or HIPAA?

People often incorrectly abbreviate HIPAA as HIPPA (two Ps rather than two As). If you do an Internet search for *hippa*, you may be surprised at how often the wrong acronym is used.

The HIPAA security rule requires the health care world to comply with security standards for health information. HHS issued security standards under the authority granted by the HIPAA statute. Responsibility for the security rule had been assigned to the Centers for Medicare & Medicaid Services (CMS), but it now belongs to the Office of Civil Rights at HHS. You can find more information on the security rule at (http://www.hhs.gov/hipaa/for-professionals/security/index.html). We won't cover the security rule in detail here because it is of interest primarily to health care providers and insurers who have to implement it.

Health Care Data Breaches

We receive many questions about the rules covering health care data breaches. The HIPAA breach notification rule tells those covered by the HIPAA privacy and security rules how to handle and respond to data breaches. (http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html). HHS posts data breaches involving over 500 records on its website at: (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf). The World Privacy Forum has a data visualization tool that visually shows a history of the data breaches listed on HHS at www.worldprivacyforum.org, click the Maps, Apps, and Data Visualizations category tag or search for "data breach" on the WPF site. FAQ 65 discusses breach notification.

5. Who is a Patient?

Interestingly, HIPAA does not use the term *patient*. Not everyone who is the subject of a health record is a patient. For example, you may be the beneficiary of a health insurance policy. The insurer has information about you, but you are not the insurer's patient. Even if that information is only your name, address, and plan number, it is *protected health information* (PHI), and that is covered by HIPAA.

The HIPAA rule uses the term *individual* to cover patients, beneficiaries, and others protected by the rule, but we find the term a bit jarring. We use the more familiar term *patient* here because just about everyone is a patient eventually. HIPAA's *individual* and our *patient* are identical. (For more about what we mean by the term *protected health information*, see FAQ 8.)

Health Files and Your Information

The individual who is the subject of a health file is the patient. Information about one individual may appear in someone else's file. For example, information about your health condition may be part of your sibling's family history. Generally, you only have rights under HIPAA with respect to information in your health file held by a covered entity.

What is PHI?

When use the term PHI -- all caps -- we mean the HIPAA-related abbreviation that means "protected health information." PHI is any information that a health care provider (or any other entity covered under HIPAA) holds about a patient. PHI covers everything from demographic information like your name, to financial information, and of course, health information.

6. Do Children Have Privacy Rights?

Yes, but it is complicated. The basic answer is that if a child has a right to make a health care decision about himself or herself, then the child has the right to control information associated with that decision. Otherwise, a parent or guardian or person acting in loco parentis can exercise privacy rights on behalf of a child.

To state the rule more specifically, a child can exclusively exercise his or her own privacy rights with respect to a health care service if:

1) The child is emancipated;
2) the child consents to the health care service and no other consent is needed;
3) the child may lawfully obtain the service without a parent's consent; or
4) the parent or guardian consented to an agreement of confidentiality between the child and the health care provider.

Legal technicalities can make a big difference here.

In addition, a special rule addresses cases where a covered entity has a reasonable belief that the child is a victim of domestic violence, abuse, or neglect. (A covered entity here is generally a hospital or other health care provider, or possibly a health plan that is required to comply with HIPAA. For more on what is a "covered entity," see FAQ 9.) The covered entity may decide that it is not in the best interest of the abused child to allow the parent to act on behalf of the child.

It gets even more complicated for minors because the HIPAA rule recognizes that States may have other policies governing privacy, health, and children. When state law specifically addresses disclosure of health information about a minor to a parent or guardian, that law preempts (supersedes) HIPAA whether it prohibits, mandates, or allows discretion about a disclosure.

RULE OF THUMB

Normally, HIPAA defers to a state law that is stronger than HIPAA. However, for minors, HIPAA defers to all state law, whether the law is stronger or weaker.

When does a child become an adult? That depends entirely on state law.

7. Do Privacy Rights Survive Death?

Not in the way that they did before. Until the rule changed in 2013, a patient's privacy rights survived death and lasted forever. The 2013 change means that privacy protections remain in place for fifty years after the date of death. However, if a State has a law that provides for additional privacy protection, that law remains in force. Further, the professional responsibilities of health care providers may require that patient records receive longer protection.

After a patient dies, that patient's legally authorized executor or administrator, or a person otherwise legally authorized to act on the behalf of the deceased patient or patient's estate, can exercise the deceased patient's privacy rights.

It is important to know that disclosures for treatment do not require consent or authorization of the patient or the patient's representative. (For more on authorizations, see FAQs 64-66). That means, for example, if information about the deceased patient is relevant to the care of the surviving spouse, the information can be disclosed by a health care provider to the health care provider for the surviving spouse.

Privacy for the dead can be especially messy when questions arise in the period after death and before anyone is formally authorized to act for the patient or the patient's estate. For many individuals, there may be no formal legal process following death. Another 2013 change helps here. It clarifies that a covered entity may disclose a decedent's information to family members and others involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. This gives health care providers and health plans the discretion to do what they consider to be the right thing for families of recently deceased patients.

8. What's a Health Record?

HIPAA introduces the term *protected health information* or PHI. The actual definition is a conglomeration of nested and complex terms with even longer exceptions. It is too messy to bother with here. Instead, we offer a rule of thumb that works just fine most of the time.

[RULE OF THUMB]

Any information that a covered entity (e.g., health care provider or insurer) has about you is PHI. It doesn't matter if the information is medical, financial, or otherwise. We tend to use the more traditional term – health record here, but we mean PHI.

HIPAA Myth

A common myth about the HIPAA privacy rule is that it only covers electronic information. That is false. The health privacy rule applies to PHI in any form or medium. If a covered entity records your information on paper, computer disk, or tree bark, it is subject to HIPAA. However, the HIPAA security rule only applies to electronic Protected Health Information. For more on covered entities, see FAQ 9.

A 2009 change in the statute made it clear that genetic information is PHI. That really didn't change anything because genetic information is no different than any other information in a health record. Genetic information was already PHI.

9. Which Health Care Entities Must Comply With HIPAA?

HIPAA doesn't apply to every health record keeper or to every health record. Only covered entities must comply with HIPAA. Get used to the term *covered entity* because it comes up a lot. HIPAA recognizes and regulates three types of covered entities.

This is a complicated area, and this is one of the longest FAQs in this guide. There are lots of types of entities, some covered by HIPAA, some partly covered, and some not at all.

HIPAA generally covers health information maintained by or for a covered entity. HIPAA generally does NOT cover health information held by those who are not covered entities. This is an especially important point that many people in the health care world do not understand clearly. Health information that is protected when held by a covered entity (like a health record held by a hospital) may have no privacy protections when the information is held by a someone who is not a covered entity. In other words, health privacy protections depend on who has the information and not on the nature of the information.

The covered entity concept is complicated. We explain related terms – business associates and hybrid entities – later in this FAQ.

Covered entities under HIPAA are:

1) Health care clearinghouses

Health care clearinghouses transmit information (typically claims and billing information) between other players in the health care system. For example, a hospital may send the bill for your treatment to a health care clearinghouse that reformats and submits the information to your insurance company. Clearinghouses are of no interest to the average patient because their function is usually invisible. Patients rarely, if ever, come into contact with them. But clearinghouses have the same obligations as other covered entities, and that is important if you ever have an issue with a clearinghouse. Otherwise, don't worry about clearinghouses. We won't mention them again in this guide.

2) Health plans

Health plans are covered entities. Health insurers, health maintenance organizations (HMOs), and Medicare are examples of health plans subject to HIPAA. So are plans covering uniformed service members. Nearly all health plans are covered entities, but some small group health plans (fewer than 50 participants) may not be covered entities. We use health plan and insurer interchangeably here.

3) Health care providers

Health care providers are covered entities, at least most are. Generally, a health care provider is a doctor, hospital, dentist, podiatrist, pharmacist, laboratory,

optometrist, and just about anyone else licensed to provide health care. The formal legal definition of health care provider is so complex that it makes lawyers wince.

It is important to understand that HIPAA does not automatically cover all health care providers. It generally depends on whether a provider bills (directly or indirectly) for services electronically. The reason for this odd, even silly, standard has to do with the structure of the health care system and the Department of Health and Human Service's authority to regulate. Unless you are a policy wonk, you probably don't want to know more.

RULE OF THUMB

What organizations are covered under HIPAA?

A simple rule of thumb is that any health care provider who bills an insurance company or health plan is a covered entity under HIPAA. If your doctor accepts Medicare, for example, the doctor is a covered entity. A free health clinic may not be subject to HIPAA because it doesn't bill anyone. A doctor who charges every patient $25 cash and does not submit a bill to any insurance company may not be covered by HIPAA. A first aid room at your workplace may or may not be covered by HIPAA.

If you want to know if the organization you are dealing with is a HIPAA-covered entity, ask. If you don't get a straight answer, ask for a copy of its privacy policy. If it has a privacy policy, the policy will explain about HIPAA's application. If it doesn't have a written privacy policy, then it is either not covered by HIPAA or it is violating the rule.

Hybrid Entities (Supermarket pharmacies, etc.)

Do you use a pharmacy at a supermarket? If so, the pharmacy's records are subject to HIPAA because the pharmacy is a health care provider that submits electronic bills. What about the records that the supermarket maintains as part of a frequent shopper program? The answer is the supermarket's other customer records are almost certainly not protected by HIPAA. An organization with both health care functions and other functions can define itself as something called a hybrid entity. HIPAA will then apply only to the part of the organization that does health care and not to the rest. This should all be explained in the covered entity's notice of privacy practices.

School health records

Most school health records are not subject to HIPAA. Instead, school records (private schools are a major exception) are usually covered by another federal privacy law, the Family Educational Rights and Privacy Act (FERPA). The federal Department of Education oversees FERPA. A school nurse is likely to be subject only to FERPA. A university hospital that runs a student clinic on behalf of the university is also subject to FERPA. However, other university hospital records about students could also be subject to HIPAA, depending on the circumstances. The relationship between HIPAA and FERPA is very complicated. For more, see (http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf). Which law is better for privacy? The short answer is that privacy rights under FERPA can be better in some ways than under HIPAA and worse in other ways.

Many states maintain immunization data systems ("Immunization Information Systems") for school children and other individuals. The privacy of records in these registries is subject to standards set of the Centers for Disease Control. (http://www.cdc.gov/vaccines/programs/iis/func-stds.html). The immunization records in these systems may or may not be subject to HIPAA.

Business associates and subcontractors

If a covered entity hires another organization to perform a function that requires access to health information, that other company may be a business associate of the covered entity. This happens routinely, for example, when a hospital hires an accounting firm to audit its records. Many covered entities have dozens of business associates. Business associates of a covered entity are now directly covered by HIPAA. That means that a business associate of a covered entity can be penalized for

violations in the same way as a covered entity. This is a good thing, as the possibility of penalties may result in better compliance with the law.

A covered entity must have a contract with each business associate. The contract must require the business associate to comply with all relevant HIPAA provisions. The basic idea is that a covered entity cannot avoid the privacy rule by hiring someone else to process health records.

If a business associate hires another entity to help process PHI, then that entity (called a "subcontractor") is also subject to HIPAA. If a subcontractor hires another subcontractor, all are covered by HIPAA. Covered entities, business associates, and subcontractors must all process your health records according to HIPAA rules. There's a lot of complexity here, but it is not the patient's problem.

Other health record holders

Who else has health records but isn't subject to HIPAA? Many organizations have health information about you, but neither the organizations nor the records are subject to HIPAA. The list of unregulated health record keepers is shockingly long. These include gyms, medical and fitness apps and devices not offered by covered entities, health websites not offered by covered entities, Internet search engines, life and casualty insurers, Medical Information Bureau, employers (but this one is complicated), worker's compensation insurers, banks, credit bureaus, credit card companies, many health researchers, National Institutes of Health, cosmetic medicine services, transit companies, hunting and fishing license agencies, occupational health clinics, fitness clubs, home testing laboratories, massage therapists, nutritional counselors, alternative medicine practitioners, disease advocacy groups, marketers of non-prescription health products and foods, some workplace wellness programs, and some urgent care facilities. Commercial providers of Personal Health Records have health records but are not covered entities. However, PHRs maintained by or on behalf of your health care provider or insurer are covered by HIPAA.

Employers may offer wellness programs. Some wellness programs do collect health information. For more about HIPAA and workplace wellness programs, see HHS guidance at (https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html?language=es).

Wait ... who outside of my health care provider has my health information?

Did you wonder why a hunting and fishing license agency made this list of organizations with health records? Some states give discounted licenses to those who are disabled. How do you prove entitlement to a discount? You must provide adequate health information to the agency. This is just one example how your health information can end up in the hands of many different types of organizations that have no direct health care or payment responsibilities. This is also why protecting the privacy of health information is so difficult. The information turns up in places that you might not expect.

Have you ever filled out a survey asking if you or a household member has a particular medical condition? Unless you gave the survey directly to your doctor, odds are that a marketing company asked for the information. Marketers are not subject to HIPAA, and they can use and sell your information without any restriction as often as they want. For example, if you tell a marketer when you are 21 that you have allergies, that marketer can use or share the information to sell you products for the rest of your life.

Is your Personal Health Record protected?

If an organization or a business maintains a Personal Health Record (PHR) for you, that PHR may not always fall under HIPAA's protections. Be cautious with PHRs because they are the subject of much attention and promotion. Many companies are trying to get in the business of storing your health records for you, especially online. But you need to know that unless a health care provider or insurer (or someone doing it on behalf of a provider or insurer) maintains the PHR, HIPAA does not apply. It's always worth checking to be sure. Read the privacy policy to know.

Here's the most important point: if you give a commercial, advertising-supported PHR service consent to store your records, the records are probably not protected by HIPAA. The PHR service may be able to exploit the records as it pleases, subject only to its own privacy policy and terms of service. If you read the PHR company's policy carefully, we bet that it says that the company can change the policy at any time.

We would not give our health records to a PHR service not covered under HIPAA. We're skeptical because some companies and websites are not forthright in describing how they use or disclose health information, even when they have a privacy policy. Even if they promise not to disclose your information for marketing, they may still use it for marketing. If the PHR service is ad-supported and if you click on an ad, a considerable amount of your PHI may be disclosed to the advertiser by

your click alone. The advertiser may have a privacy policy that differs from the PHR service provider, or the advertiser may have no privacy policy at att.

Further, it is easy for companies to change their privacy policies at a moment's notice. This means that you can lose control of your sensitive health information if the company changes its business model, merges with another company, or goes bankrupt. For more on PHRs, see the World Privacy Forum report *Personal Health Records: Why Many PHRs Threaten Privacy* at (https://www.worldprivacyforum.org/2008/02/blog-legal-and-policy-analysis-personal-health-records-why-many-phrs-threaten-privacy/).

A health record covered by HIPAA can lose its privacy protection if transferred to a third person who is not a HIPAA-covered entity. This is a very important aspect of HIPAA. Some would call it a loophole. The original record in the hands of the covered entity remains subject to HIPAA, but the copy sent to a non-HIPAA-covered entity falls outside the scope of the HIPAA privacy rule.

We offer five examples of health information transfers that you may see it in daily life. However, each of our examples has a weasel word ("probably") because the rule is complicated. If we stopped to explain this kind of thing further, this document would quadruple in size.

- You tell your doctor to give part of your health records to your employer to explain your absence from work. The record will probably not be subject to HIPAA in the hands of your employer. But your health information may have some protections under other laws covering your employer.

- You download your health record from your health care provider to your mobile phone. When your record is at the provider, it is covered under HIPAA. But on your phone, the record is not covered.

- A health researcher obtains your health records for use in a properly authorized research project. The records probably have no HIPAA protection in the hands of the researcher. However, if the researcher is treating you as part of the research (as in a clinical trial), then HIPAA is more likely to apply.

- You apply for life insurance, and the insurance company obtains your health records with your consent. The records are not subject to HIPAA in the hands of the insurance company. The records may be subject to a state insurance privacy law. Some of the information you authorize the insurer to have may also end up at the Medical Information Bureau (MIB), another organization not subject to HIPAA. If you read the fine print in your application/authorization, you will learn that signing the form authorizes disclosure to MIB as well. MIB is subject to the Fair Credit Reporting Act, a different privacy law that provides you with some rights and some

protections. (To assert your Fair Credit Reporting Act rights, you would, for example, request a copy of your consumer file from MIB. See (http://www.mib.com).

- Your doctor tells you that you have a communicable disease (e.g., tuberculosis). The doctor must report your illness to the state public health department. The part of the health department that receives your record is probably not subject to HIPAA.

We could list additional examples, but we offer a rule of thumb instead.

[RULE OF THUMB]

If a covered entity discloses a health record to anyone who isn't a covered entity, the record is generally outside the scope of HIPAA in the hands of the recipient. This is a major way that health records escape from privacy protections. This is true online and offline.

If you share health information with your family, a neighbor, or co-worker, the information that you share is not protected under HIPAA in the hands of the recipient. If you share your health information with a website that isn't a covered entity under HIPAA, then the information you disclose is not protected under HIPAA in the hands of the website. This is a complex area that has created a lot of confusion among some consumers. Web sites that are medical web sites may very well not be covered under HIPAA, even if they say they are "HIPAA compliant." See Rule of Thumb, HIPAA Compliant, or HIPAA Covered?

[RULE OF THUMB]

HIPAA Compliant, or HIPAA Covered?

If a company is not covered by HIPAA, it may still say that it is "HIPAA compliant." HIPAA compliant does not mean the same thing as being a HIPAA-covered entity. If you see the words HIPAA compliant, find out if the company is a HIPAA-covered entity. This is a yes or no question; there is no "maybe" answer here. If a company is HIPAA compliant but not a HIPAA-covered entity, we urge caution. The use of the term HIPAA compliant can be deceptive in that circumstance. HHS has a bit of guidance on misleading marketing claims at :(https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/be-aware-misleading-marketing-claims/index.html?language=es).

10. What are Fair Information Practices and How Do They Relate to HIPAA?

If you read the HIPAA privacy rule – and stayed awake while doing it – the rule would appear to be a welter of detailed and uncoordinated provisions. It actually has a structure, but that structure is difficult to appreciate unless you know about Fair Information Practices or unless you read the original preamble to the rule from 2000.

