Patient's Guide to HIPAA

How to Use the Law to Guard your Health Privacy

WORLD PRIVACY FORUM

HIPAA and Reproductive Health

A companion FAQ to the Patient's Guide to HIPAA

July 2022

The World Privacy Forum publishes and maintains ***A Patient's Guide to HIPAA***, https://www.worldprivacyforum.org/2019/03/hipaa/ which is a plain language explanation of how to use the law to guard your health privacy. This companion FAQ on HIPAA is focused on reproductive health privacy in response to the many questions we are receiving from patients. We will be updating this FAQ regularly.

Introduction: Why is the law for health data privacy so complicated?

In the United States, we don't have a single privacy law covering all personal data. We have different laws covering different record keepers (e.g., banking, education, federal agencies, credit reporting, health care providers and some others). For many record keepers (e.g., phone apps, websites, data brokers, and others), HIPAA – the federal health privacy regulation in the US — only rarely applies, and even then, it will apply under specific conditions determined by the regulations.

Even though HIPAA is the major federal health privacy law in the US, it's still messy and complex. It can be difficult to know when your health information is covered under HIPAA, and when it is not. For example, personal health data has some privacy protections when held by doctors. But the same exact information will not have HIPAA protections when it is held by a third party company that is not specifically regulated by HIPAA. Federal health privacy protections do NOT follow the data, so even a lawful transfer of health data may result in data that was protected in the hands of your doctor has no meaningful protections in the hands of a third party. Some state laws may apply, but state laws vary in their protections.

Federal health privacy rules are important, and they do help — but they are by no means a 100 percent protective shield. For example, HIPAA does not adequately protect your health data from relatively easy access by law enforcement.

When HIPAA applies to health data, rules for reproductive health data are pretty much the same as all other health data. There's no special federal law on reproductive health data privacy. Some *genetic* data has protections in some contexts, but not in others. Some data that many would consider health data (e.g., pre-natal vitamins) is not treated as health data unless the vitamins are obtained through a prescription.

HIPAA is the Health Insurance Portability and Accountability Act. One part of this complicated law authorized the federal Department of Health and Human Services to issue regulations about health privacy. You can learn more at https://www.hhs.gov/hipaa/for-individuals/index.html. WPF maintains an extensive FAQ about HIPAA that is written in plain language here: https://www.worldprivacyforum.org/2019/03/hipaa/

What to do? Be careful about where you allow your health data to be held. Try to avoid leaving a paper trail. Pay cash when you can. Use search engines (like DuckDuckGo) that don't keep a copy of your searches. Be extra careful when giving your health information to a website that you don't know well. There will often be a risk that what you buy and what you search for and what you disclose online can be linked back to you. And you are not likely to get a Miranda warning about the possibility that your data can be used against you. You won't know in most cases who shares your data and when they share it.

In this FAQ, which is an extension of our Patient's Guide to HIPAA, we respond to concerns about reproductive health privacy and HIPAA.

1. Is the privacy of all reproductive health information protected by law?

The short answer to this question is that it depends on who is holding the health information. Personally identifiable health information in general has some legal privacy protections in the U.S., but there are many gaps in protections. Further, the legal privacy protections may not cover reproductive health information under all circumstances or in all states. Some health information (including reproductive health information) has no meaningful health privacy protection at all, depending on where or by whom it is held.

2. How can I tell if my health information is protected by HIPAA?

This is a hard question to answer briefly. Here is some general guidance for all health information, including reproductive health information.

Determining whether HIPAA applies is the first step to determining what kind of privacy protections apply to your information. Not all health information is covered under HIPAA (the federal health privacy law) and this can cause a lot of patient confusion.

To determine if your health data has HIPAA protections, the first step is to determine who or what entity has your information. For example:

- If a **health care provider** or **health insurer** has your information, then the information almost certainly has some federal health privacy protections. What you are looking for is to find out if your information is being held by what is typically called a **covered entity under HIPAA**. See FAQ 3 in this document for more details on who or what is a covered entity under HIPAA.
- If your health data is held by anyone other than a health care provider or health insurer, then there is a high probability that the information does not have federal privacy health protection under HIPAA. To clear up any doubt, ask them if they are a "covered entity under HIPAA." The answer to this question should be yes or no.
- If you are still not sure the entity that is holding your health data is regulated under HIPAA, look to see if the holder of your health information has a privacy policy.

Be aware: "HIPAA compliant" or a covered entity under HIPAA?

Entities regulated under HIPAA must have notices of privacy practices that refer in detail to the rights you have under HIPAA. These privacy notices let you know how you can exercise your rights.

