MINTZ

Protecting Health Information Post Roe Part 1: Steps for Women

July 05, 2022 | Blog | By **Dianne J. Bourque**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity
- Health Care
- Women's Health and Technology

RELATED PRACTICES

- Privacy & Cybersecurity
- Health Care Enforcement & Investigations

RELATED INDUSTRIES

- Health Care
- Women's Health and Technology

In the wake of the Supreme Court's ruling in ***Dobbs vs. Jackson Women's Health Organization***, much has been written about how existing privacy laws, such as the Health Insurance Portability and Accountability Act ("HIPAA"), are unhelpful to women because of provisions that permit the sharing of health information (called "protected health information" or "PHI" under HIPAA) with state regulatory authorities seeking to enforce abortion prohibitions. For example, HIPAA permits health care providers to disclose health information when required by law, such as state-mandated abortion reporting laws, or for purposes of law enforcement, such as in response to a warrant, subpoena or summons.

However, HIPAA has other provisions, including enumerated patient rights, that are potentially helpful to women seeking to protect their reproductive health information. There are also state laws and practical strategies that women can use to protect their privacy. In the first of this two-part blog post series, we will highlight legal rights and practical strategies that women can use to protect their own information. In a second installment, we will highlight strategies that health care providers can use to protect their patients' information post *Roe*.

OCR Guidance

The Department of Health and Human Services Office for Civil Rights ("OCR") recently posted a **guidance** document (the "Guidance") on how HIPAA supports women's efforts to keep their reproductive health information private. The Guidance discusses the scope of HIPAA's exceptions for disclosures required by law and law enforcement and highlights the important point that health care providers may only disclose health information to regulatory or law enforcement authorities when it is *required* by law. If a state law does not mandate reporting, any disclosure of a woman's health information under that law would potentially violate HIPAA and provide the basis for a complaint to OCR by the affected patient.

Accounting Right

How would a patient know if her information was used or disclosed by a health care provider in response to a government request? HIPAA gives patients a right to an accounting of disclosures of their PHI. An accounting is a notice that tells a patient how her health information has been used or shared for certain purposes. For example, if a health care provider shares records with a public health authority for public health surveillance activities, all records shared with the public health authority have been "disclosed" for purposes of HIPAA. If the patient requests an accounting, the provider must provide the identity and address if known, of the public health authority to which the records were disclosed, a description of the records and the PHI disclosed, the purpose for the disclosure and when access was provided. The accounting right will not help a patient to prevent a disclosure, but it could at least alert a patient to the fact that a disclosure has occurred and would allow the patient to independently evaluate the validity of the disclosure.

Right to Request Restrictions

Patients have the right under HIPAA to request restrictions on how a health care provider uses or discloses their PHI. For example, a patient may request that a covered entity restrict uses and disclosures of PHI to treatment, payment or the provider's healthcare operations (which are uses necessary to run the provider's business). A patient may also request special privacy protections, for example, a patient can prohibit the disclosure of PHI to family members or request the provider to use an alternative mailing address or PO box for treatment-related communications. Under HIPAA, providers must allow patients to request restrictions, however, providers aren't required to grant requested restrictions. There is one exception: if a woman pays for a reproductive health care visit, a prescription (or any health care for that matter) out-of-pocket in full and requests that the health care provider or pharmacist not share information about that visit with her health plan, the provider and pharmacist must agree to that restriction. This HIPAA provision doesn't fully insulate reproductive health information, but it

narrows the universe of authorized recipients, reduces the potential for re-disclosure and reduces the number of places where regulatory authorities can gather information about a woman's reproductive health.

All of the rights described above must be addressed in a health care provider's HIPAA Notice of Privacy Practices. These notices are provided to patients on their initial visit to a health care provider, they must be posted on the walls of a provider's facility and must also be available upon request and on the website of any provider with a website. Finally, patients have the right to complain to OCR if any of the above patient rights requests are ignored or denied, or if a patient believes that her health information has been used or disclosed in a way that is not permitted under HIPAA. Patients can **file a complaint with OCR** OCR will follow up, but there is no right for patients to sue for damages (called a "private right of action") under HIPAA.

