11 Myths About HIPAA and Medical Records Privacy for Patients

By Trisha Torrey Fact checked by Dale Brauner on February 24, 2020

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress and signed into law by President Bill Clinton in 1996. It was originally intended to protect a patient's access to insurance. Later, security policies were added to cover the electronic sharing of medical records. Despite the fact that these rules have been in effect for more than two decades, there is still confusion over their application.

HIPAA calls those records "protected health information." It sets forth policies and standards for how patient information, including doctors' notes, medical test results, lab reports, and billing information may be shared.

Providers fear the fines they will be forced to pay if they share the information with someone or some entity outside the rules, so they often over-protect patient information.

Patients get frustrated trying to gain information for themselves and loved ones, some of whom are excluded from obtaining access without written permission from the patient. Patients are often surprised to learn just who is allowed by law to access their records.

Payers, the government, sometimes employers, and many others have access to medical records.

You can be an empowered patient or advocate by knowing the basics of HIPAA and having the confidence to request records from providers. Here are some myths about HIPAA and how they affect you, the patient.

1. **Myth: HIPAA Prevents Sharing of Information with Family Members**

With specific permissions from you, in writing, records can be shared with anyone you designate.

2. **Myth: Only Patients or Caregivers May Get Copies of Health Records**

This is also false. In fact, there are many other individuals and organizations that can access a patient's medical records without a patient's permission, some legally and some illegally.

Personal medical information can be obtained by anyone who helps you pay for your healthcare, from insurance to the government to your employer.

It can also be obtained by anyone who wants to buy it, although it may be aggregated and de-identified when it's purchased.

And sometimes it's either stolen or given away by mistake.

3. **Myth: Employers Are Payers and Can Gain Access to an Employee's Records**

In most cases, HIPAA prohibits employers from accessing a patient's records, regardless of the fact that they are paying for care. This applies whether the employer participates in an outside insurance plan, or is self-insured.

If the employer wants access to your records, you must supply your permission, in writing, for her to do so. There are some exceptions to the rule, especially for self-insured employers.

4. **Myth: HIPAA Laws Prevent Doctors from Exchanging Email With Their Patients**

Not true, even if your doctor told you it's true. It's possible your provider will use HIPAA as an excuse, but HIPAA does not prohibit the use of email between doctors and patients.

HIPAA requires only that health information is safeguarded, and the regular email that we use every day is not safeguarded at all.

There are programs that exist to ensure email is safeguarded. For example, some email programs will "encrypt" an email before it travels through the internet, turning it into unreadable code until someone who has the key to unlock the code receives it. Others set up systems that alert their patients that a message is waiting for them on the doctor's secure server. In both cases, all the information patients need to be able to read a secured email from their doctor is provided ahead of time.

However, for too many providers, and like with other aspects of this set of laws, email security requirements may be more than they want to handle, and they may use HIPAA as an excuse to not exchange email with you.

5. **Myth: Providers Are Required by Law to Provide All Medical Records to You**

In fact, some records may be withheld and not provided to you.

If you request records that the provider or facility deems may be harmful to you, they may deny you access. These records are often mental health records. They cannot be withheld just because the provider believes they will upset you. But you can be denied if the provider thinks you will do harm to yourself because of their outcome.

If you have requested your records, but they have not been provided to you, it may be because you did not follow that provider's required steps in order to get copies of your medical records. If you have followed those steps and still cannot get those copies, then in most states, the provider must notify you in writing, within a specified amount of time, that you won't be receiving them.

6. **Myth: Patients Denied Access to Their Records May Sue to Get Copies**

There are remedies for patients who are denied copies of their medical records, but a lawsuit is not one of them.

The U.S. Department of Health & Human Services (HHS) provides a procedure patients may follow if they believe their rights have been violated under HIPAA laws. It includes filing a formal complaint through an online process.

If the violation is heinous enough, the HHS, or even the Department of Justice, may invoke a penalty to the violating entity, ranging from a $100-50,000 fine for each violation to 10 years in jail and a $250,000 fine, and even reach a maximum of $1.5 million for identical provisions during a calendar year.

7. **Myth: HIPAA Laws Cover Privacy and Security for All Medical Records**

This is partially true, but only under certain circumstances.

