



Data After *Dobbs*

**Best Practices for Protecting
Reproductive Health Data**

May 2023

cdt CENTER FOR
DEMOCRACY
& TECHNOLOGY



The **Center for Democracy & Technology** (CDT) is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1996, CDT has been a trusted advocate for digital rights since the earliest days of the internet. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.



Among other activities, CDT convenes a **Task Force on Protecting Reproductive Health Information** that [brings together experts](#) from reproductive rights groups, healthcare providers, civil rights and privacy organizations and technology companies to identify ways to protect the privacy and access to information of people seeking reproductive care.



Data After *Dobbs*

Best Practices for Protecting Reproductive Health Data

Author

Andrew Crawford



Acknowledgements

This CDT report is informed by consultations with a variety of stakeholders including reproductive rights groups, health service providers, data privacy experts and members of CDT's Task Force on Protecting Reproductive Health Information.

May 2023



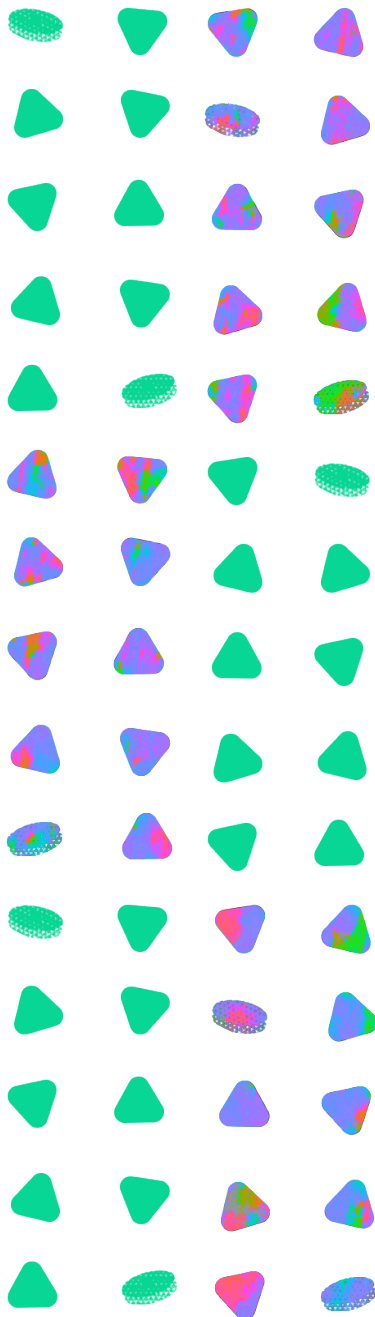
*This report is licensed under a Creative Commons
Attribution-Sharealike 4.0 International License.*

Table of Contents



Introduction	5
Best Practices	6
<i>For Health Data</i>	8
<i>For General Data</i>	10
<i>For the Content of Communications</i>	12
<i>For Employment Health Data</i>	13

Introduction



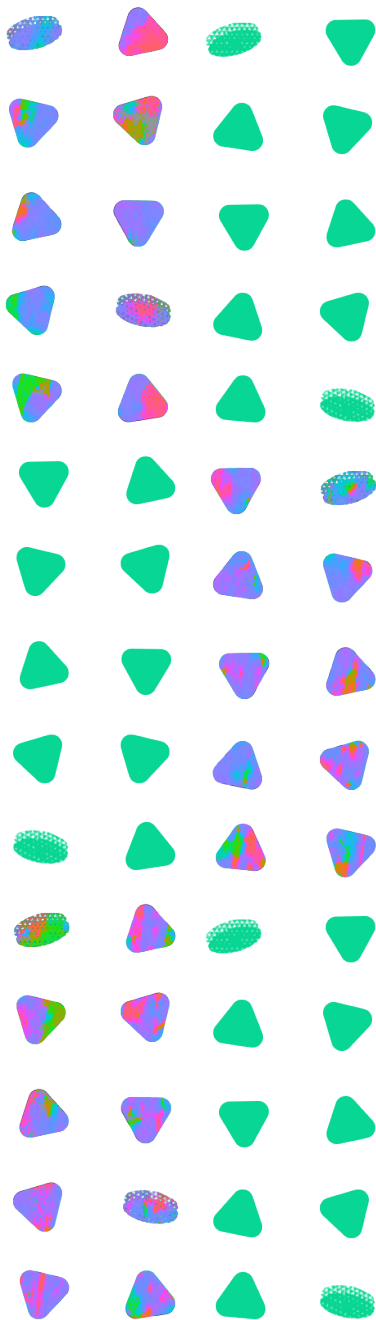
This document outlines best practices for companies that collect, retain, share, sell, and use data about people’s reproductive health. While not exhaustive, these recommendations are a starting point for companies, including small companies, to reduce the likelihood that the information they collect could be used in abortion-related prosecutions and civil lawsuits.