The rule implements Fair Information Practices (FIPs), an established set of principles for addressing concerns about information privacy. FIPs are especially significant because they form the basis of many privacy laws in the United States and, to a much greater extent, around the world. Understanding FIPs makes it easier to make sense of the HIPAA privacy rules.

The eight FIPs generally recognized are:

1. Openness
2. Use Limitation
3. Purpose Specification
4. Collection Limitation
5. Data Quality
6. Security
7. Access and Correction
8. Accountability.

We could discuss FIPs here in more detail, but it would be a distraction. Different versions of FIPs exist, and the actual application of FIPs to any set of personal records can be complex, variable, and controversial. We just want you to know that there are basic principles of information privacy that HIPAA mostly implements. You can read a short introduction to FIPS here: (https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/). Understanding FIPs is not essential to understanding HIPAA, but it may help some people. But if you are interested, you can find a longer history of FIPs at (http://bobgellman.com/rg-docs/rg-FIPshistory.pdf).

Fair Information Practices are important for privacy of records other than health. Whenever you consider whether any record keeper properly protects the privacy of your personal information, you can use FIPs as a checklist for assessing privacy practices.

If you see a privacy policy for an Internet site, a bank, or a government agency, try to determine if the policy addresses all eight FIPs. If it doesn't, then you already know that the policy isn't as good as it could be or should be. When a policy addresses FIPs, see how good a job the policy does in protecting your privacy.

For example, a good policy may say that personal information is only disclosed when required by law or for necessary business purposes. A mediocre policy may allow for disclosure to affiliates for marketing or when disclosure is allowed by law. "Allowed" can be a major weasel word in a privacy policy. A weak policy may not address disclosure at all.

11. Does HIPAA Protect Privacy?

This is a tough question to answer. Health care providers generally care about patient privacy, but health care providers have only some control over the records of their patients. Our complicated health care treatment and payment system places patient health information in the hands of many different providers, insurers, agencies, and others. Before HIPAA, we believe that the health care system mostly paid lip service to privacy. How many hospitals offered you a notice or privacy practices before HIPAA? How many trained their staff in privacy? How many told you that you had a right to see and copy your own records? Before HIPAA, active privacy policies were a rarity in health care. By this measure, HIPAA made some definite improvements.

Our health care system – with third-party payors and lots of government involvement (e.g., Medicare and public health) – places many demands on health

records. Everyone wants low-cost, high-quality health care for all. Achieving these objectives often affects privacy in negative ways. The trade-offs can be sharp. HIPAA is decidedly a mixed bag for privacy. It does some good things and some not-so-good things. It protects privacy rights in some ways and undermines those rights in other ways at the same time.

HIPAA gives each patient some rights. There are seven formal rights, not all of which are new everywhere. (See the heading Basic Patient Rights to learn more about the seven rights HIPAA gives patients). However, some of the new rights are not especially meaningful. HIPAA also permits many uses and disclosures of health records without the patient's consent. Many will find some of these uses and disclosures objectionable. A patient doesn't have the opportunity to control most uses or disclosures of his or her records.

If you just look at the disclosure provisions, then you might conclude that HIPAA allows many disclosures that you may not think are appropriate. For good or bad, many of those disclosures were routine before HIPAA. However, if you consider the overall state of privacy protections before HIPAA, you might see a marked improvement in many aspects of privacy today.

So does HIPAA protect privacy? Everyone is entitled to his or her own answer to this question. We prefer to say that HIPAA offers patients Fair Information Practices. (See FAQ 10.) Whether the implementation of Fair Information Practices in HIPAA meets your own privacy standards is for you to say. Everyone has different privacy needs, preferences, and desires.

12. How to Solve Problems Presented by HIPAA

In this guide, we point out some shortcomings with the HIPAA rule. The rule doesn't require covered entities to do everything that you might want. It may not protect privacy sufficiently or define your rights as expansively as you think it should.

In many instances, deficiencies in the rule can be addressed when covered entities (See FAQ 9) and patients work together in good faith to address problems that arise. The rule generally doesn't prevent covered entities from treating patients better than the rule requires.

We suggest that when the rule doesn't give you a formal right that you think is reasonable, ask the covered entity to consider doing what you need anyway. The rule gives a covered entity discretion to take actions that can benefit patients and their privacy. If you ask politely and persistently for help, you may get it. If one person won't bend the rules or procedures, then ask another person a supervisor, or to the Privacy Officer at the covered entity. Try to work cooperatively with the covered entity.

This is a real story. A patient parks his car in a parking lot adjacent to a doctor's office. Another individual leaves the doctor's office, gets in her car, and backs into the car of the patient who just arrived. The damage is minor. The driver is not aware of the accident and drives away. The arriving patient goes into the doctor's office to ask for the name and address of the patient who just left. Under the HIPAA rule, the office could not disclose the name of the patient driving the other car. None of the disclosure exceptions applies.

However, this doctor's office does the right thing, something not required by HIPAA. The office calls the driver and asks her to speak to the owner of the car that she hit. The driver agrees, and the problem is solved. The office facilitated the exchange of information between the two patients, but it disclosed no information in violation of HIPAA. The two individuals disclosed information to each other. The creative and cooperative action by everyone avoided much more complicated and expensive responses to the problem (e.g., calling the police to report a hit-and-run accident). Not everything needs to be a federal case.

Part II: Basic Patient Rights

This section covers the rights that HIPAA grants to patients. The rule defines seven patient rights, but not all of those rights are meaningful. We discuss the rights in the order of importance as we view the rights. Your mileage may vary.

A. Right to a Notice of Privacy Practices

13. What is a HIPAA Notice of Privacy Practices?

The rule requires each covered entity, like a hospital, to publish a notice of privacy practices. You may see this abbreviated as NPP in some cases. The notice describes how each entity implements the rule. Notices from different health care institutions may look similar because the rule is the same for everyone. However, each notice should have some details (procedures, addresses, etc.) that are specific to the institution. If you want to learn more about health privacy, a notice of privacy practices is a good place to start. So is this FAQ!

14. Why Are the Notices Long and Boring?

One answer is that the rule is long and complicated. Another answer is that lawyers write many of the notices. Often, lawyers write like…lawyers, and the results are sometimes complete, precise, and incomprehensible. Some privacy notices – and not just notices for health – are deliberately written to be obscure. Even other lawyers can't understand them. Not every organization really wants you to understand or exercise your privacy rights.

In the end, health privacy is a complex subject. Health records have quite a few uses and disclosures that you probably never thought about. All of these factors contribute to the length and complexity of the notices. Still, the notice is your friend and your guide if you want to pursue your rights.

15. Should I Read the Notice?

Only if you want to. Every expert says that people should know their rights and understand privacy. We agree, but we recognize that people often don't have the time or interest needed for privacy management. Don't feel guilty if you just don't want to read the notice from your doctor, hospital, laboratory, or pharmacy today. What's important is that the notice exists and that the record keeper who produced the notice has a privacy policy and – we hope – actually implements the policy appropriately.

The HIPAA requirement that each covered entity prepare a notice was a big advance in privacy protection. That remains true even if most patients never read the notice. The notice also tells a covered entity's employees what the privacy rules are. That is just as important as telling patients what the rules are. In the past, employees often didn't know whether there were privacy rules or what those rules stated.

To put it another way, you have privacy rights whether or not you know the details. Your rights do not depend on your level of understanding. You can do a better job of protecting your rights if you know more, of course.

Here's what's really important:

- Read the notice when it matters to you. If you decide that you want a copy of your health records, that's a time to read the notice and find out how to obtain the records.

- If you think that there is an error in your record, read the notice and learn how to ask for a correction.

- If you think that your records were improperly used or disclosed, read the notice to see if you are right.

- If you have a privacy complaint, you can read about the complaint procedure that the rule provides.

When it makes a difference to you, get a copy of the notice and read it. That could be today or two years from now. You can always ask for a copy, even if you are no longer someone's patient. If a provider or insurer maintains a website, it should post a copy of its privacy policy on the website. That may make it easier for you to find the notices that you need.

16. What Are the Forms that My Doctor's Office Asks Me to Sign?

The rule generally requires a health care provider to make a good faith effort to obtain an acknowledgement that each patient received the notice. Some people think that it is a dumb requirement and a paperwork burden, but that's what the rule says. Signing a standard acknowledgement does not waive your rights.

You do not have to sign the acknowledgement. Your rights do not change if you sign or don't sign. However, the requirement for a signature is poorly understood. Some receptionists think that a signature is mandatory, and they will hassle you if you don't sign. Some will tell you that you must sign or you can't see the doctor. That is wrong.

You can fight about signing the acknowledgement if you want. We suggest, however, that this isn't a fight worth having. Save your energy for another battle. The acknowledgement – if that's all that the form contains – is meaningless. If you see something on the form that you don't like, you can just cross it out. Odds are that no one will even notice what you did.

We hear that some doctors are asking patients to sign broader forms that limit the ability of patients to file malpractice suits, that prevent patients from talking about the doctor to other people or on the Internet, or do accomplish other things that benefit the doctor and not the patient. We suggest being careful if offered these types of documents. We wouldn't sign one.

In the pre-HIPAA days, most patients were given actual consent forms to sign when they came to see the doctor. The forms often gave your health care provider permission to disclose your records to just about anyone. It was the

privacy equivalent of a blank check. Most people signed the forms without reading or understanding them.

HIPAA eliminated consent forms, something that some people find objectionable. However, the old consent forms mostly waived any rights that you had and did more to protect your provider than to protect you. HIPAA eliminated the need for routine consent forms, but at a price. The discussion later about uses and disclosures will make that price clearer. (See FAQs 55-67.)

What you really need to know:

When you visit your doctor's office for the first time, someone should offer you a copy of the doctor's notice. You may be offered the same notice on each visit because many offices find it easier to give every patient a notice on every visit rather than keeping track of first visits.

Sometimes, the notice will be sitting on a counter or table. You have the right to take a copy home. Remember that you can always ask for a copy later or find it on the website of your doctor or insurer. If you don't care about it today, it should be available to you later, even if you are no longer a patient of that doctor or covered by that insurer.

Your health plan also will provide you a notice, but the rules for getting you the notice are somewhat different for health plans. Patients really don't need to know those rules. You probably received a health plan notice in the mail, but you may have ignored it. If you want a notice from your health plan, ask for it or look on the health plan's website.

17. What Are the Most Important Parts of the Notice?

Almost any health privacy notice will tell you something that you probably didn't know. For example, a notice is supposed to include examples of the uses and disclosures that a covered entity can make. These examples will likely be both enlightening and disturbing.

Notices from most HIPAA-covered entities are quite similar because you have the same rights everywhere the rule applies. If you read one notice, you've generally read them all. However, there may be some variations here and there between

notices from health care providers and notices from insurers. Differences in state law may result in different notices from covered entities in different states.

When you want to exercise your rights at a particular covered entity, the local procedures described in the notice are likely to be different in each notice. That's the time when reading the notice may matter a lot. Each notice should describe the covered entity's procedures for exercising patient rights. Make sure you follow any specified procedures. Otherwise, here are some notable features to look for.

What institutions are covered by the notice?

If the notice is for a hospital or other large institution, read the description of which institutions and providers are covered. We have a notice for a hospital that says that more than a dozen different institutions in three states are part of the same institution. That means that patient information can be readily shared among all the affiliated organizations without your consent. That ability to share records widely may not be unusual or should not always be troubling. Further, being able to obtain care at related institutions may be a good thing.

Consider, however, if your cousin works in a health care facility in a nearby state. You may not realize that facility is connected to the health care provider that you see regularly. You might not be happy knowing that your cousin may have access to your record. It may or may not be lawful for your cousin to do so, but the possibility may be unnerving.

What are the directions for requesting amendments, copies of your health records, accounting of disclosures, and restrictions of disclosures?

HIPAA contains seven rights for patients, and the notice of privacy practices is a good place to find out how you can utilize these rights. A notice should have clear instructions for you, as well as contact information, about how you can make requests and follow up on them. (For details about the basic rights of HIPAA, see FAQs 13-54.)

What does the notice say about fundraising?

A hospital can use your records in a limited way for fundraising. You have the right to tell the hospital not to use your records for fundraising. If you say nothing, then use of your records for fundraising is permissible. Each fundraising communication must include a clear and conspicuous opportunity to opt-out of future fundraising communications. Exercising this opt-out right may not be of critical importance, but it helps everyone if some people exercise opt-out rights when they exist.

What does the notice say about disclosures for national security?

Look for the national security disclosure provision. A covered entity can disclose your records for just about any national security purpose. The rule does not require a warrant, court order, subpoena, or any procedure prior to the disclosure. We point this out because it is perhaps the most privacy-invasive of the HIPAA disclosure provisions.

You are also invited to look for other broad and objectionable disclosure provisions in the notice. Don't blame the hospital or doctor. The rule allows these disclosures to be made, and privacy notices usually reserve the right for a covered entity to make allowable disclosures. However, the disclosures are not necessarily mandatory. In other words, a doctor can disclose your record to the CIA, but the doctor can usually say no.

Provision allowing covered entity to change the notice

There will be a provision that says a covered entity can change the notice at any time and with retroactive effect. This isn't quite as bad as it looks. HIPAA limits the ability of a covered entity to change the policy. The covered entity must comply with HIPAA, and it cannot change the notice and take away your rights. However, if HHS changes HIPAA or if Congress passes new laws, then your rights can expand, diminish, or disappear.

Most privacy policies elsewhere (such as on commercial websites like search engines or clothing retailers) are not based on formal legal requirements and are changeable at the discretion of the record keeper. Changes are not always bad, but it is okay to be a bit suspicious.

Find the right to request alternate methods of communication

Find the right to request alternate methods of communications. This right may be important to you, and the notice tells you how to exercise this right. We explain this right in full later. (See FAQs 25-28.)

Contact information

At the end of the notice is where your will probably find contact information for the covered entity's privacy officer. If you have any questions or want to exercise your rights, the privacy officer for the covered entity is probably the first person to contact.

Wait - the notice says my records can be disclosed without my consent. What's up with that?

If you read the notice, you will likely come away with the feeling that your health records aren't really private. It's not an unreasonable conclusion. The notice describes many uses and disclosures that do not need your consent and that are permissible even over your express objection. We don't like it either. Still, we recognize that we have a complicated health care system, and there are many demands on health records for socially beneficial purposes. There is a legitimate policy justification for most of the disclosures permitted under HIPAA. Nevertheless, we think that some of the HIPAA standards for use and disclosure should be higher and that some of the procedures should create more barriers.

Sadly, we don't know any way to return to a health care system where only you and your doctor knew about your health and where no disclosures of your records were ever made without your approval. That system disappeared decades ago. We repeat again that we don't like it either. We do like it, however, when an insurance company pays for our treatment or Medicare pays our doctor bills. We like it when researchers find new treatments for diseases. We also like it that public health authorities can alert people about contagious diseases. Patients do benefit at times when their records are shared for appropriate purposes and with appropriate protections. We wish some of those protections were better.

In 1999, Maine implemented a health privacy law that required patient consent for many routine disclosures (e.g., to doctors, family members, hospital visitors). People hated the law so much that the legislature suspended the law within weeks after it took effect, and the consent requirements that upset people later disappeared. Some discretion is needed to make the world operate smoothly and in accordance with patient expectations. If you want to know more about the Maine experience, go to (http://www.worldprivacyforum.org/wp-content/uploads/2007/04/MaineHealthPrivacy1998_Gellman.pdf).

B. Right to Inspect and Copy Your Record

18. Why Both Inspect and Copy?

HIPAA provides each patient with the right to inspect his or her record and to have a copy of the record. These are two different things. You cannot be charged a fee if you want to inspect your records. This means that you can always see your record, even if you don't want to pay.

If you want a copy of the record to take with you, then you can be charged a fee. You can also be charged an additional fee if you ask for a summary or explanation of your record. You do not have to ask for a summary or explanation.

HHS has guidance for covered entities about patient access. While the guidance is for health professionals, individuals may find it useful at times because of the level of specificity. If you have a dispute about access with a covered entity, the official HHS guidance may help convince someone about the scope of your rights. (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html?language=es).

19. Do I Want to See or Copy My Record?

There are many reasons you might want to review your health record at your health care provider or insurer. Decide if any of these appeals to you:

- You plan to move to another city and want to bring your records to a new doctor so that the doctor has your current information on your first visit. You may not know who the new doctor is in advance so you cannot arrange a doctor-to-doctor transfer.
- You want a second opinion from another doctor and want to avoid having duplicate tests. If you have the records, you don't have to let your first doctor know about the second opinion.
- You want to make sure that your new consulting doctor knows about earlier treatments and previous tests.
- You want to keep a permanent copy of all your health records in one place and in your possession.
- You are curious.
- You want to make sure that your children have your records because you think that something in your record (e.g., genetic information or family

history that they may not know) may eventually be relevant to their treatment.

- You have given your medical power of attorney to your grandson, and you want him to have all of your records (not just those for your current treatment) so that he can make informed decisions or so he can obtain assistance in making choices. By the way, the records that you give to your grandson are not covered by HIPAA in his hands (except, perhaps, if he is a physician or other health care provider).

- You want to talk to a lawyer about medical malpractice and don't want your health care provider to know about it.

- You think that there might be incorrect or irrelevant information in your record.

- You think that you are a victim of medical identity theft.

- You think that your insurance company improperly denied your claim, and you want to see the record about you that the company maintains.

- You think that your doctor or insurance company is lying to you.

- Any other reason or no reason. It is your right to see or have a copy of your record. You don't need to have a reason. You do not have to tell anyone what your reason is.

20. Which Records Can I Get and in What Formats?

You can generally ask for your all of your records maintained by any covered entity, but the covered entity can withhold some records. We will cover that subject in FAQ 24.

The copying of paper records is familiar to everyone. For electronic records that a covered entity maintains (whether or not the information is formally maintained in an electronic health record), you have the right to obtain the information from a covered entity in an electronic format.

Generally, you can choose the electronic format you want as long as the information is readily reproducible in that format. In order words, a covered entity has to give you the format you want if it can without a great deal of trouble. Be sure to state your preference and ask for alternative formats if you can. You can also ask the

covered entity what formats it is capable of providing and then make an appropriate choice.

