

My Health My Data

Washington's consumer health data privacy law.

**HIPAA protects health data based on who holds it.
My Health My Data protects it based on what it is.**

What it is

The My Health My Data Act is Washington's consumer health data privacy law. It took effect in 2024. It was written to cover health information that falls outside HIPAA: the data collected by apps, websites, marketing tools, and other systems that were never regulated as medical records.

It is not HIPAA, and it runs alongside it

This law does not replace HIPAA. Both can apply to you at the same time. The exemption people rely on follows the **data**, not the organization: your PHI is exempt, but the non-PHI health data you hold is not exempt just because you are a HIPAA-covered entity. There is no general nonprofit carve-out either.

What data it covers

"Consumer health data" is defined broadly, far wider than the medical record. It includes:

- Conditions, diagnoses, treatment
- Mental and behavioral health
- Reproductive and sexual health
- Gender-affirming care
- Prescribed medications
- Biometric and genetic data
- Precise location tied to seeking care
- Data identifying someone seeking care

Who it can reach

- An organization that **conducts business in Washington**, or targets products or services to Washington consumers, and decides how consumer health data is handled.
- A "**consumer**" is a Washington resident, or a person whose consumer health data is collected in Washington. The entity itself can be based elsewhere.

Three common misreads

"We have HIPAA, so we're covered."

The exemption covers your PHI, not everything you hold. Non-PHI health data can still be in scope.

"A cookie banner handles consent."

Most trackers fire when the page loads, before anyone clicks the banner, so the data has often already gone out.

"We don't sell data, so this doesn't apply."

Letting an ad platform use health-related data for targeting can count as a sale under this law.

Questions to bring back to your team

1 • Find the data

- ☐ Do we collect or process consumer health data as the Act defines it?
- ☐ Where does it come from: record, public website, intake forms, marketing, analytics, vendors?
- ☐ Who owns each of those systems, and is anyone outside compliance touching health data?

2 • Decide what is in scope

- ☐ Which of our data is PHI (exempt), and which is non-PHI health data that may be covered?
- ☐ Do we serve Washington residents, or collect or store data in Washington?

3 • Look at your website and tracking

- ☐ What tracking actually runs on our health-related pages right now?
- ☐ Does any of it fire before the visitor has consented?
- ☐ Where does that data go, and to which third parties or affiliates?

4 • Check your policy and obligations

- ☐ Do we have a separate, standalone consumer health data privacy policy, linked on our homepage?
- ☐ Does that policy match what our site actually does?
- ☐ Are we handling consent, consumer rights, sale/authorization, safeguards, vendors, and geofencing?

5 • Assign ownership

- ☐ Who owns the answer across privacy, legal, marketing, IT, and compliance?
- ☐ What is our plan, and who is accountable for the next step?

Start with one question.

Start by looking at your own website. Find out what tracking runs on your health-related pages, and where that data goes. Finding out is the first real step.

This handout is educational and is not legal advice. For your own organization, consult your attorney.

Learn more, Washington State Attorney General, My Health My Data:

atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy

Prepared by Sorticulture Systems · sorticulturesystems.com