When the Supreme Court reversed *Roe v. Wade* in *Dobbs v. Jackson Women’s Health Organization*, it enabled [states to further restrict and criminalize abortion](#). Some [states can now prosecute abortion providers, insurers](#), and, in some cases, [even patients themselves](#). Some [states also allow civil actions](#). Increasingly, law enforcement and civil litigants may turn to companies to gain access to data that could help prove that a person sought, received, aided, or provided an abortion.

Many types of data can reveal sensitive information about a person’s health and healthcare choices. Search queries, browsing history, the contents of communications, and a person’s location data can all reveal such private information, despite not typically being thought of as sources of “medical” or health-related data. Because of this, companies inside and outside the healthcare sector must be responsible for carefully assessing and limiting the private information they collect, store, and share. Without thoughtful action, a company’s data practices may be complicit in sending their customers to prison or exposing them to civil litigation, for personal choices that are still legal in the majority of the United States and that were constitutionally protected for almost 50 years.

In the post-*Dobbs* era, companies must play an active role in protecting their customers’ and users’ private information. This document details how. It is intended as a practical guide for company decision makers, product designers, developers, advocates, and concerned customers to understand the privacy concerns inherent to many data collection practices, and how companies can act.

Best Practices



The best way to prevent data that companies collect from being used against abortion-seekers is to simply not have that data in the first place.

By being diligent and knowing what data is needed for products and services, and declining to collect additional data, companies can help reduce the likelihood they will have to respond to law enforcement or civil litigants' requests for data in abortion-related prosecutions. In instances where companies *must* collect personal data, companies can and should retain that data only for as long as necessary to perform the task that the data was originally collected for. And then it should be deleted.¹ Data should not be kept, shared, or sold for unrelated purposes. When data is shared with third parties performing services on behalf of a company, companies must require these third parties to safeguard the data and only use it for purposes limited to the business service being performed. Further, while companies hold personal data, it [should be encrypted so that only customers can access their data](#).

A wide variety of data can be [used in abortion prosecutions](#). It is therefore important for companies to know what data they collect, how they use that data, and who they share that data with. This effort cannot be limited to obvious health data (biometrics, health conditions, health measurements, etc.). It should include all data the company deals with, because information that may not appear to be health-related can reveal a person's health conditions and choices when used in certain ways or combined with other data points. Such data includes location data (visiting a provider or specific clinic can be very revealing about a person's health), browsing history, and search queries.

Once a company understands the types of data it collects, it can

¹ This guidance recognizes that there will be instances when companies are required to collect and/or retain data to address instances of fraud, harassment, or illegal activity; to comply with a legal obligation; or to investigate, prepare for, or defend legal claims. However, in instances when an applicable law or regulation requires collection and/or retention of certain data, a company should pledge to not use or share this data for any other purpose.

assess the necessity of that collection, and examine how long sensitive data is stored, how it is shared, and what steps the company can take to protect users' privacy. Such actions can help decrease the likelihood that a company will be called on to participate in reproductive-related prosecutions, increase consumer trust, and help companies get ahead of the regulatory curve as more jurisdictions protect the treatment of customers' sensitive information.