Remember that some electronic records (e.g., 3-D images created by an MRI) may be maintained in a format that requires special software to read. If your goal is to be able to share an electronic record with a physician, then the native format may be okay because your physician will likely to able to read it in that format even if you can't.

Depending on your purpose, you may be interested in records of your hospitalization, records from your family physician, records from your insurance company, records from your pharmacy or pharmacy benefit manager, or your records any other covered entity. You can ask every covered entity for all of your records, but the next few questions suggest reasons for narrowing your request.

You can tell a covered entity to transmit your record directly to someone you designate. Your request must be in writing, signed, and clearly identify the designated person and where to send the copy of protected health information. This is not the same as an authorization, which has many more elements to it. Authorizations are discussed in later FAQs.

We think this rule was needed because some hospitals made it hard for a patient's lawyer to obtain the patient's record. It's fine to use this capability, but be careful that you don't casually or accidentally sign a form that allows someone to get your health records. Whoever gets your records in this fashion may not be subject to HIPAA, and your records could conceivably be made public or used for marketing or profiling. If you allow a data broker or marketer to have a copy of your health records, you are not likely to be happy about the result. This particular change in the rule has potential for mischief, but your can protect yourself by being careful what you sign. That's good advice all the time.

21. How Much Will It Cost For a Copy of My Health Record?

A covered entity can charge a reasonable, cost-based fee for providing a copy. The fee may include only the cost of labor for copying, the cost of supplies for creating the paper copy or electronic media, and the cost of postage. Any other copying charges – including but not limited to administrative fees, overhead, retrieval costs for locating data – are improper.

Don't let anyone charge you more than is allowed by the HIPAA rule. If you don't think that the fees are proper, complain about it. You have a right to complain to the Secretary of HHS (via the Office of Civil Rights), and that right will be covered later. (See FAQs 46-50, 51.) Remember that state law may establish lower fees than

HIPAA allows or may not allow any fees at all. If you need records and can't afford to pay, ask for a waiver of fees. Some covered entities may provide some or all records without charge or at a discount, but they are not required by HIPAA to do so.

Standard copying costs can be as much as $1.00 a page or perhaps more. If you want a hard copy of an x-ray, the fee could be considerably more (but an electronic copy may be cost-free if transmitted to you electronically). Many health care institutions hire outside firms to handle copies. Copying hospital records is a business. Insurance companies and lawyers tend to be frequent requesters of records, and copying charges can be expensive because these requesters don't much care about the cost and because there is no competition. The result is that the standard charge per page can be high.

Your best strategy may be to narrow your request (see the discussion in FAQ 23 about what records to request) or just obtain an electronic copy of records that are already electronic. Copies of electronic records may be less expensive.

22. How Do I Make a Request for Access?

Start by reviewing the covered entity's copy of the notice of privacy practices. Remember that every covered entity must provide a copy of its notice to anyone who asks for one. In addition, a copy should be available on the website of each covered entity (if the covered entity has a website).

The notice of privacy practices describes your right to inspect and to obtain a copy of your record. It should also tell you the local procedure for making a request. You will likely be asked to write a letter or fill out a form in order to make your request for access. A covered entity can insist on a written request and may ask you for identification. Asking for an ID is reasonable because you don't want someone else to get your records without your consent. However, avoid letting a covered entity make a copy of your driver's license. Someone with access to your health records may use that copy to make you a victim of identity theft.

When you make a request, the covered entity must act on your request within 30 days. Don't count on an instant response. The entity can take an additional 30 days to respond if it provides you with a written explanation of the delay. If you need the records more urgently, say so. It might help, but the rule allows the covered entity to wait 30 days or more no matter what. Your doctor might be responsive to your need for fast access, but bigger institutions have formal procedures and may not be inclined to do anything but the minimum required of them.

This is a real-life example. A patient needed a copy of x-rays and CAT scans in

order to get a second opinion on a critical injury that required immediate surgery. The hospital told the patient to make a written request and wait 30 days for a response. The patient's medical needs were urgent, but the hospital didn't care to help. The patient found another way. He explained the problem to a nurse who was sympathetic. The nurse quietly made an electronic copy of the needed records on a thumb drive and gave it to the patient. The nurse may not have followed the hospital's internal procedures, but the disclosure to the patient did not violate the law. The lesson is that if the official methods don't meet your needs, see if you can find another way. Just don't break the law doing it. Remember to thank (and protect!) your sources.

23. What Records Should I Ask For? The Strategy of Asking for Records.

A covered entity must allow you to inspect or obtain a copy of your record. Some records can be withheld. (See the next FAQ.) Just figuring out who to ask and what to ask for can be complex. Don't assume that you need a copy of all records from all health care providers and insurers.

Obtaining your health records can be surprisingly complicated, may present some hard choices, may be expensive, will require some planning, and can take time. Managing many records from many different providers may be a challenge too. This FAQ tells you about the strategy for requesting health records.

First, copying costs for paper records may be considerable. You may want to think about the costs involved before you ask. A hospital record can have hundreds or even thousands of pages. Think about whether inspecting your records will meet your needs. If you can inspect first, you might be able to narrow your request and cut the cost. Copies of electronic records may be much less expensive than copies of paper records.

You might be able to inspect your records and make a copy with your digital camera, cell phone, or a portable scanner. If you try using your own equipment, don't be surprised if the covered entity doesn't like it and tries to stop you. However, if you can see the record, you should be able to make your own copy. Nothing in the HIPAA rule says that you can't. However, if you want to wheel in a 500-pound copying machine, you'd better ask permission first.

Second, if you have been using the same hospital or doctor for 20 years and the reason for your request relates only to your treatment from your last visit, you might limit your request to recent records, or records dating back one visit, one month, or one year. The same idea may work if you want records from your insurer.

You may not know which records you need at first. The point is that you want to obtain records that you think are relevant, but you may not want every record from every HIPAA-covered entity. Most people have had dozens of health care providers and insurers in the course of their lives. Many records will not be important or worth the time and effort to find for most people. Old records from individual practitioners may be hard to locate and obtain. However, hospitals and other long-standing institutions are more likely to have older records, although they may be in storage offsite.

If you want your records because you think you might have been a victim of an identity thief, you will find some more specific advice at the World Privacy Forum's FAQ for Medical Identity Theft Victims, available at: (https://www.worldprivacyforum.org/2012/04/faq-victims-of-medical-id-theft/).

It is possible that a thief used your name to obtain services from a health care provider, clinic, pharmacy, or laboratory that you never used yourself. Don't be surprised if the trail leads you to unexpected places.

One part of the health care world that few people recognize is the Pharmacy Benefit Manager or PBM. A PBM is a company that contracts with managed care organizations, self-insured companies, government programs, and other insurers to manage pharmacy network management, drug utilization review, and other activities. A PBM is likely to be the organization that fills your drug prescriptions by mail. A PBM may have relevant records. Your health plan hires the PBM, and you may have to seek access to PBM records through the plan. The notice of privacy practices should tell you what you need to know on this front, or it should tell you how to find out. PBM records may duplicate records that exist elsewhere, but they can be important sources of information at times. If you are seeing more than one doctor, clinic, or hospital, PBM records are likely include information from different providers.

It can be especially important to correct errors in Pharmacy Benefit Manager (PBM) records. If you apply for individually underwritten life insurance or certain other types of insurance, the insurance company will insist that you sign a consent for disclosure of your health records. The insurance company wants to know if you have a health condition that affects your insurability. The easiest place for the insurer to obtain your records may be from a PBM rather than from your doctor. PBM records are electronic and can be shared quickly.

Your doctor may not respond to the insurer's request as promptly

Third, asking for a copy of your complete paper health record may provide more information than you need. It may also be especially expensive. Your health records may include results of x-rays and other diagnostic tests that may be costly to duplicate.

On the other hand, if records are electronic, it may be easy and inexpensive to obtain an electronic copy of everything or almost everything. If the covered entity has electronic records, it must give them to you in electronic form if you want them in that form. You can ask for hard copy of electronic records, but the cost might be higher. Not all electronic records can be printed on paper. You can obtain electronic records in the format you want if the covered entity can reasonably provide them in that format.

Consider how you might limit your request for access so that you limit your costs. See if you can talk to someone in the record keeper's office when you make a request so that you can negotiate what you really need. One idea is to not ask for a hard copy of an x-ray unless you know that x-rays are essential. Even then, an electronic copy may be sufficient. If other records are especially expensive to duplicate, you may want to defer asking for those records too. Ask for a price list before requesting all records. Another idea is to ask to inspect your records first so you can decide which parts you want to have copied.

Fourth, once when you receive some records, you may be able to focus your later requests. You may find that the provider used a lab or other independent provider that has some of your records that you may want to have or that you may want to inspect.

Fifth, there are health records and there are billing (and other administrative) records. These records may be controlled by different offices at a health care provider. You are entitled to both health and billing records, but you may not want both. It depends on your purpose. If you narrow your request, the response may be faster and less expensive.

Finally, copying of electronic records can be very inexpensive. If you want a copy of all of your electronic records, you can ask for them. It's a reasonable request. Understand that the records may not arrive in a single, chronological file, however. You may receive many different files in different formats.

If you are planning to maintain your own health record archive for your lifetime, remember that computer record formats may change over time. Some formats go out of date. For example, it can be difficult or impossible today to read a file saved by

a 1992 word processing program. Consider asking for records in formats likely to remain in use in the long run. Experts think that PDF may be one of those formats, but there may be others. This can be a complex issue to assess.

More on requests for electronic health records

There are many reasons why you might want to have an electronic copy of your health records, whether in whole or in part. We do not take issue with that in any way. We do, however, want to offer a thought from a different perspective.

How are you going to secure that electronic record? Do you want to keep it on your phone? On your notebook computer or tablet? On your work computer? In the cloud? There are many options here, and each presents its own security issue. Security is neither simple nor automatic. Securing electronic information is hard to do, even if you are good at it.

When you take possession of your own electronic health information, you take responsibility for the security of that information. If you lose your phone, if your computer gets hacked, if you accidentally attach the wrong file to an email message, the health record that you had may lose some of the legal and security protections it once had.

If your child uses your desktop computer, there's a chance that the child will find the health record stored there, whether it is his, yours, or your spouse's record. You can't withdraw the knowledge once the child obtains it, and that knowledge may affect family relations forever. If you accidentally share a document showing your diagnosis with your brother-in-law, there's a chance that he will share it with other relatives.

Failure to control health information in your possession may have major consequences for you and your family. The same thing can happen with paper records, of course, but it may be true that the dangers are greater with electronic records.

Institutions that have your records, including health care providers and insurers, do not necessarily have perfect security all of the time. (There are regularly reported breaches of health care institutions.) However, we suggest that most health care institutions probably have better security for the health records they maintain than you do. The HIPAA security rule imposes many requirements on HIPAA-covered entities. Even if a covered entity does security poorly, it's still probably better than the security on your phone or your local network at home.

File this under "you have been warned".

24. Can a Covered Entity Withhold Any of My Health Records?

Yes. In some situations, a covered entity can withhold records.

First, the right of access under HIPAA does not extend to psychotherapy notes and materials compiled for litigation.

Second, a covered entity can deny you access to some records, including records maintained by a prison, some records about research participants, and records obtained from someone other than a health care provider under a promise of confidentiality. The HIPAA privacy rule does not require a health care institution to allow you to appeal the denial of these records, but some institutions might accept an appeal if you file one. Read the notice of privacy practices to learn if there is an appeal option. We recommend that you appeal to the head of the institution (or to the privacy officer) even if you don't have the right to do so. An appeal may result in a review of the initial decision. If it doesn't, then you only invested the energy of writing a letter.

Third, a covered entity can deny you access to some records if a licensed health professional determines that access is reasonably likely to endanger the life or physical safety of you or another individual. Records about other people can be withheld if a licensed health professional has determined that access is reasonably likely to cause substantial harm to that individual or another person. Requests made by an individual's personal representative can also be denied if disclosure would cause substantial harm. If an institution withholds records for any of these reasons, it must provide a written denial explaining the reason for the denial. It must also explain any appeal rights that you have.

Remember that state law may grant you greater access rights than HIPAA. If state law has an access provision for health records – and many states do – then you may be able to obtain records exempt under HIPAA. If a federal agency has your records, rights of access under the Privacy Act of 1974 may be greater than the rights under HIPAA.

To be complete, we will tell you that HIPAA has a complex definition for something called a designated record set. You can get access to records that meet this definition and that aren't otherwise exempt. There may be some records about you that are not part of the designated record set, but they are likely to duplicate the records that you can see. This limitation in the rule solves some administrative problems, and it isn't a sinister plot to deny you access. We suggest that you not worry about it.

For example, if you had surgery, some of the records about your operation may

be kept in the operating room records in addition to being in your main hospital health record. A patient normally doesn't need to see the same information twice. However, if you request your records and the covered entity tells you that none of your records are part of a designated record set, something may be wrong. There must be some records that are part of a designated record set.

C. Right to Request Confidential Communications

25: What is the Right to Receive a Confidential Communication?

You have the right to ask a health care provider to communicate with you by alternative means or at alternative locations. This means, for example, that you can ask your fertility clinic not to call you at work or to send you an email notification of an appointment. You could ask your psychiatrist not to leave a message about an appointment at your home telephone voice mail. You might also ask a specialized clinic not to send you a post card reminder of your appointment but to use a closed envelope. A provider must accommodate reasonable requests. We think that all of the examples in this paragraph are generally reasonable. We also think that that asking for written communications – including bills – to be in plain envelopes with no identification of the provider in the return address is also reasonable.

Did you ever get an unwanted robocall from your doctor, pharmacy, optometrist, dentist, or other health care provider? If you hate robocalls, you can use the right to request a confidential communication to ask that you not receive automated calls. In our opinion, a request for no robocalls is reasonable.

You may be aware that the Telephone Consumer Protection Act (TCPA) limits robocalling with some exceptions. The TCPA rules are complex, and we won't pause to explain them here. But the TCPA has a big exception for robocalls that comply with HIPAA. HIPAA allows a health care provider to communicate with you for treatment, case management, and under other circumstances, including prescription refill reminders. A provider can't robocall you for marketing, but the distinction between a marketing call and a treatment call can be a fine one. An optometrist who

calls saying it's time to examine your eyes to see if you need new glasses wants to sell you goods and services, but that call (robocall or not) is probably allowed under HIPAA.

You may be happy to have reminders from your health care providers (whether automated or not). If not, the next FAQ tells you how to go about making a request that stops robocalls.

The right to receive a confidential communication is a real right that may be important to you. Not everyone will care or will care all the time. You may not object to a postcard from your dentist reminding you to make an appointment to have your teeth cleaned. However, many people would likely object to receiving a postcard informing them about a follow-up visit to a sexually-transmitted disease clinic.

The right to receive a confidential communication is important because a provider doesn't need express permission to contact a patient at home or to leave a message on an answering machine. For a patient who doesn't want others in his or her family or household to know about a form of treatment, then exercising the right to receive a confidential communication will be crucial. For some, this right may provide a vital privacy protection that will make the greatest difference to your life or wellbeing.

26: How Do I Exercise the Right to Receive a Confidential Communication?

A provider may require you to make a written request to receive a confidential communication in writing. Read the notice of privacy practices to find out the local procedure. In a small office, an oral request may be sufficient. Still, if you orally tell the receptionist not to call you at your office, the doctor may not know about your request. A written request may be safer because it creates a formal record of the request. You should keep a copy of your written request.

The rule says that a provider must permit a patient to make a request, but it does not expressly say that the provider must respond at all, or in writing. However, a provider must agree to a reasonable request. It's a good idea to ask for a written acknowledgement and to save the acknowledgement. If you only receive an oral response, you might want to send a written confirmation to the provider, and keep a copy of your confirmation. The written confirmation should summarize the request and identify the person who agreed to comply. Ask the provider to respond if the summary is incorrect.

You do not have to tell the provider why you made the request. Indeed, the rule expressly prohibits a provider from requiring an explanation as a condition of fulfilling the request. However, the rule does not prohibit the provider from asking for you reason. You don't have to disclose your reason if you don't want to.

Here's a draft letter that you can use as a model to make a request for confidential communications. We offer two different examples, one about robocalls and the other about emails to a work address. You can easily modify these examples to cover to redirect unwanted calls to a different phone number or to stop some other type of unwanted communication. Remember that a covered entity's notice of privacy practices is likely to include details about how to make the request and where to send it. Check that notice before you sent your letter.

Note that a HIPAA-covered entity can ask you to specify an alternative method of conduct so we include several options in the draft letter. You can choose one or both options or another option of your choice.

Sample Letter Version 1: No Robocalls

[Name and address of health care provider or health plan]

This is a request for confidential communication pursuant to the HIPAA health privacy rule at 45 C.F.R. §164.522(b)(1).

I request that [name of covered entity] stop calling me at [phone numbers] using an autodialer that delivers a pre-recorded message of any type. These calls are sometimes referred to as robocalls.

As an alternative to robocalls, you may send me snail mail at [address].

I would appreciate a written response acknowledging and accepting this request. Thank you.

Sample Letter Version 2: No Emails to my Work Address

[Name and address of health care provider or health plan]

This is a request for confidential communication pursuant to the HIPAA health privacy rule at 45 C.F.R. §164.522(b)(1).

I request that [name of HIPAA-covered entity] stop sending me electronic mail at my work address. My work address is [me@employer.com].

As an alternative to electronic mail to my work address, you may send message to me by sending:

- electronic mail to my personal address at [me@personaladdress.com] or
- postal mail to my home address, which is [Me, 1234 Main Street, City, State, Zip].

  [Choose one, both, or another option]

I would appreciate a written response acknowledging and accepting this request.

Thank you.

Confidential Communications

We think that the right to receive a confidential communication is a real right that will be meaningful for some patients. If you don't want your psychiatrist leaving an appointment reminder with your secretary, make a request for a confidential communication. Remember that a covered entity must agree to a reasonable request so don't take a denial of your request from a lazy staff member without a fight. If you make a reasonable request and your provider doesn't accept it, you can complain to HHS.

Remember that having a written document about your request in your health record is a better protection than reliance on an oral agreement. The current receptionist may know of your request, but a new or temporary receptionist may not.