For example, all HIPAA covered entities must disclose that consumers have the right to access their health information, the right to receive an accounting of disclosures, and more.

The privacy policies of entities that are not actually regulated under HIPAA may say they are "HIPAA compliant." They typically will not spell out all of the rights under HIPAA in their privacy policies. The term "HIPAA compliant" is confusing, perhaps to encourage consumers to think that there are HIPAA protections when there are not. HHS published guidance about the use of the term "HIPAA compliant": https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/be-aware-misleading-marketing-claims/index.html

Many privacy policies of health care providers will say "Notice of Privacy Practices." Entities regulated under HIPAA will disclose to you in detail what your rights under HIPAA are, and explain how you can exercise those rights. So, look for the term "Notice of Privacy Practices" and for a listing of your rights under HIPAA and how to use the rights.

- Be cautious of a privacy policy that uses the words *HIPAA Compliant*. Some companies that are not subject to HIPAA say they are *HIPAA compliant*, a confusing term that few consumers understand.

3. What does the federal health privacy law (HIPAA) cover?

HIPAA covers your health information when your data is held by health care providers, health insurers, and some others, as defined in the law. These are the HIPAA *covered entities*.

When HIPAA applies to your health data, it applies to all personally identifiable information (whether it is strictly "health" data or not) when it is held by providers, insurers and other "covered entities." But remember: HIPAA does not protect the privacy of all health data, everywhere. A**ny entity that is not a HIPAA covered entity is not covered by HIPAA requirements.**

If a HIPAA covered entity discloses health information to a third party that is not a HIPAA covered entity, that information is not protected by HIPAA in the hands of that third party. This is true whether it is shared with or without your consent.

The protections of HIPAA do not apply to health information independently of who possesses the information. The protections apply only to health information held by HIPAA covered entities. Other privacy laws may or may not apply to data held by third parties who are not HIPAA covered entities.

Does HIPAA apply to websites and phone apps?

HIPAA applies to most health care providers and all health insurers. This is not the case for most websites and phone apps. These can share your personal health information without regard to HIPAA, because none of the HIPAA limits are relevant to these websites and apps unless directly offered by a HIPAA covered entity. Remember that privacy policies that say "We are HIPAA compliant" do not necessarily mean that the entity making the statement is actually regulated under HIPAA.

Be careful when you think about sharing reproductive health data with a web site, app, or entity, and make sure that HIPAA actually applies. For more information about this topic, see A Patient's Guide to HIPAA FAQ 9: Which Health Care Entities Must Comply with HIPAA? https://www.worldprivacyforum.org/2019/03/hipaa/

4. Is HIPAA the only law that protects the privacy of health information?

No. There are other federal laws that cover some types of personal information held by federal agencies. There are federal laws that also protect the privacy of health information about substance abuse. See Patient's Guide to HIPAA, FAQ 3: https://www.worldprivacyforum.org/2019/03/hipaa/. In addition, some states have their own health privacy laws that may help, but state laws are beyond the scope of this FAQ.

5. Does all reproductive health information have privacy protections?

The short answer here is that not all reproductive health information has HIPAA privacy protections. It will depend on who or what entity is holding the data.

- If a HIPAA covered entity holds the information, then the reproductive health information has the same privacy protections as all other health information held by covered entities.

- If any entity other than a HIPAA covered entity is holding the health information, then it is possible that no health or other privacy rules apply. Most websites or phone apps are not subject to HIPAA. There are major gaps in the protection of health information when it is held outside of HIPAA.

Just when you think it can't get more complicated, there is something called a hybrid entity under HIPAA. An example of a hybrid entity is when a pharmacy covered under HIPAA is housed within a grocery store that is not covered under HIPAA. For more on this scenario, see Patient's Guide to HIPAA, FAQ 9.

6. I agreed to let a health app access my health records. Is my health information protected under HIPAA?

If the health app is provided to you directly by a health care provider in a manner that makes the records subject to HIPAA, in this case, yes, your health information is protected under HIPAA.

But – beware. It can be difficult to tell for sure if a health app is or is not covered under HIPAA. The majority of apps that you can download from an app store are not likely to be covered under HIPAA. Check the privacy policy, and ask your health care provider if the app is covered under HIPAA or not.

If HIPAA **does not** apply, then the privacy protections for your records in the hands of the app are those provided by the app in its privacy policy. And that privacy policy may be subject to change by the app as it sees fit. State laws may offer some additional protections, and these protections will vary.

Please note that even if the app is one of the few subject to HIPAA, there are still real risks that law enforcement could obtain data in states that make abortion a crime. See the other FAQs here, including FAQ 7.