Companies should also be transparent with their customers. They should share information about the data they collect, and how they protect it. They should also inform customers about how they will handle law enforcement and civil requests for information, such as publicly committing that a government data request will be satisfied only if accompanied by a judicially enforceable order. Whenever possible, companies should immediately notify customers when their data has been sought and turned over to law enforcement or a civil litigant. Additionally, companies should publish periodical transparency reports on government data requests that include details and metrics on the types of requests received and compliance rates.

The following sections address specific best practices for various types of data.

The best way to prevent data that companies collect from being used against abortion-seekers is to simply not have that data in the first place.

For Health Data



Companies that collect and share health data have a special responsibility to protect their users' privacy. While such companies can include health care providers whose records are, in most instances, governed by the Health Insurance Portability and Accountability Act (HIPAA), this also includes non-HIPAA covered entities such as companies that sell health-related products or produce wearables, fitness trackers, and other consumer services that track people's symptoms and other health information.²

Health Data Includes:

- **Medical records** - This is a very specific data set that is intended to cover records that were created by a HIPAA-covered entity but have been transferred, via the patient, to a non-HIPAA covered entity, like a health records app on a smartphone. These records are very sensitive as they can include doctors' notes and referrals, medical images, and test results.
- **Data generated by health and fitness tracking apps** - Examples of this data include information on apps like a period tracker. This sensitive data can reveal missed periods that later resumed, which could suggest a birth, abortion, or miscarriage. These apps may also be connected to wearables, fitness trackers, and Bluetooth location trackers that collect revealing health-related information.
- **Data generated by service providers** - Examples of this data include information people share with services that connect users with medical providers, like mental health providers or pharmacies. For some companies (such as websites providing information on how to access abortion care or connecting people to abortion funds), it may include even basic pixel data revealing that a person visited their website. This data is very sensitive as it can reveal a person's physical and mental health conditions.

2 While these best practices are designed to aid companies who are not subject to HIPAA and its associated regulations, these recommendations are designed to complement and be consistent with the privacy protections afforded to health data held by HIPAA-covered entities. For more information about current and proposed privacy obligations of HIPAA-covered entities, the Department of Health & Human Services (HHS) [has numerous resources](#). Moreover, in December 2022, [HHS released a Bulletin](#) highlighting the important privacy obligations under HIPAA that health providers (such as doctors' offices and hospitals) must follow when using apps and websites. Finally, in April 2023, HHS released a [Proposed Rulemaking to Support Reproductive Health Care Privacy](#) that would further limit instances when reproductive health records can be shared.

For these health-centric data sets, the following practices should be implemented whenever possible:

- Companies that collect health data should use this data only to provide directly requested services.
- Health data should not be used to create user behavioral profiles or shared or sold for secondary purposes, even if the data is de-identified, as it can be re-identified when merged with other datasets.
- Whenever possible, this data should be encrypted such that only the customer can access it.
- People should be able to access, make clerical edits to, and delete any health data collected and retained by the company.
- Health data should be retained only for a limited time; when it is no longer needed to provide the direct service or product requested, it should be deleted permanently.

For General Data

Many types of data can reveal information about a person's health or healthcare choices, regardless of whether the company collecting it provides health-related services. People's online searches and browsing history have already been used in abortion-related prosecutions, and investigative reporters have shown that location data can be purchased revealing where visitors to an abortion clinic went immediately before and after their visits, which can be highly revealing of a person's identity. Companies across the spectrum must consider how they collect and treat this type of information.

General Data Includes:

- **Search history** - This is data generated from web searches or using search functionality within an app or website. It could include data showing that a person searched for the address of a reproductive care provider; sought information about the legal status of abortion in a person's state; or the products people search for in online stores. Whether someone actually clicks on a link for a product returned via a search should also be included in the scope of protected information.
- **Browsing history** - This is data generated from people when they navigate the internet. In its most basic form, it is a list of the websites, and pages within websites, a person has visited. It can include specific data about when, where, and how long a person visited unique websites or specific pages of larger websites.
- **Purchase history** - This is behavioral data comprising records of people's purchases. It can include histories of specific products and services people have purchased from specific companies. When it comes to reproductive health data, this can include information about a specific person's purchases of prenatal vitamins, a pregnancy test, or medications like misoprostol. This data could also include items from credit card statements or data collected as part of a company's loyalty programs.
- **Location Data** - This data reveals where a person has been in the past or present and can be extremely sensitive, especially when it comes to a person's health. Knowing what clinic a person visited, when, and how much time they spent there can be extremely probative.