Facebook and Health Confidentiality

If you share your health information with a non-covered entity, and social media companies are generally not HIPAA-covered entities, you may lose some of your privacy. You can read more about this in our report on Personal Health Records where we discuss the risks to confidentiality when health files are stored at third party commercial web sites that are not covered entities under HIPAA. (https://www.worldprivacyforum.org/2008/03/resource-page-personal_health_records/)

How does this apply to you? If you "like" your health care provider's page on Facebook, don't be surprised that others know you are a patient of that provider. You may care much less about the disclosure if the provider is a dentist than if the provider is a psychiatrist.

If you reveal details about your health condition on commercial (or even non-commercial) health or social media websites using your real identity, privacy issues may arise. For example, if you join a disease advocacy group, others may assume that you or a member of your family suffers from that disease. Not all of this sharing may be troublesome for you. Concern about privacy varies widely.

The point is that you should be aware what can happen when disclosing your protected health information with those outside the umbrella of HIPAA. Once you disclose health information to the world, it may be captured by an advertiser, marketer, database company, put in a profile about you or your household, and used to affect you (or your children) for the rest of your life.

27. Does the Right to Receive a Confidential Communication Apply to Health Plans?

Yes, but the rule is a bit different. To make a request to a health plan, the individual must clearly state that the disclosure of all or part of the information could endanger the patient. The plan may require that a request contain a statement that disclosure could endanger the patient. The plan can demand a written request.

It is not apparent, however, that the patient must identify what the harm is. The statement that disclosure could endanger the patient seems to be enough. Perhaps the most likely example of endangerment is a threat of domestic violence. A battered spouse may not want information about her location or activities to be accessible by her batterer.

We can't be sure about everything that might constitute endangerment. We take the position that it is up to the patient to decide what it means. If you say that disclosure could be potentially endangering or merely embarrassing, that's enough to convince

us. If a disclosure to the wrong person might persuade you to stop seeking treatment, we would argue that also constitutes endangerment.

We can't predict how plans will respond, but we emphasize that plans must accommodate reasonable requests. Asking to send mail to an alternate address (physical or email) strikes us as reasonable. Asking for phone calls only to your cell phone and not to your home phone also strikes us as reasonable. Asking for messages to be sent by carrier pigeon will not be viewed as reasonable by anyone.

28. Are There Any Other Requirements for the Right to Receive a Confidential Communication?

A plan or provider can condition the accommodation on the patient providing an alternative address or means of contact for information about how payment will be handled. This means that you can't ask someone to send all bills to the White House unless you are the President.

There's an exception for emergencies. No matter what restriction a covered entity agreed to, it can ignore the restriction in case the information is needed to provide emergency treatment. Fair enough.

D. Right to Request Amendment

On our list, the right to request an amendment of your health record is only the fourth right out of seven. Normally, access and amendment go hand in hand. We list amendment lower because the limits on the amendment right seriously undermine its utility. Nevertheless, if you can use it, the right to request an amendment may be important to you.

We want to underscore that the law does not give you a right to amend your record. You only have a right to request an amendment. We see this as a reasonable implementation of a patient's interest in amending a record. The record keeper has rights and interests as well as the patient, and these rights and interests deserve respect too. You cannot, for example, reasonably expect your doctor to change the record so that it no longer shows that you were treated. A doctor has a legal and professional obligation to maintain treatment records.

This part of HIPAA comes as a surprise to many who believe they have a right of outright deletion. This is not the case.

Is there a right to deletion of information?

This is a question we are asked frequently. Health care providers in the US that are covered under HIPAA do not have requirements to respond to requests to fully delete data from health records. There is a process under HIPAA to request an amendment. (See FAQ 29.)

It is often surprising to patients when encountering a refusal to delete information by a health care provider, and it can cause a lot of dismay. This is especially true if a patient is trying to get inaccurate information removed from a file. See FAQ 30 for more on how to approach this issue.

29. How Do I Make a Request for Amendment?

Start by obtaining a copy of the notice of privacy practices. You may already have a copy. If not, each HIPAA-covered entity must provide a copy of its notice to anyone who asks for one. In addition, a copy should be available on the website of each covered entity (if the covered entity has a website). The notice of privacy practices describes your rights, including your right to ask for an amendment. The covered entity's notice will tell you where to submit your request for amendment.

You might be asked to write a letter or fill out a form to make your request for amendment. You might be asked to tell the record keeper what information is wrong or is not about you. You may have to explain why you want the amendment.

When you make a request, the covered entity must act on your request within 60 days. The entity can take an additional 30 days to act if it provides you with a written explanation of the delay.

It is hard to object to the formality of the amendment process allowed by the rule. We hope, however, that covered entities don't use it inappropriately.

If you want to report a change of address or corrected telephone number to your family doctor, you should be able to tell the provider or the provider's receptionist without any formality. A covered entity can ask for a written request, but it doesn't have to do so.

If someone in a doctor's office who knew us said that we had to write a letter to change an incorrect telephone number, we would complain to a supervisor or

physician. But if you are not known to the provider, it might not be unreasonable if the provider first asked you to show identification. Changing an address is one way that medical identity thieves try to hide the trail of their activities.

30. Can I Ask that Incorrect Information be Removed From My File?

Yes, but it may not be that easy. A HIPAA-covered entity does not necessarily have to remove incorrect information. It can mark the information as incorrect and add additional notes that show the correct information.

There is a reason for this policy. Suppose that your doctor suspects that you have an infection. Before the test results come back, the doctor prescribes an antibiotic. When the test later shows that you didn't have the infection, the doctor tells you to stop taking the antibiotic.

Now suppose that you ask the doctor to remove the initial diagnosis of an infection. If the information is totally removed, it will be impossible for the doctor to explain or justify the prescription for an antibiotic. It may not be appropriate to remove the entire incident from the record because the doctor will be unable to explain the treatment provided or the bill for the services. The doctor also needs to keep the record in the event that there are complications from the drug. The doctor rightly needs a history of the treatment for his/her protection for both legal and medical reasons. Your health record isn't just about you. It's about your provider too.

Some requests for amendment present real conflicts between the interest in having an accurate record on the one hand, and having a record reflecting what treatment was provided to a patient and why, on the other. These objectives will conflict at times. Information that seemed to be correct one day may be incorrect on another day. A health record may need to reflect both conclusions, even though they are different.

If you disagree with your physician's diagnosis, but the physician insists that the diagnosis is correct, you are not likely to prevail with an amendment request. You have to right to put your views in the record, as we explain later. (See FAQs 34 and 35.)

Health care providers are typically nervous about removing information from health records. For the most part, they have a reasonable concern for the reasons explained above. However, when the information in your health record is not about you, the provider's concern is weaker. When the information in your record is not about you and the presence of the information did not affect your subsequent care, the argument for removal is stronger. For example, if your record includes a lab slip belonging to another patient, it may be appropriate for the record keeper to remove the slip entirely and put it in the right record.

However, if the incorrect information affected your treatment – even if that treatment was inappropriate – then retaining some or all of the incorrect information (suitably marked as incorrect and including a full explanation) may be legally and medically justifiable. You may be able to negotiate with the provider about how the information should be marked or otherwise segregated from your health record.

The problems faced by medical identity theft victims seeking amendment of their record can be particularly difficult. See the World Privacy Forum's FAQ for identity theft victims at (https://www.worldprivacyforum.org/2012/04/resource-page-medical-identity-theft/).

If there is information in your file that is not about you at all – whether because of a filing error, medical identity theft, or other reason – you should ask for its total removal. The covered entity may still be unwilling to comply.

Another possible remedy is to ask the entity to put the information about another individual in a wholly separate record that is not directly associated with your health record or in a sealed part of your record.

The two records might contain references to each other, but the substantive health information about the other person will not be in the normal file that a doctor would review when treating you. A covered entity may not agree to do this, but it is worth a try.

31. What Other Limits Are There on the Right to Seek Amendment?

A covered entity does not have to amend a record that it considers accurate and complete. It does not have to amend a record that is not available for inspection by you under the access provision.

More importantly, a covered entity is not required to amend a record not created by the covered entity. That means if the information in your record came from any third party – including another provider, an insurer, a relative, or anyone else – the covered entity has no obligation to amend your record or even to consider your request. We find this limitation on the right to seek an amendment to be unfair, inappropriate, and dangerous. Be aware that state law may not have the same limitation on amendment rights.

A provider can treat you using information in the file that you contend is incorrect, but that provider has no obligation under HIPAA to determine whether the information is wrong when you contend that it is wrong. This is why we think that this exception is unfair, inappropriate, and dangerous.

The covered entity must consider your request for amendment of third-party information if you provide a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment. Thus, if the record contains information from a previous physician who is no longer in practice, you may be able to force your current provider to consider amending information supplied by that physician. We note that it can be difficult to prove that the originator of information is unavailable, and an uncooperative covered entity can string a requester along if it doesn't want to deal with a request for amendment honestly.

If the covered entity that is the originator of the incorrect information is available but does not act on a request for amendment, the information in the subsequent covered entity's record may be just as wrong and could have a continuing detrimental effect on the patient. This can present a real Catch-22 for patients.

In most circumstances, a health care provider will act reasonably to verify information that may affect patient care. For example, if you tell your surgeon that you think that your blood type is A, the surgeon is not likely to cavalierly accept contrary information just because it came from a third party. Any health care provider is likely to be suitably concerned about the possibility of a medical error based on wrong information.

However, there may be real problems with third party information in some circumstances. Health insurers may not be as worried about an error, especially if the error provides an excuse to deny a claim.

Consider an identity thief who has an appendectomy while masquerading as John Doe. The real John Doe has an appendectomy a year later and submits the bill to his insurance company. The insurance company rejects the bill because no one has two appendectomies. If John Doe asks the insurer to amend or delete the record of the first payment, the insurer can refuse the request under the HIPAA rule because the information came from a third party, namely the surgeon who operated on the identity thief. If John Doe then asks the surgeon to correct the record, the surgeon will likely reject the request saying that the request came from a John Doe who used the same health identification number, and the surgeon may decline to figure out who is who.

The HIPAA health privacy rule provides no real assistance or remedy under these circumstances. Unless someone goes beyond the minimum requirements of the HIPAA rule and addresses the real problem, it is possible that a patient will have no remedy at all under HIPAA. It may be necessary to find another way to force attention to your problem, such as filing a complaint, hiring a lawyer, writing your congressman, or some other activity. We think that HIPAA should provide you a real remedy here, but it does not.

If the rule doesn't provide a remedy when one should be available, the patient may only be able to ask for the good will, understanding, and cooperation of all concerned. Providers and insurers who proceed in good faith may solve a patient's legitimate concerns notwithstanding the deficiencies of formal legal remedies. If you are not getting the cooperation you need, try talking politely to the privacy officer of the covered entity. Filing a complaint with HHS is another option. The last step may be litigation (or the threat of litigation), and that is often an expensive and unattractive alternative for everyone concerned, even when litigation is possible.

32. Do I Have Greater Amendment Rights under State Laws, other Federal Laws, or Hospital Policies?

Maybe. Some states have health privacy laws that provide greater rights of amendment. If your records are held by the federal government (e.g., Medicare, VA, or Indian Health Service), your rights to ask for amendment of records under the Privacy Act of 1974 may be greater than under HIPAA. These two sets of privacy

rules overlap, and you are entitled to the best parts of both laws. Not only may other laws provide patients with better amendment rights than HIPAA, but they may offer better remedies and clear causes of action in case you have to sue to correct records.

33. What Happens When a Covered Entity Agrees to Make an Amendment?

The covered entity that agrees to make an amendment must:

- Make the amendment;
- Tell the requester what it did; and
- Make reasonable efforts to inform others about the amendment within a reasonable time.

The third requirement is most noteworthy. If you convince a covered entity to amend your record, the covered entity must tell any persons that you identify who received the original incorrect information and who need the amendment. In addition, the covered entity must notify any persons who have the information that was the subject of the amendment and who may have relied or could foreseeably rely on the information.

To make sure that amendments have been appropriately distributed, you may want to ask for an accounting of disclosures. The right to receive an accounting is explained elsewhere in this guide. (See FAQs 37-44.) What is important is that amendments be provided to those who may rely on the original incorrect information. Each patient has the right to tell a covered entity to send the amendment to anyone who received the original information and needs the information.

Be sure to ask that any amended information that bears on your future medical treatment be shared with other providers. Similarly, be sure to ask that amended information that bears on insurance and payment matters is shared with insurers and, possibly, with employers. The goal is to find and eliminate any incorrect information that others have and that may affect you adversely.

It may take considerable effort to make sure that every appropriate person has the information and that those with the information correct their own records. Every covered entity must act when it receives a notice of amendment, but that doesn't mean that it will be done quickly or properly. It may be appropriate to ask each covered entity that received an amendment to confirm that it actually made the amendment. You may have to request a copy of your record from that covered entity

to be certain. Should you do all of this? It may depend how important the information is to your future treatment.

Be aware of any Health Information Exchanges that may impact where your records are located. For example, covered entities in some states exchange electronic health records through a third party called a Health Information Exchange. Ask about the presence of an exchange or network so you can locate all of the copies of your records.

As health records and health networks expand, some aspects of seeing and amending records may become easier. But some things may be harder, especially if no entity has clear responsibility for a health record. This is an evolving area, and there may be a lot of learning for everyone to do.

There may be some strategy involved in asking a covered entity to send notices of correction to recipients. When you look at the accounting of disclosures, you may be surprised at the number of people and institutions that received the original, incorrect information. You may not want all of them to receive the correct information.

Suppose that (with your consent), your doctor reported to your employer that you were justifiably absent from work because you had the stomach flu. A later test reveals that you had a more serious illness or were pregnant. You might not want this additional information shared with your employer, but you might want another physician to know.

If the correct information would affect how a health care provider might treat you, then sending the correction is the right thing to do. But you might not care about sending a correction to a physician who treated you in an emergency room if you have no expectation of ever being treated there again. Whether you want your health plan to know about a correction may call for some evaluation.

34. Can I Appeal if a Covered Entity Refuses to Make an Amendment?

Maybe. An institution must accept complaints about its health privacy policies and practices. Filing a complaint with an institution may not be the equivalent of filing an appeal of a denial of a request for amendment, but it may help if it forces someone new at the covered entity to review your request. However, some institutions may accept formal appeals. Consult the institution's notice of privacy

practices to see if there is an appeal method for a denial of a request for amendment. Talk to the privacy officer at the covered entity to see if you can obtain help.

You can also complain to the Secretary of the federal Department of Health and Human Services about how your request was handled. The Department's Office of Civil Rights processes complaints. You can find information about the process at (http://www.hhs.gov/hipaa/filing-a-complaint/what-to-expect/index.html).

You have another alternative. When a covered entity denies your request for amendment, it must tell you that you can request the covered entity to provide a copy of your request for amendment with any subsequent disclosure of the disputed information. In some instances, it may be important to make the request. Remember that the covered entity is not required to tell others about the dispute unless you ask. Read FAQ 35 for more information about other remedies if your request is denied.

35. Are There Other Remedies if My Request for Amendment Is Denied?

Yes. You have the right to file a written statement of disagreement, and that is an important right. When a covered entity denies your request for amendment, it must tell you about this right.

The statement of disagreement gives you the opportunity to explain your side of the story. The covered entity can reasonably limit the length of the statement of disagreement, so don't plan on writing a novel-length document. We also suggest that your statement should be factual and should refrain from making personal attacks on anyone involved in the process. The covered entity can prepare and circulate a rebuttal to your statement of disagreement. If it does so, it must provide you with a copy of its rebuttal.

HIPAA offers another protection even if you don't file a statement of disagreement. The rule requires a covered entity that received and denied an amendment request to append or link the record in question to your request for amendment if you ask it to do so. The purpose here is to make sure that whoever sees the disputed record will also see the request for amendment.

If you ask for a change and it is denied for a good reason, you may not want to ask that your request be shared. However, if you still disagree and you want others to know your views, then you should ask. One reason to ask to inspect or have a copy of your record is to see if the covered entity properly handled this requirement.

36. Can a Covered Entity Still Disclose The Information that I Disputed?

Yes, but HIPAA offers additional rights. First, if you submitted a statement of disagreement, the covered entity must disclose it when it discloses the disputed information.

Second, if you choose not to submit a statement of disagreement, the covered entity must include your request for amendment (and its denial) along with any subsequent disclosure only if you requested that the covered entity do so. If you ask for a change and it is denied for a good reason, you may not want to ask that your request be shared. If you still disagree and you want others to know your views, then you should ask.

E. Right to Receive an Accounting of Disclosures

37. What's an Accounting of Disclosures?

For a disclosure of health information about an individual, an accounting is a record of:

- The date of the disclosure
- The name of the person or entity who received the information
- A brief description of the information disclosed
- A brief statement of the purpose of the disclosure (or, as an alternative, a copy of the request for a disclosure).

The non-intuitive term accounting comes from an older privacy law. It's clearer to think of an accounting as a disclosure history. We will stick with the rule's accounting terminology here because that's the term commonly used in HIPAA circles.

38. Why Should I Care about Accounting of Disclosures?

Many patients won't care, and that is okay. However, the accounting of disclosures can be crucial in some instances. You may want to ask for an accounting if you think

that your records were improperly disclosed, if you think that you may be a victim of medical identity theft, or even if you are just curious about the circulation of your health records. Be warned, however, that if you ask for an accounting, the response is likely to undermine whatever faith you had that your health information is confidential. Records may be lawfully disclosed to other institutions that have nothing to do with your treatment or the payment for your treatment.

The accounting of disclosures will be invaluable if you need to follow the trail of your information and learn who has information about you. If you corrected your record through the amendment process, the accounting should allow you to find out who received the original information and who received the corrected information. It provides a way for you to tell whether the covered entity properly distributed the amendment.

The accounting may reveal some disclosures that are normal (e.g., to your health plan). You may also learn that the covered entity disclosed your records to a researcher, public health agency, or government auditor. These disclosures may not have any immediate consequences for you, but you may be either interested to know about the disclosures or unhappy that they occurred.

However, if you learn that your records were disclosed to law enforcement or health oversight agencies, you might have reason to worry that the information disclosed will be used against you in some manner. By learning the purpose of each disclosure, you will be better able to make judgments.