7. When does HIPAA allow a HIPAA covered entity to give reproductive health information to law enforcement?

This is complicated, but we will explain this as plainly as possible.

Remember first of all that if HIPAA does not apply to the holder of the reproductive health information, then there may be no limits on sharing with law enforcement. So, the first step is to determine if your health information is being held by an entity regulated by HIPAA. See FAQ 2 in this document for more about this. HIPAA is not perfect. But it offers better protections than none at all.

For entities that are in fact regulated by HIPAA, HIPAA does have limits on the sharing of health information with law enforcement. However, these protections are not absolute. HIPAA contains meaningful exemptions to its substantive and procedural protections regarding law enforcement access, and the sharing of health data with intelligence agencies is virtually unrestricted.

There are several situations in which health information can be shared with law enforcement entities. They are as follows:

Sharing pursuant to a subpoena, court order, summons, or warrant:

If a law enforcement agency obtains a subpoena, court order, summons, or warrant, then HIPAA allows for the sharing of any health information (reproductive health information or otherwise). HIPAA does not

compel the sharing on its own. HIPAA rarely requires the sharing of health data. It merely *allows* sharing. In the case of a subpoena, court order, summons, or warrant, the compulsion comes from the court that issued the process.

Sharing pursuant to administrative requests:

HIPAA also provides that a covered entity may turn over health information to law enforcement in response to an administrative request. What is an administrative request?

- An administrative request could be an administrative subpoena issued by a government agency.
- An administrative request could also be an oral request from any police or law enforcement officer.

Regarding oral requests, law enforcement officers from any local, state, or federal agency can go to a hospital (or other health care provider) and make an oral request for reproductive health information. There is no requirement for an official subpoena, court order, or even that the request be in writing. There is no requirement for approval of the request by the law enforcement officer's supervisor.

Limiting conditions for sharing pursuant to administrative requests:

There are three conditions that limit these law enforcement administrative requests.

- **Information must be relevant to a legitimate law enforcement inquiry:** First, the information sought must be relevant to a legitimate law enforcement inquiry. If abortion (or any other medical procedure) is illegal in any given state, any request that pertains to a possible illegal abortion or medical procedure would likely meet this condition.
- **The request has to be specific and limited in scope to the extent reasonably practicable in light of the purpose of the request:** The second limiting condition is that the request has to be specific and limited in scope to the extent reasonably practicable in light of the purpose of the request. Under this standard, it is likely that a police officer in a state where abortion is illegal could ask a hospital or other provider for information about any woman who was admitted with a miscarriage or under other circumstances that suggest the possibility of an illegal abortion. Still, the answer here is not clear. When is a request specific enough and limited in scope to meet the standard in the law? Lawyers can argue about this at great length.
- **Identifiable information is only allowed if de-identified information could not reasonably be used:** The third limiting condition is that a request by law enforcement personnel for identifiable information is only allowed if de-identified information could not reasonably be used. For any law enforcement inquiry focused on a possible violation of an anti-abortion law, this standard might be easy to meet.

8. Does HIPAA really allow a covered entity to give reproductive health information to the police in response to an oral request?

Yes, HIPAA does allow this. Remember, however, that a HIPAA covered entity is not *required* to turn over information in response to an oral administrative request. HIPAA allows the disclosure, but it does not mandate that a covered entity turn over the records requested. Many hospitals and other health care providers would not casually turn over any personal health information to oral law enforcement requests.

For example, many hospitals may have their own internal procedures that control when hospital personnel can share information with law enforcement. But if a hospital or provider opposes abortion or operates in a

state where abortion is a crime, information might be shared, depending on the policies. It will be difficult for the average patient living in a state where abortion is illegal to be sure what policy or procedure a hospital or other provider will follow before turning personal health information over to law enforcement.

9. Are there other circumstances in which HIPAA allows disclosure to law enforcement?

Yes. Another provision in HIPAA allows reporting of health information about the victim of a crime. If abortion is illegal in a state, and a fetus of any age is considered a victim of that crime, some information about that victim could be shared.

Yet another provision in HIPAA allows a covered entity providing emergency health care in response to a medical emergency to disclose information to law enforcement if the disclosure appears necessary to alert law enforcement about the commission and nature of a crime, the location of the crime, and the identity of the perpetrator. This too might allow notification of some reproductive health information to law enforcement by a HIPAA covered entity in states where abortion is illegal.

10. If I have a miscarriage and seek treatment at a hospital, can the police get my information from the hospital to see if I can be prosecuted for an illegal abortion?

If you live in a state where abortion or another medical procedure is illegal, it is quite possible that the police can obtain your health care records for a prosecution. There are multiple ways under HIPAA for the police to seek and obtain reproductive health information. See the previous three FAQs.