Healthcare providers, healthcare facilities, and sometimes insurers are the only entities bound by HIPAA.

But there are many others who may have that information, and they are not obligated or regulated by HIPAA. In the past few years, dozens of web applications have become available, many for free, that

invite patients to upload their own health and medical information, usually for storage purposes. They claim that these PHRs (personal health records) become convenient and available in an emergency when stored in this manner. And so it would seem they are.

But these organizations are not under any restriction from doing what they want to with those records, even if they claim the records are private and secure.

8. **Myth: Providers Are Required to Correct Any Errors Found in Patient Records**

Again, this is partially true. You do have a right to request changes to your records, but that doesn't mean they will get corrected.

If your provider refuses to make the changes, you may write a dispute letter about the errors you have found. The provider or facility must include your letter in your patient file.

9. **Myth: Your Health and Medical Records Cannot Affect Your Credit Records**

Wrong! When services have been provided to you by a provider or facility, they are entitled to be paid. They are allowed to do whatever is legal under bill collecting statutes to collect that debt, including turning your files over to a collection agency.

If you fall behind in paying your medical bills, that will be reported to credit agencies and your payment struggles will be recorded on your credit report.

10. **Myth: Medical Information Cannot Be Legally Sold or Used for Marketing**

This is also untrue, depending on how that information will be shared, and to whom, and of course, these rules are also confusing to providers. That means these rights may get violated, whether that is intentional or unintentional.

An example of when information can be shared for marketing purposes is when a hospital uses its patient list to inform you of a new service it provides, a new doctor who has joined the staff, or a fundraising program.

An example of when information cannot be shared without an additional authorization from you is when an insurer who has obtained your information from one of your providers, then uses or sells your information to sell you additional insurance, or another product related to services you have already received.

There are many other ways your medical information is sold and used for marketing purposes, too.

11. **Myth: HIPAA Can Be Used as an Excuse**

In general, patients and caregivers may find HIPAA being used to either prevent them or require them, to behave or conform to someone else's rules, even when it doesn't apply at all.

This is much easier understood with examples:

Example: A family member or advocate wants to stay at a patient's bedside in the hospital after visiting hours. One of the hospital personnel tells them they cannot stay because doing so would violate HIPAA because it impinges on another patient's privacy.

Not true. HIPAA says nothing about violating anyone else's privacy and has nothing to do with hospital visiting hours. In this case, the hospital is attempting to explain their unacceptable policy of making a protector leave the bedside.

Example: An elderly patient visits her doctor and waits in the waiting room until she is called. When she is finally called, her first name is used. "Anne!" She objects - because she doesn't like the 20-year-old medical assistant calling her by her 85-year-old-name. She is told they have no choice because HIPAA means they cannot use her last name.

Not true. HIPAA released interpretations of "incidental use" in 2002 which addressed this question specifically (page 7), saying that as long as the information called out is limited, there is no problem with calling out names. Think about it: when someone's name is called, no one is calling out their diagnosis or symptoms, meaning there is no medical information being used in conjunction with the patient's name. Using just a first name, or just a last name (Mrs. Smith) is perfectly acceptable and cannot be construed as violating HIPAA.

Example: A patient advocate posts his patient's name on a sign over the patient's hospital bed as a way to ensure that patient will be identified correctly, and to prevent errors such as the wrong drug or other therapy being administered to his patient. A hospital employee insists he remove the sign because it's a HIPAA violation to identify the patient.

Not true. The same document, on page 9, explains that this, too, is an incidental use of the patient's name and the sign is not a violation of the HIPAA law.

Article Sources: Verywell Health uses only high-quality sources, including peer-reviewed studies, to support the facts within our articles. Read our editorial process to learn more about how we fact-check and keep our content accurate, reliable, and trustworthy.

Edemekong PF, Haydel MJ. Health Insurance Portability and Accountability Act (HIPAA) [Updated 2019 Jun 18]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2020 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/

U.S. Department of Health & Human Services. Your Rights Under HIPPA. Health Information Privacy. Updated January 31, 2020. hhs.gov

U.S. Department of Health & Human Services. Covered Entities and Business Associates. Health Information Privacy. Updated January 31, 2020. hhs.gov

Gropper A, Peel D. How can my insurer or employer access my medical records without my permission? Patient Privacy Rights. patientprivacyrights.org