39. How Do I Make a Request for an Accounting of Disclosures?

Start by obtaining a copy of the notice of privacy practices that your provider or insurer publishes. You may already have a copy. If not, each HIPAA-covered entity must provide a copy of its notice to anyone who asks for one. In addition, a copy should be available on the website of each covered entity (if the covered entity has a website).

Follow the directions for a request in the notice. You might be asked to write a letter or fill out a form in order to make your request for amendment. The covered entity must act on a request for accounting within 60 days, but it can extend the time limit for another 30 days if it provides a written explanation of the delay.

40. Who Has to Provide Me with an Accounting of Disclosures?

Any HIPAA-covered entity must provide a copy of an accounting of disclosures. For most individuals, your health care providers (doctors, hospitals, laboratories, pharmacies, etc.) and health insurers (HMOs, health plans, Medicare, etc.) will have accounting records that you may want.

You may also want to ask your *Pharmacy Benefit Manager* or PBM. A PBM is a company that contracts with managed care organizations, self-insured companies, and government programs to manage pharmacy network management, drug utilization review, and other activities.

41. What does it Cost to Obtain an Accounting of Disclosures?

You are entitled to receive at no charge one copy of the accounting of your health record in any 12-month period. If you make more than one request, the institution may impose a reasonable, cost-based fee. The institution must tell you the cost in advance so you have a chance to modify or withdraw your request.

If you have a good reason why you need to request an accounting more than once a year, ask the covered entity to waive any fees. For example, if you are a victim of medical identity theft and need repeated accountings to check on current activities of the identity thief and responses to corrective actions, ask for a fee waiver. Argue that both you and the covered entity are victims of the identity thief. You need to work cooperatively with the covered entity to correct the problem. Ask the institution's fraud investigator or compliance officer to help you if the usual HIPAA channels aren't responsive.

42. What are the Limitations of an Accounting of Disclosures?

Limitations in the HIPAA rule make the accounting of disclosures much less valuable than it should be. First, covered entities do not have to account for all disclosures. They don't have to keep an accounting of disclosures for treatment, payment, or health care operations. Most disclosures are likely to be for one of these purposes so this loophole is large.

Second, covered entities also don't have to keep an accounting of disclosures if you authorized the disclosure. That means that you may not be able to track if the covered entity actually disclosed records as you directed. If you casually signed an

authorization that allowed the disclosure of any or all information about you (e.g., for a background check), a covered entity can disclose your health record and not even keep a record that it did so. This is another loophole.

Third, health care institutions do not have to account for uses. A use of information occurs when a record is made available to someone within the institution that maintains the record. A disclosure occurs when a covered entity shares a record with someone outside the covered entity. The accounting requirement only covers some disclosures and no uses.

If you are hospitalized, hundreds of different individuals in the hospital may see your record. The use exemption to accounting can seriously undermine your ability to hold an institution accountable for leaks or other inappropriate activities. Still, in hospitals with modern computers, there is a greater likelihood that a complete audit trail, including uses, will be maintained routinely.

Unfortunately, HIPAA does not expressly require that a covered entity share that audit trail for uses, although there may be an argument that disclosure of an entire audit trail is required otherwise by HIPAA or by state law. Ask for a copy of the entire accounting because a reasonable institution will share it with you. Institutions with computerized systems that track all activity might find it easier to provide a requester with the entire history rather than part of it. However, they are not required to do so. It doesn't hurt to ask.

Fourth, sometimes a covered entity must withhold a particular accounting record from an individual who requests a copy of the accounting. A covered entity may make some disclosures to law enforcement, for example, without telling the record subject for a limited time.

Fifth, the HIPAA requirement for an accounting started on April 14, 2003. A health care institution covered by HIPAA did not have to maintain accounting records before that date.

Finally, perhaps the biggest limitation is that the federal health privacy rule does not require an accounting of disclosures for treatment and payment. This means that a lot of information that you would want to find in an accounting will not be available. Covered entities also don't have to tell you about disclosures for health care operations, an expansive category that covers many management and other functions.

For example, if a hospital gave care to someone in your name and billed your insurance company, you would want to know the details. You may not be able to obtain that information from the accounting of disclosures. Even worse, if a hospital told a credit bureau or collection agency that you did not pay your bill (i.e., a bill run up by an identity thief), the accounting may not reveal the disclosures. These

disclosures may be exempt from the accounting requirement because they fall within the exception for disclosures for payment and health care operations.

In 2011, HHS proposed changes to the accounting for disclosures rule. As of 2019, the changes have not yet been made final. Once final, it may be a while before covered entities must implement the changes. As proposed, some of the accounting changes were better for patients and some were not. We must wait and see when and what happens.

43. Why Bother Asking for an Accounting if It Has so Many Loopholes?

Why seek an accounting of disclosures? You may not need an accounting, but here are reasons why you might want one.

First, obtaining a copy of the accounting is free. All you have to do is fill out a form or write a simple letter.

Second, an accounting may help even if it isn't complete. You should be able to learn something about how the covered entity disclosed your records from the accounting. It may point you to some record keepers you didn't realize had records about you.

Finally, even though there are many exceptions to accounting, some institutions will nevertheless have a record about disclosures (and even uses) even though the records are not required by HIPAA. If you ask for more, you might just get what you want. Nothing in HIPAA prevents a covered entity from providing a more complete accounting than the minimum required by the rule.

44. Do I have Greater Rights under State Laws, Other Federal Laws, or Hospital Policies?

Maybe. A few states may have health privacy laws that require health care institutions to maintain better accounting records or to disclose more accounting records to you. If the federal government has your records (e.g., Medicare or VA), your rights to have a copy of an accounting under the Privacy Act of 1974 are

greater than under HIPAA. These two sets of privacy rules overlap to your benefit. See FAQ 2 to find other online resources that may help you understand state laws.

45. What's the Best Strategy for Making a Request?

You only are entitled to one free request in any 12-month period. Think about the best timing to make that request. If you learn that you were a medical identity theft victim two years ago, you probably should make the request right now. However, if your reason for asking relates to a current activity (perhaps a hospitalization that just ended), it can take time for your records to be updated. Actions that follow a hospitalization, such as submitting a bill to an insurer or to the government, may not occur immediately. You might want to wait a week or two before asking for the accounting. If the institution's privacy officer is helpful, the officer may be able to offer useful advice about timing.

Many institutions with computerized record systems have accounting records that exceed the HIPAA requirement. Modern computer systems routinely track every use and disclosure of a health record. HIPAA does not require a covered entity to give you all the accounting records that the entity has. That's unfortunate. It doesn't mean that you can't ask for non-HIPAA required accounting records if they exist. We suggest that you make a broad request.

If you are dealing with a federal or state institution, you might be able to use other privacy or freedom of information laws to seek records about you that may not be available under HIPAA. If the records are important to you, ask first for all the records. Even if there is no right, an institution may still be willing to share the accounting records, if only because it is cheaper and easier to do so than to separate the required from the non-required parts of the accounting.

If you ask for more, you might just get what you want. If asking doesn't get you what you need, use other laws and procedures if they are available.

F. Right to Complain to the Secretary of HHS

46. Can I File a Federal Complaint about a HIPAA Problem?

Yes. Any person who believes that a covered entity is not complying with the HIPAA privacy rule may file a complaint with the Office of Civil Rights (OCR) at the Department of Health and Human Services. You do not have to be a patient of a health care provider or a beneficiary of a health insurance plan to file a complaint. For example, if you visit a relative in the hospital and see a violation, you can file a complaint.

You generally must file a complaint with OCR within 180 days of when the incident occurred or when you learned about it.

You can find information about the complaint process at (https://www.hhs.gov/hipaa/filing-a-complaint/index.html). There is a list of regional offices at (https://www.hhs.gov/ocr/about-us/contact-us/index.html) including phone numbers. OCR wants you to file a complaint at the regional office for your state, and the website provides addresses and fax numbers. However, OCR doesn't necessarily make it easy. There is no email address for each regional office. If you look hard enough through the OCR website, you will find that you can submit a complaint by email to OCRComplaint@hhs.gov. An emailed complaint does not require a signature.

OCR has a complaint form that you can fill out at (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf). The complaint website has information in other language about how to file a complaint. You can use email to ask questions or need help. You can e-mail OCR at OCRComplaint@hhs.gov.In recent years, OCR opened a large number of investigations in response to complaints from individuals and otherwise. The total number of investigations that found a violation of HIPAA privacy and security rules averaged 2000 a year in recent years. That is a lot of violations and a lot of activity by OCR. There's a reasonable chance that a well-founded complaint will result in a review and change. Filing a complaint with OCR should be worthwhile.

You can file a complaint about the Security rule and find instructions on filing a complaint in other languages at (http://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html).

47. What Information Belongs in a Complaint?

The Office of Civil Rights at HHS wants a complaint to be signed and to include:

- Your name, full address, home and work telephone numbers, email address.
- If you are filing a complaint on someone's behalf, provide the name of the person on whose behalf you are filing.

- Name, full address and phone of the person, agency or organization you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule.

- Briefly describe what happened. How, why, and when do believe your (or someone else's) health information privacy rights were violated, or the Privacy Rule otherwise was violated?

- Any other relevant information.

- Your name and the date of the complaint.

Optional information that OCR requests includes:

- Do you need special accommodations for us to communicate with you about this complaint?

- If HHS cannot reach you directly, is there someone else to contact?

- Have you filed your complaint somewhere else?

48. Will Filing a Complaint Really Help?

There's now a reasonable chance that filing a complaint will produce a response and may lead to action. In the early years of HIPAA, enforcement of the Rule by the Office of Civil Rights was rare. In the last few years, OCR has become much more aggressive in enforcing the HIPAA privacy and security rules. Some of the penalties imposed on covered entities run in to the millions of dollars. If you file a complaint, it should receive appropriate attention. Remember, however, that the Privacy Rule complaint process is for HIPAA complaints. OCR receives and rejects many complaints because they are not about HIPAA matters.

We wouldn't hesitate to file a complaint if we thought that a covered entity violated HIPAA. But we remind you that filing a complaint may have the effect of spreading your health information around more widely. Not all complaint investigations will involve disclosure of the intimate details of your medical history, but some may. It is for you to judge whether a complaint will invade your privacy more than you can tolerate. Nevertheless, if you are just trying to get a hospital to respond to your request for a copy of your record, the additional threat to privacy may be small and your complaint to OCR may help you get what you want.

49. What Should I do if I See a Privacy Violation?

Now that the complaint process is working, filing a complaint with OCR has real potential to help. There is a real reason for the public to show interest in privacy laws and to use the process to protect individual rights guaranteed by law.

However, we think that the first step should be to complain directly to the covered entity that did something you think was wrong. Each covered entity has a privacy officer, and the name, address, and telephone number of the privacy officer should be included in the notice of privacy practices. Everyone makes mistakes, and everyone deserves the chance to make things right. It is also important for covered entities to know that people pay attention to privacy and that people care when privacy violations occur.

If the covered entity does not satisfy you, then you can look elsewhere. We don't think that every minor violation should become a federal case. Our first choice is to complain locally about any violation. If you do not get satisfaction locally, then consider a complaint to OCR. Remember that filing a formal complaint may bring more attention to you and to your health record. You may want to be guarded about how much of your personal health information you include in the complaint. In other words, the complaint process may further invade your privacy. But complaints keep the whole system honest and they can be important to patients and to covered entities trying to manage HIPAA compliance. It's your choice about how far to pursue a complaint.

Here are some ideas if you want to pursue a federal complaint.

- Complain to OCR as described above.

- If you do complain to OCR, consider sending a copy of your complaint to your congressman or Senators. Ask them to write to the Secretary of HHS and report back about what happens to the complaint. When an elected official writes to an agency on behalf of a constituent, the constituent's file gets a pink slip and that may get your complaint faster attention. The downside may be sharing your personal information more widely.

- You might be able to complain to a state official. Every state has a health department and an insurance department. If your complaint is about a health care provider, complain to the health department. If the complaint is about an insurer, complain to the insurance department.

- Health care providers hold licenses from state boards. If the violation is serious, see if the state licensing board accepts public complaints.

- If your problem is newsworthy and you are willing to make it public, you might look for a local reporter who covers health issues and who may be interested in your story. Remember that going public may make the privacy violation worse, but it may get better results. A hospital may be very unhappy to see a news story that said it violated someone's privacy or denied a patient rights guaranteed by law. A call from a reporter may produce a response that you couldn't get on your own.

- Use the Web. You may find websites where you can post your story and the basics of your complaint. Posting a complaint about a health care provider may help others and may be satisfying all by itself. If you post information publicly, be sure that you are not revealing too much of your personal health information.

- Tell your friends and neighbors. A national insurance company may not care what you say. However, local providers and local hospitals care a lot. A bad reputation can result in the loss of clients and revenues. Write something in a local listserv or blog.

- You may be able to file a lawsuit. HIPAA does not provide patients with the right to sue covered entities. However, other laws may allow you to sue. If the courts recognize that HIPAA establishes a standard of care, then it may be possible to sue for breach of contract, malpractice, violation of standards of professional conduct, or on other grounds to enforce HIPAA requirements. However, remember that lawsuits are not fun, take a long time, and can be expensive. Finding a lawyer willing to take a privacy case can be hard. Obtaining monetary damages can be highly uncertain. Lawsuits are remedies you should consider pursuing only after you tried other potential remedies and then only for major problems.

50. Should I Worry that a Covered Entity will Retaliate if I File a Complaint?

Each covered entity's notice of privacy practices must say that there will be no retaliation against a person who files a complaint. We would like to believe that.

But in the real world, there are no guarantees. We have seen, for example, a notice from a hospital that says – as required by the rule – that there will be no retaliation. The next sentence in the notice says more ominously that the hospital reserves the right "to take necessary and appropriate action to maintain an environment that serves the best interests of our patients and staff." We have no idea what that means or why the hospital chose to add that statement directly after the required language about not taking retaliation. But it sure sounds like a threat to us.

We would be happier to see a privacy notice that included a statement to the effect that the hospital reserves the right to take additional actions to protect the privacy of its patients. However, hospital lawyers don't like statements like that, lest they be interpreted to oblige the hospital to do more than the bare minimum.

G. Right to Request Restrictions on Uses and Disclosures

51. What is the Right to Request Restrictions on Uses and Disclosures?

The right to request restrictions is the least meaningful of the seven HIPAA patient rights. A covered entity must allow a patient to request a restriction on the uses or disclosures of the patient's information to carry out treatment, payment, or health care operations. A patient can also ask for a restriction on disclosures to a family member, relative, or close personal friend. Some requests made at a human level are likely to be fulfilled than those made at an institutional level. If you ask your doctor not to reveal something to your grandson, the doctor is likely to do what you ask. If you ask a hospital not to share your information with its administrative staff, the hospital is not likely to agree.

You can read later in this document about the scope of permissible uses and disclosures for treatment, payment, and health care operations. (See FAQs 55 - 67.) No covered entity needs your consent to make disclosures for those purposes. *Health care operations* is a particularly broad term that includes many activities that are in the interest of the covered entity and not necessarily in the interest of the patient.

However, there's a new element that came in 2013. You have the firm right to demand (not just request) that a provider not disclose PHI to a health plan if the disclosure is for treatment or payment, the disclosure isn't required by law, and if the PHI pertains solely to health care for which the patient (or someone on behalf of the patient) paid in full. We'll explain that new option in FAQ 53. It's well-intentioned but very messy to use.

52. Why is the Right to Request Restrictions Almost Meaningless?

The rule does not require a covered entity to agree to a restriction requested by a patient. The covered entity does not have to agree even if the patient's request is reasonable. Contrast this provision with the right to request confidential communication. A covered entity must agree to a reasonable request for confidential communication.

However, if you ask for a restriction on use or disclosure, the covered entity does not have to agree, does not have to state a reason for denying a request, and does not have to even respond to your request. Because it is a patient right without a corresponding obligation on the part of a covered entity, we conclude that the right is almost meaningless.

It gets worse. The rule expressly provides that some restrictions that an institution might agree to are not effective. These are uses or disclosures that are permitted for facility directories (separate rules govern facility directories), to the Department for oversight of the rule, or for any of the scores of other permissible disclosures allowed under the law. Thus, if an institution agrees to your request not to make a discretionary disclosure to the CIA, that agreement is not effective under the rule.

If the unlikely event that a covered entity agreed to a patient request and violated the agreement, OCR might respond to a complaint from a patient. But if OCR took aggressive action, covered entities would see that as a reason not to agree to any restrictions. It's not clear that any covered entities need more incentive not to agree than they already have.

A patient who had an agreement from a covered entity might be able to enforce the agreement through a complaint about professional misconduct or through a legal action for breach of contract. This is all rather hypothetical because it will be hard to convince any covered entity to agree to your request in the first place. It would be much easier to enforce an agreement if it were in writing.

It is highly unlikely that any large institution will agree to any restriction on use or disclosure. It is conceivable that you might get a small provider – e.g., a psychiatrist in a solo practice – to agree with your request. A bigger institution – especially one with a staff of lawyers – will probably never agree. Frankly, trying to get a voluntary agreement for a large covered entity is not likely to be worth the time and trouble.

53. The Right to Pay Out of Pocket

A 2013 change offers a new and mandatory restriction. You have the firm right to demand (not just request) that a provider not disclose PHI to a health plan if the disclosure is for treatment or payment, the disclosure isn't required by law, and if the PHI pertains solely to health care for which the patient (or someone on behalf of the patient) paid in full.

This looks like it is more meaningful than the right to request a restriction. If you meet the terms and make the request properly and in a timely fashion, a covered entity must agree. However, it will be hard for most patients to meet the requirements. As you read the following discussion of the problems with the new mandatory restriction, you will see what we mean.

The PHI must relate to fully paid health care: If a treatment included a service that was partly paid by insurance and partly by the patient, it does not qualify. So if you have surgery for a deviated septum paid for by your health insurance with a little added cosmetic surgery at the same time that you pay for, you cannot make a request to keep the cosmetic surgery restricted. The surgery was not solely paid for by the patient. If you pay for a treatment, but let your insurer pay for a related blood test, it will probably not qualify as a treatment solely paid by you.

Paying in full may be difficult for many patients. At some HMOs, payments by patients for some services are not allowed. Medicare may prohibit providers taking any payment from some patients. Costs may be too much for many patients, and patients paying on their own may not qualify for the negotiated lower prices that health plans pay.