11. I use a period tracker. Does my information have privacy protections?

Probably not under HIPAA. Unless a health care provider (a covered entity under HIPAA) operates the tracker as part of the health care offered to you, HIPAA will typically not apply. For example, if a provider merely suggests that you use a tracker, that is not enough to bring the tracker under HIPAA. That is true even if you authorize the tracker to report your information directly to your health care provider. Your information may be protected in the hands of the provider, but that same information in the hands of the commercial tracker app is not protected by HIPAA.

Beyond HIPAA protections, state-level laws may apply to apps and websites, but protections vary a lot. Health apps and websites typically have their own privacy policies. But even if those policies offer reasonable protections for your data, the website promises do not equal the statutory protection that HIPAA offers for your health data. Also, HIPAA requirements and protections rarely change, but many commercial privacy policies are subject to change without notice. That means that website or app that promises limits on data sharing today can remove those limits at will. This is why determining whether or not your data is being held by an entity regulated under HIPAA is still important.

12. If I obtain a "morning after" pill from a pharmacy, is the privacy of my information protected by HIPAA?

HIPAA protects prescription drug information. Pharmacies, including mail order pharmacies in the United States, are HIPAA covered entities. However, Plan B ("morning after" pills) pills may be available without a doctor's prescription. The Plan B drug may be offered as an over-the-counter drug or a "behind the counter"

drug for which no prescription is required. Remember that if you go to a drug store and buy items that do not require a prescription – such as aspirin or soap or soda – it is highly likely that the record of your purchase is not subject to HIPAA protections.

An in-person pharmacy that manages Plan B drugs as a behind-the-counter item might or might not keep purchase records in a manner that complies with HIPAA. Read the privacy policy to find out. Assume that HIPAA does not apply unless you are sure otherwise.

Any merchant selling a Plan B drug without a prescription is not obliged to comply with HIPAA, and it is likely that most do not. Whether they comply with HIPAA or not may depend whether they also sell prescription items and on how the merchant organizes its records. It can be complicated and hard to be sure from the outside. Don't necessarily trust the pharmacist or pharmacy assistant to know the specifics of the store's privacy policy.

13. If I obtain an abortion pill from a pharmacy, is the privacy of my information protected by HIPAA?

Yes. HIPAA protects all prescription drug information. Pharmacies, including mail order pharmacies in the United States, are HIPAA covered entities. Because abortion pills require a prescription, this information is subject to HIPAA.

Remember that if you have health insurance that covers abortion pills, and if you use that insurance to pay for an abortion pill, the records that the health insurer maintains are also subject to HIPAA. However, your health insurer may be located in a different state than your pharmacy. That means that different state laws may apply. In the state where your doctor or pharmacy operates, state law may provide additional protection for reproductive health information. Your insurance company may be located in a different state with different or lesser protections against law enforcement access and use of the records.

If possible, consider paying cash for an abortion pill. You might also consider obtaining the pill from a pharmacy that you do not otherwise use for your other prescriptions. Your regular pharmacy will keep all your prescription records in the same file, and that entire file might be shared with your insurance company at some time.

14. I have a copy of my health data on my mobile phone, and I have not allowed anyone else to access it. Is this information protected?

When you have downloaded a copy of your health files to your mobile phone, this is considered to be information held outside of HIPAA in most circumstances. The data on your personal mobile phone, if it is saved in the cloud, could be accessed through your cloud provider, or through your app provider that stores your data.

If you downloaded your health records and store it totally on your phone with no cloud or online backup, and your phone requires some form of password or biometric to unlock, the records will be more secure. If you really want to lock things down, encrypt your files and keep them stored in an encrypted state, and do not allow these items to be backed up to the cloud.

15. A federal law protects illegal drug users who seek treatment from having their treatment records turned over to the police to be used for prosecution of illegal drug activities. If abortion is illegal in a state, is there any comparable protection for health records about abortions?

No. Please see *Patient's Guide to HIPAA, FAQ 3 "Confidentiality of Alcohol and Drug Abuse Patient Records Regulations"* for more information about this topic. https://www.worldprivacyforum.org/2019/03/hipaa/ To summarize here, illegal drug users who seek treatment have specific legal protections against disclosure to the police. These rules for illegal drug users were created to encourage drug abusers to seek treatment without risk of arrest. These same kinds of protections do not exist for reproductive health information.

Most recent version: July 7, 2022
Original Publication: July 7, 2022

Authors: Robert Gellman, Pam Dixon
Design and illustration: John Emerson

World Privacy Forum
www.worldprivacyforum.org