For general data sets, the following general practices should be implemented whenever possible:

- Companies that collect these types of data should use them only for the direct service a person is requesting - e.g., to provide search results based on a specific search query.
 - » This data should not be used to create user behavioral profiles or make inferences about a person's health.
 - » This data should not be shared or sold for secondary uses.
- People should be able to access, edit, and delete their data wherever legally permissible.
- This data should be retained only for a limited time; when it is no longer needed to provide the direct product and/or service a person has requested, or to comply with other legal obligations, it should be deleted permanently.
- Search data should be used for limited contextual advertising, meaning advertising based on the search terms that were entered *in this search only* and not prior searches.
- Whenever possible, companies should immediately anonymize location data associated with sensitive locations (such as hospitals, clinics, pharmacies, etc.), by removing identifying information from the dataset, with the intention of quickly deleting the data entirely.

For the Content of Communications

The content of communications is some of the most personal data companies can possess. Current law recognizes the sensitivity of this data and requires a probable cause warrant when law enforcement seeks this information. However, as [news reports](#) have shown, law enforcement has been able to compel disclosure of the contents of communications involving people's reproductive health. It is also possible for law enforcement to [sidestep traditional legal requirements by obtaining data on Americans through commercial purchases from data brokers](#).

Content of Communications Includes:

- **Emails** - This data includes not only the text of an email, but also any associated attachments like photos or documents.
- **Messages** - This data includes messages exchanged via smartphone messaging apps, messages to individuals or groups on social media platforms, and other web-based messaging services.
- **Calls and Audio Messages** - There are long standing expectations around the privacy of phone calls. But audio messages are not limited to phone calls. This data also includes video-based calls and direct audio messages.

For contents of communications, the following general practices should be implemented whenever possible:

- Companies should deploy end-to-end encryption as a default on all direct communications on their service or platform to ensure that only the sender and intended recipient can access private communications.
- Companies should be transparent with their users and make it clear when the contents of their communications are not encrypted.
- Companies should tell users when their data has been disclosed to law enforcement unless this type of notice is precluded by court order, in which case users should be told as soon as any court-imposed delay of notice expires.
- Companies should offer and then encourage users to use ephemeral types of messages, such as automatically-deleting messages.

For Employment Health Data



Most people in the U.S. obtain their health insurance or other health-related benefits via their employer. As such, there are instances where an employer may have very intimate knowledge about an employee's reproductive health. For example, some employers are now offering to pay for travel and related expenses of employees seeking an abortion.

Employment Health Data Includes:

- Data used to provide employees health insurance or other health-related benefits can include more than just an employee's name and contact details. This can include data about specific types of care and services employees utilize, the frequency of use, and even employee use of sick and family medical leave time.

For employment health data, the following general practices should be implemented whenever possible:


- Employers should avoid collecting and retaining sensitive medical information about their workers. For example, a third party service can administer a company's program to reimburse employees who travel to receive out-of-state medical treatment. Employers can also ensure their out-of-state travel reimbursement programs apply to medical services other than abortions, so that employees using such programs do not inherently reveal the purpose for which the program is being used.
- Companies who collect health data about their employees should use this data only to provide health insurance or other health-related services to their staff.
- Employment health data should not be used to create user behavioral profiles, or shared or sold for secondary uses.
- People should be able to access, make clerical edits to, and (where appropriate) delete their employment health data.
- Employee health data should be retained only for a limited time. When it is no longer needed to provide the health service an employee has requested, it should be permanently deleted.


***In the post-Dobbs era,
companies must play an
active role in protecting
their customers'
and users' private
information.***



 cdt.org

 cdt.org/contact

 Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

 202-637-9800

 @CenDemTech