The health care system is complicated and interconnected. You may pay for a service out-of-pocket and tell your doctor not to tell the health plan. Yet if the doctor sends a prescription electronically to a drug store, the drug store may not be aware of the restriction and is likely to automatically query the health plan. The same problem can arise with a laboratory or x-ray facility. A patient seeking to keep treatment information from a health plan will have to think ahead and be adept at finding non-standard ways of managing referrals or ordering tests. Requests to restrict may need to be made in advance of treatment or billing. Covered entities are sure to insist (as the rule allows) that requests be made in writing.

From the perspective of a covered entity, managing a mandatory request not to tell a health plan can be challenging. A health care provider will have to think how to tag or separate restricted information so that it remains available to those treating patients but does not casually slip off to insurers. Even a provider trying to act in good faith will face challenges. All providers will have to think long and hard how to handle mandatory requests.

For most patients, paying in full out-of-pocket is not realistic. Some patients have the ability to pay and will want to use the mandatory restriction provision. It is generally well known that some individuals receiving mental health treatment are zealously protective of their privacy and will pay for their own treatment. Others will also want treatment to be as confidential as possible. For patients who want to make use of the mandatory restriction in the Rule, we tentatively offer this advice.

1. Recognize up front that getting a mandatory restriction to work will require a lot of advance planning. Find out the covered entity's requirements for a mandatory restriction. Be prepared to make your written request before you make the actual appointment. Come to that appointment with a written request in hand. Have multiple copies of your letter with you. For a large provider, consider talking in advance with the privacy officer to make sure that you can meet the provider's requirements. A larger provider is more likely to have a formal procedure, and you will want to make sure that you do the things necessary to follow that procedure.

2. If the treatment you need normally requires pre-certification from your health plan, you may need to take action well before your appointment. A provider may routinely seek pre-certification on your behalf if you don't make it clear that you do not want the information shared with the insurer. Telling your doctor may not be enough if the clerk who handles the pre-certifications does not know. Work this out well in advance with the provider's administrative staff. Try to talk to the office manager rather than to a receptionist.

3. If you get a referral to a second provider, your request for restriction will not automatically follow with the referral. You have to ask the second provider for a restriction, which may mean doing the same advance work that you did with the first provider. In emergencies, this could prove to be especially difficult or impossible.

4. If you are having an outpatient surgical procedure, it's possible that the same procedure will involve a surgeon, anesthetist, and a hospital, each of which is a separate provider. Your request may have to be made to each provider separately. There may well be other circumstances in which a single type of treatment involves more than one covered entity. You will have to ask a lot of questions to be sure.

5. If your provider orders lab tests or x-rays, your request for restriction will not automatically be transferred with the sample or order. You will have to make the same request for restriction with each subsequent provider (a lab is a provider).

6. You may want to decline to let your provider take a blood sample to send to the lab. Consider getting an order for a test from the doctor. Take the order to a lab, pay in cash, and don't let the lab bill your insurance company. Remember, however, that the cash price may be much higher than the insurance price. If you use a lab that your doctor uses for other tests, your records may end up intermingled and could be disclosed even though you told the lab not to disclose some of the results.

7. Make sure that you can pay for your care. If you don't pay or if your check bounces, a provider may bill your insurance company anyway. If possible, pay for your care at the time of receipt so there is no question about the need to bill your insurer.

8. See if you can arrange for care from a small provider rather than a large provider. A psychiatrist in solo private practice may be much more adept at billing you than a university hospital with many formal procedures, separate billing offices, automated claims submissions, and the like. There's no guarantee that a small provider will do better, but we guess that you have a better chance.

9. Consider having the treatment you want to keep confidential from your health plan at a health care provider that you don't see for other types of treatment. If you establish a relationship with a new provider, make it clear that you will pay for the care yourself, then you may be able to not tell the provider about your insurance at all. Try to avoid even sharing your insurance information if you can.

   Here's an example. Suppose that you usually fill your prescriptions at the "ABC Pharmacy" that has your health plan information on file. It could be easy for a pharmacy to accidentally bill your health plan despite your request. It's also possible that when you fill your next unrestricted prescription, the record of your restricted prescription will go along to the insurer anyway. Avoid the risk, if possible, by filling a restricted prescription at a different pharmacy where you do not do business otherwise. Don't give the second pharmacy your health plan information.

   There's a real downside here, however. There's a risk here that if the new drug conflicts with another drug you already are taking, you could have a serious or fatal reaction. It is important to discuss the issue with the prescribing physician. You could encounter the same type of problem if you receive care from one provider that your regular provider does not know about. You could endanger your health or even your life. It's definitely something to think about.

   Second example: if you need treatment for a sexually transmitted disease and you don't want the information to circulate in the health care payment system, go to a walk-in clinic that takes cash. We can't advise you to use a pseudonym. We don't know that it is legal to do so. However, some people do.

10. If the provider is part of a local Health Information Exchange, keeping your information out of a shared record is something to ask about. You don't have a right to keep PHI from being shared with other providers, but once information is shared, it is more vulnerable to inadvertent disclosure to your

insurer. However, as we just pointed out, it is possible that treatments or drugs from different providers could conflict in some way and endanger your life or your health. There's an advantage when your provider has a more complete medical history. Still, you may want to look for a provider who is not part of a Health Information Exchange.

11. Remember that the mandatory restriction is hard for everyone in the health care system. As should be clear from the above discussion, it raises many complications for patients and for providers. If you happen to be the first person who asks for a mandatory restriction, you may have to work carefully with the provider to work out the proper arrangements. Put another way, you may have to be highly motivated and persistent to have your restriction properly honored.

12. Document everything. Keep copies of your restriction request letters. Try to get receipts for the restriction letters. Keep a log of everyone you talked to in every provider's office and what they said.

13. Don't assume that your doctor will remember that you have a restriction demand on file when you show up for a second, third, or tenth visit. Repeat your demand before every appointment, during each visit, and when you check out of the provider's office. You can't be too careful. In many offices, providers automatically bill insurers after a visit, and they may do so if you don't remind everyone about your restriction demand. The right to restrict the flow of information to an insurer is a firm right, not just a request that a provider can decline to honor. You may have to fight to have your rights honored.

14. Unfortunately, we have not yet exhausted the problems presented by the new disclosure restriction mandate. Here's another possibility. You go to a provider and successfully impose a restriction on disclosure to your health plan. The treatment results in a complication that requires additional treatment, possibly including hospitalization, additional tests, and new prescriptions. If you cannot afford to pay out of pocket for the additional treatment, your health care will begin to receive claims and may ask why the additional treatment is needed. It is also possible that the additional treatment itself will identify to the plan something about the treatment that you kept secret.

    Here's another example. You pay out of pocket for a genetic test to see if you have a gene that predisposes you to colon cancer. The test is positive, and you schedule a colonoscopy that you cannot afford to pay for yourself. Your health plan may ask why it should pay for a colonoscopy for someone of your age when the test is only recommended for someone much older. You may be forced to reveal the test and the result that you wanted to keep secret. All the effort and expense that went into keeping the test from your health plan may

be wasted in that case. One lesson is to think through what you are requesting and what are the possible consequences.

15. Will a restriction demand really make your health record private? Sadly, the answer is no. Don't get your expectations raised too much. The restriction only applies to disclosures to health plans. Other disclosures allowed by the Privacy Rule – to public health agencies, researchers, law enforcement, private litigants, the CIA, and others – are not affected in any way by a patient's restriction. Also unaffected are disclosures to a covered entities business associates, disclosures for health care operations, and disclosures to other health care providers for treatment. Think about that if you want to undertake the efforts to ask for a restriction and make it work. It provides a narrow degree of confidentiality. That may be what you need, but don't expect any more. Only you can decide if the expense and the effort are worth the limited result.

So why did OCR adopt this messy, complicated, nearly-impossible-to implement change in the Privacy Rule? Because Congress directed the change in the HITECH Act. It's a well-intentioned provision, but we have many doubts that it will work well in the real world. If a health care provider does not protect your confidentiality required by law, you can complain to OCR. However, any complaint is only likely to exacerbating sharing of the information that you wanted kept secret in the first place.

54. Is the Right to Limit Disclosures to Relatives and Friends Meaningless Too?

Not entirely. There is a bit of hope if you want a provider to agree to limit disclosures to relatives and friends. If you tell your doctor or nurse not to talk to a relative, that provider is likely to comply regardless of the rule. The rule doesn't make those disclosures mandatory. It does, however, make it harder for a patient to obtain or enforce an agreement.

If, for example, you ask your provider not to disclose your diagnosis to your children, the rule requires the provider to document the request. Since formal documentation is less likely to be done for casual requests, any agreement may be unenforceable under the rule. Further, the required formality of the rule allows providers to insist that patients make requests in writing, and most will demand a letter. If you are a patient in a hospital about to receive a visit from a relative, how can you possibly make a written request and get a timely agreement from the hospital?

Even if you do make a written request, the rule doesn't require any response to your request or any response in a reasonable period. If you are prepared enough to

present a formal request at the start of your hospitalization, the hospital could take 30 days or more before it agreed. Your hospitalization will likely have ended well before any response, if you even get a response.

Luckily, while the rule makes these requests to limit disclosure mostly meaningless, the human element that still exists in the health care system may supply what the rule does not. If you make a personal request to your provider, that provider will likely abide by your wishes regardless of the rule and its required formality. Your request may not be legally enforceable under the HIPAA rule, but enforcement may not be important.

Generally, we don't see much of a reason to bother with formal requests for use and disclosure restrictions, but the decision is yours. If you read many notices of privacy practices, you will find that covered entities say that they won't agree to most requests. That is a polite way of saying that they won't agree to any requests.

If you want to control disclosures to family members or friends, the formal process under the rule isn't likely to help you at all. Make your requests orally and informally to your providers, just the same way that patients have always done. Be clear. Be repetitive. Hope for the best. The HIPAA rule does almost nothing for you.

If you are a movie star, politician, other celebrity, or hospital executive, most hospitals usually fall all over themselves to protect your privacy. They may admit you under a fake name, take other special actions to limit access to and disclosure of your data, and may even agree to your special requests for confidentiality that far exceed legal requirements. Ordinary people are likely to get only basic HIPAA rights, and you may have to fight to get those. If you seek to exercise the right to request restrictions on uses and disclosures, you will almost certainly get little to no help in most cases. Still, if it is important to you, make the effort to ask for what you want.

Part III. What You Should Know about Uses and Disclosures

The HIPAA health privacy rule is long and complex. Implementation guides for use by the covered entities that must comply with the rule can be hundreds of pages. For example, the rule sets out ten administrative requirements for covered entities. They are designation of a privacy officer, privacy training for staff, establishment of safeguards, sanctions for violations, and the like. We are happy that the rule

includes these requirements, but we don't think that you need to know the details. The parts of the rule directly relevant to patients are long enough.

The most important part of the rule – after the provisions that define the rights of a patient – restricts use and disclosure of health information by covered entities. We've already discussed the seven patient rights. (See FAQs 13-54.) The rest of this guide focuses on the use and disclosure provisions.

55. Does HIPAA Really Restrict Use and Disclosure of My Health Records?

This is a tough question to answer in a simple way. The answer depends in part on your perspective. If you thought that your health records would never be disclosed without your consent, then you won't think much of the HIPAA use and disclosure provisions.

Another answer is that HIPAA regulates all uses and disclosures. If the rule does not allow a use or disclosure, then the only way that a covered entity can use or disclose the record is with your written authorization. If you think that sounds good, you should keep reading because the rule allows a large number of uses and disclosures without your consent. By the way, a use of information occurs when a covered entity makes a record available to someone within the organization that maintains the record. A disclosure occurs when a record is shared with someone outside the organization.

Mapping Health has a map that shows data flow within the health care system. Have a look for yourself at (http://www.mappinghealth.com). There another map maintained by Harvard Professor Latanya Sweeney about health sector data flows at (https://thedatamap.org). Both of these maps are works in progress.

A third answer is that HIPAA allows many uses and disclosures to occur without any need for your approval. Typically, these are uses and disclosures made so a covered entity can be paid for services, manage its operations, provide treatment, or comply with government reporting requirements. In most cases, these disclosures are reasonable and expected.

It is genuinely difficult to count the number of categories of permissible uses and disclosures. Much depends on how you do the counting. The number of government and private institutions that can ask for and receive health records without your permission numbers in the tens of thousands. A covered entity can make nearly all permissible uses and disclosures without your consent or authorization. Indeed, with only a few exceptions, a covered entity can make most allowable uses and disclosures even over your express written objection.

A fourth answer is that HIPAA did not really change the practice for most covered entities regarding use and disclosure in any major way. Instead, HIPAA established universal standards and procedures for covered entities. These standards and procedures were new. However, the uses and disclosures that HIPAA allows are largely those that became routine in the last half of the twentieth century. Most health care providers were not aware of how widespread the use and disclosure of health records had become. Before HIPAA, many providers thought that they only disclosed patient records with the consent of the patient, but it just wasn't true. HIPAA made everyone pay attention to and learn about privacy, often for the first time.

The biggest drivers for the sharing of health records are:

- Growth of third party insurance (including Medicare)
- Pressures for increased controls on the cost of health care
- Development of quality controls for medical practice
- Growth of health care fraud and fraud investigations
- Increase in public health activities
- Expansion of records-based health research
- Electronic health records and electronic health networks such as Health Information Exchanges (HIE). For more about HIEs, see WPF's HIE resources at (http://www.worldprivacyforum.org/hie.html).

All of these activities and others contributed to the demand for access to individually identifiable health records. Most of these activities serve important public or personal purposes, and it is not always easy to dismiss the HIPAA rule's policies as anti-privacy. Disclosure often serves another significant but competing goal. Protecting privacy is only one objective in the health care system.

Some health activities can be and are conducted with records that do not include any identifying data about individual patients. However, use of anonymous or non-identifiable records doesn't meet all the needs for health information for several reasons. First, some activities really do require records with identifiers. For research that tracks the course of disease over years, the only way to link records may be with the use of identifiers.

Second, too many activities that could have used non-identifiable records

started at a time when few paid attention to privacy or to alternatives to the use of identifiable records. Methods that might have increased use of non-identifiable records do not always exist because nothing forced their development.

Third, it is increasingly difficult to talk about non-identifiable records. As the amount of data recorded and available throughout society increased, the domain of truly non-identifiable records diminished. It is easier and easier to identify records even though overt identifiers have been removed. To make the point, more than 85% of the population of the United States can be uniquely identified just by date of birth, gender, and five-digit zip code. All records, no matter how they may have been edited or masked, may be potentially identifiable with enough time, effort, and other data. Powerful modern computers make it easier to link records and to re-identify records that have been "de-identified." Even snippets of DNA can sometimes be linked to identifiable individuals, and the ability to link DNA with real people will only expand over time.

Another interesting and important part of the rule tries to limit use and disclosure to the minimum amount of information necessary to accomplish the purpose of the use or disclosure. This is a fine principle, but its implementation is complex and controversial. All uses and disclosures to a health care provider for treatment purposes are exempt from the minimum necessary rule. It's a big exception to the principle, but it is one that makes some sense to us.

Providers need broad access to records for treatment. However, as health records become lifetime records, there may be justification for allowing a patient to control some records some of the time. For example, there may be no need for a physician treating an adult patient for allergies to have access to the patient's record of sexual abuse that occurred decades earlier. The health care system may need to develop tools that allow patients reasonable controls over disclosures for treatment some of the time (and that allow providers to override restrictions if there is a good reason).

Disclosures pursuant to a patient's authorization are also exempt, which is a reason that a patient should be careful when signing any authorization for disclosure of his or her records. If you sign an authorization for the disclosure of "any or all" of your records, your entire medical history can be disclosed.

56. Is My Consent Needed to Disclose Records for Treatment or Payment?

No. Medical records can be used and disclosed without your approval for treatment, payment, and health care operations. Treatment is the providing, management, or coordination of health care by a health care provider. The formal definition is slightly more complicated, but the basic concept is relatively simple.

The definition of payment is more complex. It includes activities by a health plan to determine coverage and provision of benefits and activities by a provider to obtain reimbursement. Payment also includes determining eligibility or coverage, including benefit coordination, cost sharing, adjudication and subrogation (making a third party pay) of benefits. It includes risk adjustment based on enrollee status and characteristics. Patient data may also be used for billing, claims management, collection activities for bad debts, and reinsurance activities.

We are not done with payment. It also includes review for medical necessity and appropriateness of care as well as utilization review, such as pre-certification and preauthorization services. Disclosure to credit bureaus of information relating to collection of premiums or reimbursement is another payment disclosure.

All of those activities, and perhaps a bit more, fall under payment. The breadth of payment activities reflects the complexity of the health care system, the multiple inter-relationships between providers and payors, and the range of insurance activities.

The definition of payment is just a warm up for understanding disclosures for health care operations, another category of disclosure that does not require patient consent. The formal definition goes on for about 400 words. It includes quality assessment, quality improvement, development of clinical guidelines, management and care coordination, review of provider competence, student training, underwriting, premium rating, medical review, legal services, auditing, fraud detection, business planning, business management, customer service, transfer or sale of a business, and fundraising.

We didn't include every type of health care operation here, but you should already get the idea. Further, many of the functions mentioned here are complex tasks that encompass other layers of activities and involve the sharing of health records with people far removed from any activity that the average person would readily identify as part of routine health care management.

One limit on use and disclosure of genetic information is the result of the Genetic Information Nondiscrimination Act of 2008 (GINA). GINA made it illegal to use genetic information for most underwriting purposes. That's good, but it's not much

in the way of health information disclosure restrictions. GINA also generally prohibits most use of genetic information in health insurance and employment. Those are good restrictions too, mostly in furtherance of preventing discrimination against individuals with genetic predispositions. There's much to debate about GINA, but not here. From a narrow privacy perspective, GINA only helps a little.

57. Are Disclosures for Treatment, Payment and Health Care Operations Okay?

At one level, yes. Health care is a complex enterprise that represents a large chunk of America's economy. There are hundreds of thousands of health care providers and probably as many support organizations. Daily transactions measure in the millions. If you think about it, you may realize that major health care treatment and payment institutions are big businesses that engage in a wide variety of activities just like other businesses. Management and internal controls require access to some records. If we spent the time to list the comparable data-intensive activities engaged in by banks or governments, we would also find a long list of uses and disclosures of personal information that are, for better or worse, a routine part of those functions.