State Law Protections

There may be additional protections available under different types of state laws, including private rights of action for unauthorized disclosure as data breaches or consumer protection actions. These will likely be tested in states with abortion bans, but let's look at the present state of the laws in those states with trigger bans. Of the states where abortion is currently banned or mostly banned, or will be banned imminently under trigger laws, only a handful include health information as "personal information" under state data breach notification statutes, and there are limitations to their applicability. In order to be considered a "breach" under state data breach notification laws, there must be unauthorized access to or acquisition of personal information. In all of the states where abortion is banned or will be banned imminently, the data breach notification laws are only triggered by "acquisition" of the personal/health information; in other words, someone actually has to take it.

The chart below outlines what possible additional protections may be available.

State	Health Information Included in state breach notification statute?	Private Right of Action?	Rules for Responding to Subpoenas?
Alabama	Yes	No	Subpoena must be HIPAA-compliant
Arkansas	Yes	No	Must notify patient (or patient's attorney) by writing or fax
Idaho	No	No	None beyond HIPAA
Kentucky	No	No	None beyond HIPAA
Louisiana	No	Yes (but since health information is not included in state statute, irrelevant)	Subpoenaed provider must receive affidavit that subpoena is for records of party to litigation and notice has been mailed to affected patient 7 days before issuance
Missouri	Yes	No	None beyond HIPAA
North Dakota	Yes	No	None beyond HIPAA

Ohio	No	No	None beyond HIPAA
Oklahoma	No	No	None beyond HIPAA
South Dakota	Yes	No	None beyond HIPAA
Tennessee	No	Yes (but since health information is not included in state statute, irrelevant)	None beyond HIPAA
Texas	Yes	Yes	Patient must be party to judicial proceeding and disclosure is pursuant to subpoena issued under (1) TX Rules of Civil or Criminal Procedure; or (2) Chapter 121 of the TX Civil Practice and Remedies Code, Safety Code, or Occupational Code
Utah	No	No	None beyond HIPAA
Wyoming	Yes	No	None beyond HIPAA

Practical Measures to Take

The world has changed in the 50 years since *Roe v. Wade*. Now, we all have vast "digital footprints" created from things such as our Internet search and surfing habits, information we share with apps, location data collected by our tablets and smartphones (even when we are unaware of such collection…). There is a concern about the ability of these digital footprints to be used against women in an attempt to enforce criminal penalties in abortion ban states.

We cannot disappear from the digital world. But, there are some practical measures that you can take to protect this sensitive information.

- Limit sharing of location data. You can turn off the location services on your smartphone or tablet. This will limit access to your activities, your location, and where you travel. On either an Apple or Android device, location services can be found in Settings/Privacy. You have the option to turn off all access to Location Services, or you can go through your apps and select those for which you want to turn off access to location data. While you're doing that, you can clean up unwanted apps on your device, clear the history and data stored in those apps, and only add apps that you trust. Also, when an app or website asks permission to access location data, you should opt out. Unless you are using a navigation or traffic app, most apps and websites do not need your location data. Avoid "free" apps: remember, if you're not paying for the "service," you are the service.

Information from Apple regarding the privacy of your data on Apple devices is available at: **https://www.apple.com/privacy/control**. Information regarding the privacy of your data on Android devices is available at: **https://www.android.com/safety**.

- Consider using a **burner phone**. If you have to arrange for services or travel, use a burner phone. If you use a personal device, any communications you send and receive (texts, calls in and calls out, email) are stored and can be tracked.
- Use a public computer for web searches. If you use a common search engine like Google, Yahoo!, or Bing, your search history may be associated with your IP address and can be obtained by law enforcement from the service provider. If you need to search for banned services, use a computer at a public library or other space.

- Alternatively, use a private search engine. There are search engines like **DuckDuckGo** that do not track your search history.
- Don't forget your smart watches or fitness trackers. These devices also collect or store information about your location, and fitness trackers may also contain information about menstrual cycles or other health-related information.

On Friday of last week, **Google announced** that it will delete location data after people visit abortion clinics, domestic violence shelters, and other sensitive locations. According to Google, the update will "take effect in the coming weeks." Additionally, the company will add a feature for users to delete multiple menstruation logs at once on Google Fit and Fitbit apps. The Google announcement says nothing, however, about history of search results.

The **New York Times** has published an informative article on how mere deletion of period-tracking apps may not be sufficient (article is behind paywall).

There are other resources out there that you should review to help reduce your digital footprint and to protect your own medical privacy.

Guidance from the Department of Health and Human Services

Guidance from the Federal Trade Commission on how to protect your phone and the data on it

How to Limit Location Data Exposure – National Security Agency

Consumer Guidance from the Federal Communications Commission – phone and cable records

Authors

Dianne Bourque

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.