At one level, then, treatment, payment and health care operations (TPO) disclosures are routine. Just about all of the functions supported by TPO uses and disclosures went on before HIPAA, although few health professionals paid attention to them. Before HIPAA, if your consent was sought for the sharing of your records for these purposes – and it frequently was not sought – you weren't told any of the specifics. Doctors, hospitals, and insurers typically asked patients to consent to "any and all disclosures" without telling patients what that meant.

Physicians and other providers didn't know themselves how widely patient information was shared.

HIPAA eliminated the need for consent for TPO disclosures. A covered entity may still seek your consent, but this seems to happen rarely. It is easier to rely on the authority provided by the rule to justify use and disclosure. Some privacy advocates see the lack of consent as a great gap in privacy protection because it removes any pretense of patient control over records. We doubt that asking everyone for consent all the time would achieve a better result, and the extra expense and bother would be considerable.

Before HIPAA, many health professionals thought that a patient's health record would be disclosed only with the patient's informed consent. However, what was called informed consent was typically neither informed nor consensual.

You had no idea what the authorization form you were signing meant, and you really didn't have much of a choice. Signing a consent form was a prerequisite to seeing the doctor or having the insurance company pay the bill. Patients – especially those who were ill – are not really able to focus on privacy. Almost everybody signed whatever form they were given without question. If a patient limited or modified an informed consent form, the changes were often not noticed or ignored.

Some experts recognize that it is difficult to expect patients – often people who are sick, impaired, or worried about their children – to be able to understand and control the complex use and disclosures of their records that have become part of health care activities. Would you prefer to be asked for your permission to disclose your records for dozens of different purposes? Could you really make a meaningful choice while suffering from the flu, undergoing chemotherapy, or worried about your nauseous child? Further, there is a limit to how much the health care system can cater to individual preferences. There is a cost involved.

Discussions about the proper role of consent for information use and disclosure in the health care process are ongoing. You are welcome to your side of this debate.

58. Do I Have a Say in Any Disclosures? (Facility Directories and Caregivers)

Yes, but only in a few circumstances.

First, if you are in a facility (e.g., an inpatient in a hospital), the facility can disclose basic information about your presence, location, and general condition through a facility directory. One limitation is that the facility can't reveal information that discloses specific health information about you (e.g., you are an inpatient on the psychiatric floor or are in a kidney dialysis unit).

The idea behind facility directory disclosures is that if someone comes to visit you or sends flowers, the hospital can say that you are there and, perhaps, where you are. The hospital may disclose your religious affiliation, but only to a member of the clergy.

You have a right to object to facility directory disclosures. The covered entity must offer you an opportunity to object to the inclusion of your information in a facility directory. If because of incapacity or emergency treatment, you weren't offered the chance to object, the hospital can make still limited disclosures in emergency

circumstances. For example, if you are unconscious, the emergency room can tell your spouse where you are. That seems perfectly reasonable.

Second, HIPAA has a complex but flexible set of rules governing disclosures to caregivers. A caregiver can be your next of kin, other family member, or another person involved in your care (e.g., a roommate). The HIPAA rule allows disclosure of information relevant to the caregiver's involvement in your care. A covered entity can make a disclosure to locate a family member or other caregiver.

If you (the patient) are present at the time of a disclosure to a caregiver, the covered entity can seek your agreement, offer you an opportunity to object, or reasonably infer from the circumstances that you do not object. Essentially, the rule specifically allows the exercise of professional judgment for the types of disclosures that have long been made to caregivers.

If a patient is not present or is incapacitated at the time of disclosure, the covered entity may exercise professional judgment and make disclosures directly relevant to a caregiver's responsibility, including payment related activities. Thus, the rule allows your spouse to pick up your prescription at the pharmacy without written consent from you or to negotiate with your health plan on your behalf.

A covered entity may also disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. This gives health care providers and health plans the discretion to do what they consider to be the right thing for families of patients recently deceased.

Another provision addresses disclosures for disaster relief purposes. An example is disclosure to the Red Cross following a hurricane. The disaster relief provision, for example, allowed appropriate health disclosures during and after Hurricane Katrina.

Disclosures by health care providers to family members are a routine part of health treatment. Those are some of the disclosures that the rule contemplates. Importantly, the caregiver exception also covers disclosures by insurance plans to family members. That allows a family member to negotiate approval of your treatment or payment of the bill with the insurance company while you are incapacitated.

In general, the caregiver provision seems to have worked well after some initial confusion. The trick is to strike a reasonable balance between privacy and the normal expectations of patients and families. It is a delicate balance, and we think that HIPAA did well here. Giving considerable discretion to health

professionals had a lot to do with the success of this provision.

Third, a covered entity can use or disclose information for its own fundraising purposes. A covered entity can use or disclose to a business associate or related foundation your name, address, other contact information, age, gender, and date of birth. In addition, it may use or disclose information about dates of care, department of service, treating physician, outcome information, and health insurance status. No other PHI may be used for fund-raising. This means that a hospital can now tell a fundraiser that you were treated by the oncology or psychiatry department. That is a bit much, if you ask us.

You can opt-out of fundraising requests. If a covered entity intends to use PHI for fundraising, it must include a statement about its intentions in its notice of privacy practices. In addition, each fundraising communication must include a clear and conspicuous opportunity to opt-out of future fundraising communications, and the opt-out method cannot impose an undue burden or more than a nominal cost. Making you write a letter to opt-out is not allowed, however. Further, a covered entity may not condition treatment or payment on the individual's choice about fundraising communications.

Fourth, you have the right to authorize the disclosure of your health records to anyone you like. The HIPAA rule sets standards for authorization forms, and if a form does not meet HIPAA standards, then the form does not constitute patient authorization. We are not going to bore you with the technical requirements for authorization forms. We discuss the strategy for authorizations later. (See FAQs 64-66.) Anyone who wants you to authorize a disclosure or is a covered entity will know the technical requirements. This isn't typically a problem that patients have to solve.

The rule uses both consent and authorization as terms that apply when a patient gives approval for the disclosure of a health record. Consent is the term that applies when a patient gives an organization permission to disclosure for treatment, payment, and health care operations. Authorization is the term that applies to all other disclosures approved by a patient. The reason for the difference in terminology is buried in the history of the rule, and it is too boring to explain. Normally, patients will encounter the term authorization.

When might a patient authorize disclosure? You might authorize disclosure if you are applying for life or disability insurance. You might authorize your doctor to send information to your employer or to a school to explain an absence. You could authorize your doctor to disclose your records to your lawyer, a family member, or a health researcher. You might want records disclosed to support a disability claim made with the Social Security Administration.

It is also possible that you might even want to share your records with the police under some circumstances (perhaps to clear you of suspicion). You might want to authorize a provider to give records to the organization maintaining your personal health record (but we think you should think twice before casually establishing a personal health record. For more on PHRs, see the World Privacy Forum report *Personal Health Records: Why Many PHRs Threaten Privacy* at https://www.worldprivacyforum.org/2008/02/blog-legal-and-policy-analysis-personal-health-records-why-many-phrs-threaten-privacy/).

For the most part, however, HIPAA defines the range of non-consensual uses and disclosures to include nearly every possible disclosure that is either necessary or convenient for the health care system to operate or for the government to carry out its many functions. After all, the HIPAA rule was written by the Department of Health and Human Services, one of the biggest users of health records in the country. The first thing that HHS did in writing the rule was to take care of its own interests in obtaining access to records.

59. Does HIPAA Allow Uses and Disclosures Without My Approval?

Yes, does it ever. The HIPAA rule allows dozens of different uses and disclosures without any need for patient consent or authorization. The rule permits so many uses and disclosures that it is hard to count them. The rule has about five pages of dense type describing allowable uses and disclosures of health records.

Many of HIPAA's allowable uses and disclosures come with terms, conditions, and procedures that the covered entity or the person seeking the information must meet. A simple list of authorized recipients or recognized purposes doesn't necessarily tell you that much.

The terms, conditions, and procedures make a big difference to the scope and ease of disclosures. We won't cover all of the details here because of the complexity. The details are crucial important if you are a covered entity concerned about when it is permissible to make a disclosure.

A patient may need to know the details when trying to decide after the fact if a covered entity made a disclosure properly. However, a patient with that requirement will have to look elsewhere for the specifics. We can't cover every detail here.

One important feature of the rule's allowable uses and disclosures is that they are mostly permissive. Just because a use or disclosure can be made without violating the rule does not mean that a covered entity must make the disclosure. A covered entity can just say no to almost any person who asks for a disclosure permitted by the rule. This means that the rule itself is not the most important factor in determining how your record may be used or disclosed. In most cases, it is up to your health care provider or insurer to decide whether to make your record available for a particular activity. If anyone tells you that HIPAA requires a disclosure, you should be suspicious.

The only two types of disclosure that the rule actually **requires** are:

1) When a patient asks for access to his or her own record, and

2) When the Secretary of HHS needs access to records to oversee or enforce the HIPAA rule itself. For all other uses and disclosures, it is up to the covered entity to decide whether the use or disclosure is appropriate, legal, and ethical. Of course, other laws may affect that decision, and many laws require disclosure of health records.

We also want to remind you that the HIPAA rule establishes a floor of privacy protection. If state law or other federal law has higher standards and better privacy protections, then that law controls. If HIPAA allows a disclosure that is prohibited by law in your state, a covered entity in your state may not make the disclosure.

We will go over one type of allowable use and disclosure in detail to give you better insight into the complexity of use and disclosure. We will then provide general information on the other permissible uses and disclosures.

60. What Are Uses and Disclosures Required by Law?

We want to discuss the category of uses and disclosures required by law. If you read privacy policies, you may see this term a lot. For purposes of this discussion, we will focus on disclosures rather than uses. HIPAA recognizes that other laws sometimes

require the disclosure of health records. In one of the shortest sections dealing with disclosure, HIPAA says that a covered entity can make a disclosure that is required by law.

What does this mean? It means that any federal, state, or local law requiring disclosure of health records remains in force. (A law means a statute or a regulation.) For example, when a state law requires a physician to report a suspected case of child abuse to a state agency, the HIPAA rule does not interfere with that disclosure (although it establishes some conditions on that particular disclosure). If a city passes an ordinance that says that the entire health record of any individual hospitalized in a local hospital must be published in full in the local newspaper, HIPAA would permit that disclosure too.

We do not expect to see laws requiring the publishing of records of patient records any time soon. We just want to point out the breadth of the HIPAA deference to other laws. Any law, no matter what its purpose or scope, that requires disclosure is sufficient for HIPAA's purposes. If another law says disclose, then HIPAA says disclosure is permissible but only to the extent of the requirements of the other law. Any compulsion about disclosure comes from that other law and not from HIPAA, however.

For some disclosures allowed by HIPAA, the rule provides that the procedures established by HIPAA continue to apply to covered entities even when disclosures are made under the authority of other laws. This is a complicated area, and you may want to skip the rest of this paragraph. For example, HIPAA allows disclosures to report suspected cases of abuse, neglect, or domestic violence to the proper authorities. Most or all states have comparable laws. HIPAA includes a set of procedures that a covered entity must comply with before or after making a disclosure of abuse, neglect, or domestic violence. Under some specified circumstances, the covered entity making the disclosure must inform the subject of the disclosure (i.e., the victim) about the disclosure. However, the rule specifies that in some circumstances, notifying the victim will place the victim in greater peril so telling the victim is not always required. The HIPAA rule says that if state law mandates disclosure about abuse, the covered entity making the disclosure must still comply with the HIPAA procedures. HIPAA also imposes additional duties for disclosures for judicial and administrative proceedings and for disclosures for law enforcement purposes.

However, for other allowable disclosures, none of the conditions in HIPAA applies if another law requires disclosure. For example, the HIPAA rule allows disclosures for health research under a lengthy set of conditions. If a covered entity wants to make a disclosure for research, it must comply with all of the HIPAA conditions. However, if a state law requires disclosure for health research with fewer or no conditions, then HIPAA says that the disclosure can be made without complying with all of HIPAA's conditions.

This is complicated stuff, and we haven't covered all the nuances. The covered entities that make disclosures need to pay close attention to the details. The message for patients is that many laws affect the confidentiality of health records. If you thought that no one disclosed your health records without your approval, keep reading to see how wrong you were.

61. What Are the Allowable Uses and Disclosures?

We list each HIPAA category of allowable use and disclosure, together with some discussion as appropriate. (If we included every detail of every disclosure, it would double the size of this guide.) A covered entity that must comply with the HIPAA rule needs to know all the specifics, but an informed patient generally only needs to be generally aware of the categories of uses and disclosures. Every covered entity's notice of privacy practices should include some information about each type of allowable disclosure. Those who want to know more can read the rule itself.

- **Treatment, Payment, and Health Care Operations**. We covered this category of uses and disclosures in detail in an earlier question. (See FAQ 57.) The category includes uses and disclosures for a very large number of purposes.

- **Required by law**. We've already covered this category in detail in the previous question. We used this category to illustrate the complexity of allowable disclosures.

- **Public Health Activities**. Public health disclosures are one of the more expansive disclosure categories under the rule. There are at least five general types of public health disclosures. Some public health disclosures are to traditional federal, state, and local public health agencies. The reporting of communicable diseases is an example. It is the type of disclosure that draws few, if any, objections. Additional confidentiality protections may apply to some of the information disclosed to public health agencies. Disclosures to manufacturers of pharmaceutical medicines and devices for the reporting of adverse events may qualify as public health disclosures. Some public health disclosures can be to employers for medical surveillance of the workplace. These disclosures to private entities explain why the public health category so expansive. Many different organizations play a role in public health, including employers.

- **Immunizations**. A covered entity can disclose proof of immunization to a school where an individual is a student or prospective student, if the school is required by law to have proof of immunization before admitting a student and the covered entity obtains and documents agreement to disclose from a

parent or guardian or from an adult student. The agreement does not have to be in writing.

- **Victims of Abuse, Neglect, or Domestic Violence**. Reporting of victims can be done to a social service agency or other government authority (including the police) that is authorized to receive the reports.

- **Health Oversight Activities**. Many federal and state government agencies regulate and oversee parts of the health care system. Disclosures are permissible for activities authorized (not just required!) by law, including audits, investigations, inspections, licensing, and similar functions. One patient protection included in the rule prevents the use of information disclosed for oversight purposes against the patient who is the subject of the record disclosed. So if an agency investigates a health care provider, it cannot use information about that provider's patients against the patients themselves. However, if the information reveals health care fraud by the patient or involving public benefits for health care or benefits based on health condition, the information can be used against the patient. The protection for patients with oversight disclosures is limited, but it has some substance.

- **Judicial and Administrative Proceedings.** A covered entity can respond to a court order or the order of an administrative agency for health records. The authority to disclose also covers subpoenas and discovery requests. The conditions that attach to these disclosures are lengthy and include some obligation to give notice to the patient who is the subject of the record. The complexity here is enough to choke a lawyer because the HIPAA rule interacts with already elaborate state laws and court procedures.

- **Law Enforcement Purposes**. The rule has six flavors of law enforcement disclosure. The loosest allows disclosures for "administrative" requests. An administrative request does not require judicial approval or even have to be in writing. Any law enforcement official can ask for information by stating that the information sought is relevant to a legitimate law enforcement inquiry, by limiting the request to information reasonably practicable to the purpose, and by saying that de-identified information cannot be used. It is hard to imagine a more unrestricted type of police disclosure. A covered entity need not comply with an administrative request, but it may do so. The other types of law enforcement disclosures are not so open-ended. One, for example, allows a provider to report a crime that occurred in the provider's office. That seems more reasonable.

- **Decedents**. A covered entity can share information about people who died with coroners and funeral directors. They may need to know if a decedent had AIDS, for example.

- **Organ and Tissue Donation**. A covered entity can disclose patient information to organizations engaged in tissue banking and transplantation to facilitate donations.

- **Research**. Researchers engaged in health research and other types of research often want access to health records. The rule allows disclosures for research but generally requires that a research project be approved by an Institutional Review Board (IRB). An IRB is an existing institution – often part of the organization conducting the research – that oversees research activities to protect human subjects. The research section of HIPAA is particularly convoluted in order to address different needs of researchers. We observe that HHS itself conducts and funds research using health records. The rule reflects the needs of HHS and researchers, while offering some procedural protections for privacy. There are many policy conflicts involving research disclosures, and the rule strikes balances that some like and some don't.

- **Serious Threats to Health or Safety**. A covered entity may use or disclose a patient record if it believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. There are a few other conditions.

- **Specialized Government Functions**. This category of uses and disclosures has six subcategories. Some relate to military, veterans, and prison functions. Another category allows disclosure to the Secret Service to protect the President and some other officials. Another broad subcategory allows disclosure to government programs providing public benefits.

- The broadest provisions in the government functions subcategory authorize disclosure to any national security or intelligence agency. HIPAA imposes no conditions or procedures for national security disclosures. The disclosures are not mandatory (at least not under HIPAA), but any national security or intelligence agency can request a health record on any individual without prerequisite and without violating HIPAA, even if the disclosure would violate medical ethics. We think this is the single worst provision in the HIPAA Privacy Rule.

- **Worker's Compensation**. HIPAA allows any disclosure authorized and necessary to comply with laws relating to worker's compensation. The worker's compensation system typically requires the routine disclosure of health information about injured workers. HIPAA stays out of the way and allows the normal processes to continue without any procedural or substantive interference.

We remind you once again that nearly all HIPAA disclosures are permissive and not mandatory. While many records are heavily used and disclosed for treatment, payment, and health care operations, many of the other permissible disclosures are likely to be relatively unusual. Just because records can be disclosed to the Central Intelligence Agency under the national security category doesn't mean that the CIA really looks at everyone's health records routinely.

62. Can a Mental Health Care Provider Disclose Health Information to Parents of College Students?

Recent violent events on college campuses and elsewhere resulted in concerns that privacy rules may affect how mental health care providers can share information. The specific concern is privacy rules create confusion about the ability of metal health care providers for adults (including college students) to communicate with parents or other potential caregivers of a patient. In the 21st Century Cures Act, Congress made a specific finding about the existence of confusion and the consequences of the confusion. Act of December 13, 2016, Public law 114-255, Section 11001(a)(9). The text of the Act appears at (https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf).

In the 21st Century Cures Act, Congress also directed the Secretary of HHS to issue guidance clarifying uses and disclosures permissible under HIPAA. The law does not suggest that there is a need for a change in the privacy rule. HIPAA provides several methods for disclosure by covered entities to caregivers of information about individuals with mental health problems. The direction to the Secretary identifies the types of uses and disclosures that Congress thinks would clarify the situation.

Permissible disclosures about an individual patient receiving or needing mental health care can be made: 1) with the consent of the patient; 2) if the patient had an opportunity to object; 3) based on the exercise of professional judgment whether the patient would object if an opportunity to object is not possible because of incapacity or emergency treatment; or 4) based on the exercise of professional judgment to be in the best interest of the patient when the patient is not present or is otherwise incapacitated. Elsewhere, this guide explains all of these types of disclosures. However, it is not possible in this FAQ to address these disclosures in great detail. Much depends on individual circumstances, specific facts, and professional judgment. Presumably, the forthcoming guidance from HHS will provide greater clarity.

This issue is difficult because of the need to balance interventions and privacy in an effective way. Congress considered different approaches, including a substantive change in the rules. In the end, Congress settled on asking for better guidance rather than a new rule. Existing HHS guidance on mental health data sharing is at (https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html?language=es).

63. What Happens to Privacy When Adult Children Are Covered by their Parent's Health Insurance? Will information of an adult child be disclosed to the parent?

Under some circumstances, adult children may have health coverage under an insurance policy of their parents. For example, some policies may cover adult children who are college students. Can the policy holder (parent) obtain health information about an adult child?

This is a messy area, with different types of answers. If the parent is a recognized caregiver of the adult child, then standard HIPAA rules allow a health care provider to share information. This is the rule whether or not the adult child is covered by the parent's insurance. Any patient can prevent these disclosures, however, by telling the provider.

A standard HIPAA rule also allows disclosure to avert a serious and imminent threat to health or safety. This provision isn't likely to apply very often, but it allows disclosure to anyone who can prevent or lessen the threat, parent or otherwise.

In other circumstances where the adult child may not want to let a parent know about the adult child's health condition, things are more complicated. Rules and rights are slightly different for health plans (insurers) than for health care providers. Insurers usually send bills and EOBs (Explanation of Benefits) to the individual who has the policy. When a parent's policy covers an adult child, those notices may go to the parent unless the adult child takes action to stop it.

HIPAA says that any individual can ask that a health plan communicate with them at a different location or using a different method than normal. Any covered entity must comply with a request if the individual says that the routine communication method would endanger the individual. Part II C of this guide explains how to make this type of request. Remember that we think that it is up to each individual to decide what is a danger to them, but whether you can convince the insurer of this is uncertain. If it is important to you, it's worth trying. Even if you make the request and the insurer agrees, it may not work since some communications may end up

with the parent who is the policy holder normally. Still, insurers may be more sensitive to this problem today than in the past.

In the end, the existing HIPAA rule does not meaningfully address this problem, and using any of these methods can be chancy and incomplete. Some state laws may offer some better protections, but it may vary by state and type of treatment.

What to do? An adult child should make the problem known to their providers and, especially, to their health insurer. Make a request even when HIPAA doesn't give a formal right. Talk to the insurer's privacy officer, if possible. Some covered entities may respond positively to a request even if not required by HIPAA. Another possibility is to pay cash for some services, an option not available to everyone for every type of treatment.

64. What Should I Do if Asked to Sign an Authorization to Disclose my Record?

Although not everyone who asks you to sign an authorization will have a sinister motive, you should be cautious in signing an authorization for more disclosure of your information. Here are some things to look out for:

- **Disclosures**: Does the authorization say that all of your information can be disclosed? If you authorize disclosure to a physician who is treating you, a broad authorization may be appropriate. If you authorize disclosure to a life insurance company, the company will likely insist on a broad authorization as part of the application process. However, if the authorization is for disclosure to your employer to explain your absence from work, you may want to be sure that the authorization only covers your recent illness and not records from the past. You may not want your employer to know, for example, about treated for a psychiatric ailment ten years ago.

- **Expiration date**: Is there an expiration date or event for the authorization? There should be in nearly all cases. You should try to understand why the date or event was chosen and be suspicious of any open-ended authorizations. Some long-term research activities may be able to justify not having an expiration date. Otherwise, you should try to insist on a short expiration date or near-term expiration event.

- **Proper description of recipient:** Is the person authorized to receive the information properly described? It is okay if the form says ABC Life Insurance Company rather than the name of a specific individual at the company. However, if the form is too vague (e.g., "bearer"), then you should definitely think twice.

- **Purpose of disclosure description**: Is the purpose for the disclosure properly described? If you tell the covered entity why you are authorizing the disclosure, you may reveal information that you don't want to reveal and don't have to share. It is okay to sign a form that merely describes the purpose as "at the request of the individual." However, we wouldn't normally sign an authorization written that way without a good reason and then only if we trusted the recipient. By stating a purpose, you may limit what the recipient can do with the information. Anyone seeking an authorization in good faith should be willing to include an appropriate purpose and, if someone does not suggest a narrow purpose, you should be wary. This can be a bit tricky when you authorize disclosure to a lawyer for a malpractice suit against a provider.

- **Marketing**: Is the authorization for a marketing activity? We would never sign a disclosure for a marketing purpose, no matter what the inducement. Once a marketer obtains your information, the marketer can use it, keep it, and sell it without any restriction for the rest of your life. Don't give away your health privacy for a chance to win a t-shirt. The Rule allows prescription refill reminders even though they are marketing, but it imposes a limit on how much a provider can be paid for sending a reminder.

- **Financial remuneration**: Generally, a covered entity needs your authorization if someone pays ("financial remuneration") the entity for the use of your information for a marketing purpose. That's good, but limiting the sale of PHI made for a complicated rule because there are some times when it's okay if a provider receives payment for disclosing PHI. For example, a health researcher may pay a hospital for the cost of providing records for the research project. The Rule explains this, but we won't because it's not relevant to most patients.

- **Research**: Is the authorization for a research project? Read it carefully because a 2013 rule change allows research authorizations to be more expansive. The same authorization can cover the project itself and the storage of a blood, data, or tissue sample about you forever. You may or may not be comfortable with that. We encourage you to ask lots of questions about research and researchers. Not all researchers are truly trustworthy.

We emphasize that while we think that you should be cautious in signing authorizations, in some circumstances it is the right thing to do. Signing an authorization should happen infrequently enough that you can spend a little time asking questions.

Be cautious if asked to sign an authorization as part of the process for admission to a hospital. The HIPAA rule allows the hospital to make all the disclosure necessary for your care and for the hospital's operations. Ask questions first if you are presented

with an authorization to sign. Some hospitals routinely collect authorizations that allow disclosures to employers. Some standard authorizations allow the hospital to film your operation or use your blood or tissue samples for purposes unrelated to treatment.

These are examples of disclosure that you may not want to permit without a specific reason. The hospital may seek a broad authorization for its own convenience so that it can make a disclosure without getting your signature later. We suggest that any extra paperwork may be worth it, because it may protect you. You can decline to sign the authorization or you can limit its effectiveness to the period while you are in the hospital or perhaps for an additional week. If asked to sign an authorization that has language we didn't like, we would just cross it out.

The HIPAA rule expressly provides that no one can condition treatment, payment, or enrollment in a health plan on signing an authorization. This is an important protection, and if any provider says "sign or leave", you should be extremely suspicious and ask for a written explanation that you can take with you. There is a limited exception to this policy if you are enrolling in a research activity involving treatment. Another exception allows a health plan to require an authorization for an individually underwritten health policy. There is one other complex but minor exception to the rule.

What happens when I authorize disclosure to a non-HIPAA-covered entity?

We told you earlier that HIPAA protections do not follow the records. When your records are transferred to someone who is not a covered entity, the records in the possession of the recipient are not covered by HIPAA. That is also true for most disclosures with your authorization.

If you agree to allow a covered entity to share your records with someone who is not a HIPAA-covered entity, no privacy law may apply to the recipient.

If you authorize a company that engages in advertising-supported activity (such as a personal health record or PHR) to obtain your records, it is possible that the recipient could use your information for marketing and share it with almost anyone.

Any privacy protections would depend on the recipient's policy. If you read the privacy policy at most advertising-supported personal health record companies (and many other websites as well), we bet it says expressly that the privacy policy can be changed at any time. You have been warned!

65. Do I Need a Disclosure Authorization to Care For My Elderly Parent?

Maybe. If you help a parent, other relative, or even an unrelated friend or neighbor, HIPAA allows a provider to disclose to a person involved in a patient's care. These people are sometimes called caregivers, and the rule governing caregivers is discussed elsewhere. (See FAQ 58.)

While the HIPAA caregiver policy usually works well, it may be useful to have a written authorization from the patient. This is good advice especially if you will be caring for someone for a long time, if there are many health care providers involved, or if you expect to have to deal with an insurance company or Medicare. Don't give away your original authorization. Keep copies because you may need them regularly. If you care for someone at a hospital or nursing home, bring a copy with you at all times. The nurse who knows you may not be there tomorrow.

If you obtain a health care power of attorney for another person, the power should specifically mention the authority to obtain protected health information about that person. Protected health information is the formal HIPAA term for a health record. You can obtain a power of attorney for a patient just for HIPAA disclosure purposes without having the authority to make substantive health decisions about the patient.

If you sign or receive a broad health care power of attorney that authorizes someone to make substantive health decisions, that same power of attorney should also authorize disclosures to support those decisions.

We think it is a good idea to have a signed disclosure authorization for any family member (other than a dependent child) if you have some responsibility for his or her care. The more remote the relationship, the more important an authorization may be, especially if a hospitalization occurs. The same is true if you are responsible for a neighbor or friend. Ask the hospital for a blank form that it will accept. Plan to obtain the signed authorization in advance of the hospitalization if possible

66. What Can I Do if I Foolishly Signed an Authorization?

You can revoke the authorization, but you have to do it in writing. Your ability to revoke an authorization is restricted if a covered entity took action in reliance on the authorization or if the authorization was a condition of obtaining insurance coverage.

Remember that revoking an authorization may not be enough. The covered entity that you authorized to disclose your records must receive a copy of your revocation. If a third party obtained the authorization, you should make sure that the third party receives a copy of the revocation. If a third party obtained the authorization for your records from a specific hospital, formally notifying the hospital in writing that you revoked the authorization is also important.

67. Can My Health Records be Used for Marketing?

The short answer is no, but the correct and longer answer is more complicated. Let's go through it step by step.

The HIPAA rule tells covered entities that they can only use or disclose health records for marketing with the authorization of the patient. One reason for being careful when signing an authorization is to make sure that you don't casually authorize disclosure of your records to a company that wants to use them for marketing.

Other activities can reveal your medical history. If you accept a drug manufacturer's coupon for a prescription drug, the manufacturer will learn your name and other information that it didn't have before. Drug manufacturers are not covered entities or generally subject to health privacy laws. Signing up for a disease-specific

newsletter also reveals your name and health information. Joining a disease support group also effectively shares health information about you or a family member. If you give your email address to sign into a disease specific website, the website operator knows what you are interested in and how to spam you.

If you chat on a health care provider's Facebook page (or on your Facebook page) openly about your condition (or your child's), you effectively reveal health information. HIPAA doesn't protect any information you post on a social network. If you provide health information in response to a "survey" that promises to provide you with coupons, that information will go straight to a marketer's database. If you use a Fitbit or other fitness tracker and you give you data to the company, the data is not subject to HIPAA, only to that company's privacy policy. Most gyms are not HIPAA-covered entities, so data shared with a gym falls outside HIPAA and has no statutory privacy protections.

HIPAA has two exceptions that allow marketing uses and disclosures. The first permits face-to-face communications by a covered entity to a patient. The second allows promotional gifts of nominal value provided by the covered entity. Under the first exception, for example, a nurse can invite you to visit the hospital's new weight loss clinic. Under the second, the hospital can give you a refrigerator magnet with the phone number of its well-baby clinic. If the covered entity undertakes any marketing activity because someone, such as an outside company, pays it to do so, then the covered entity must tell you it is being paid.

The Rule also allows prescription refill reminders, but it imposes a limit on how much a provider can be paid for sending a reminder. If you don't like refill reminders, you may be able to opt-out of them. A pharmacy can send you a letter telling you to refill an existing prescription, but the Rule does not allow so-called switch letters. A switch letter tries to get you to use a different drug than the one you were originally prescribed.

The basic marketing rule is pretty good as far as it goes. Most doctors believe, and will tell you, that using – and especially disclosing – health records for marketing is unethical anyway. That's fine, but in many instances, doctors practice in group settings where the doctors don't control all uses and disclosures of health records.

So far, so good. The rule allows uses and disclosures for treatment purposes and for health care operations. When does a treatment recommendation constitute marketing? The line can be hard to draw. Advice from HHS says that any communication for the patient's treatment, case management, care coordination, or recommendation of alternative therapies is permitted to the extent reasonably necessary. Further, population-based activities for health education or disease prevention ("Don't Smoke!") can also be okay.

The problem in line drawing here is that legitimate health activities overlap at the edges with marketing activities that many people are likely to find objectionable.

Activities that fall on those edges can be characterized differently. Some activities that fall under the broad (and permissible) category of health care operations will look like marketing to some. When the answer requires a lawyer to dissect words, the result will be controversial at best.

The HIPAA rule helps a bit in limiting marketing disclosures. For example, because of HIPAA, you can expect that no covered entity will sell or rent lists of patients to drug manufacturers for the purposes of sending spam or junk mail. However, there may be other forms of marketing-like activities that a covered entity's lawyer may say is allowed under HIPAA.

We are not done yet, but we need more context to continue. If you receive mail hawking allergy medicines or medical devices for diabetics, does that mean that your allergist or internist or insurer or pharmacist gave your name and diagnosis to the advertiser? Anything is possible, but there are other, more likely, sources of the same information.

Marketing companies and data brokers sell or rent mailing lists of people by diagnosis. They offer lists of millions of people by dozens of different diseases and conditions. Where does the information come from? The answer is from many places, but you are the most likely source. If you show interest in a medical product by making a purchase, calling an 800 number, registering at a website, using a coded coupon, subscribing to a magazine, filling out a quiz, or entering a sweepstakes, you may reveal your interest and your diagnosis. If you fill out a warranty card or a consumer survey, any information about your health condition ("Why did you buy the vaporizer?") that you reveal is likely to end up in a personal or household profile and can used and sold forever for marketing purposes.

Websites that show ads and the advertisers often collect information about you, what you see online, and what you click on. That can all reveal health information not protected by law. Those who read carefully already saw our warning about turning your health records over to a commercial, advertising-supported company offering personal health record (PHR) services. (See FAQ 9.) That's another way your records can leak into the marketing system. Any slip puts your personal information in the permanent possession of list brokers, marketers and profilers.

We almost never fill out warranty cards. You have the same warranty protections whether or not you fill out the card. The main purpose of warranty cards is for the manufacturer of a product to learn information about its customers that it can use or sell for marketing purposes. We do not fill out warranty cards even if the manufacturer promises a one-in-a-zillion chance of winning a prize. If we had a good reason to fill out a warranty card, we wouldn't give all the information requested or we might lie.

We need to remind you again that HIPAA does not protect all health information. It only applies to health information held by a covered entity (health care provider or insurer). If you give health information to a product manufacturer, it's not likely to be protected by any privacy law.

Over-the-counter medications and HIPAA

Be careful when buying over-the-counter medications on the Internet or using frequent shopping cards from drug stores or pharmacies. The information about your purchase is not protected under HIPAA because the rule only covers prescription drugs.

If the merchant is not a covered entity, then HIPAA does not stop it from recording your name and purchase and selling that information to others for marketing purposes. Here's the same advice that makes the point more succinctly: Never buy a tube of Preparation H using a frequent shopper card.

A chain drug store or supermarket is only a covered entity for the pharmacy in the back of the store. Anything that merchant knows about you other than prescription drug purchases will not be protected under HIPAA.

The final answer about marketing is that HIPAA mostly does the right thing when it comes to marketing uses and disclosures of health information. However, there are gaps at the edges. Beyond HIPAA, there are non-regulated sources of health information about many Americans. For many organizations with health information, the pressure to exploit health data for marketing purposes is great. That pressure is even greater on the Internet.

Many health care companies are for-profit organizations, accountable to their shareholders. We generally trust individual doctors to do the right thing here, but we don't necessarily trust large institutions. We worry especially that information maintained by non-HIPAA entities in Personal Health Records will leak into the marketing system. We remain cautious and observant about marketing. Once a marketer gets your health information, that information is "in the wild" and the marketer has that information forever. The information may be used during your lifetime and the lifetime of your children.

68. What Does the Breach Notice I Received Mean?

Let's start with the basics. What's a breach? A breach is impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The full definition of what is and is not a breach is too complicated for this FAQ. In general, if a covered entity has a qualifying breach, it will send you a notice to let you know. The notice will include details about the breach and advice about what you should do to protect yourself.

A breach can lead to negative consequences for you, but we don't want you to overreact. Yes, you could become a victim of identity theft, either financial identity theft or medical identity theft. Yes, you are at greater risk because of the breach. Do not panic.

We cannot assess the probabilities, but not every breach results in consequences for the victims of the breach. If a covered entity offers you free credit monitoring, you may want to accept it. If the breach included disclosure of your credit card number or your health insurance number, you may want to pay even closer attention to credit card bills or explanation of benefits. Frankly, you should pay close attention to these anyway. You should always make sure that all charges to your credit card are correct, and you should follow up if any are not. Same with explanations of benefits from a health insurer. If it doesn't look right, call the insurer or provider and ask questions.

We do not advise paying for identity theft insurance or even buying credit monitoring unless you have a specific reason for doing so. Identity theft insurance is rarely worth the cost.

You can learn more about medical identity theft at the World Privacy Forum website at (https://www.worldprivacyforum.org/category/med-id-theft/). There are lots of resources and advice. For more on financial identity theft, go the Identity Theft Resource Center at (http://idtheftcenter.com/).