MAY 2023

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Washington's New Health Care Data Law is Expansive and Takes Effect Soon. Are You Ready?

On April 27th, Washington State's governor signed the Washington State My Health My Data Act—a law the legislature nominally designed to increase healthcare privacy. But it does more than that. The law uses sweeping definitions and expansive provisions that will have ramifications for companies collecting biometric information, internet activity, or data that could identify someone as seeking to learn about (or improve) their health. And the stakes are high because of onerous obligations, unclear effective dates and a private right of action.

Key Takeaways

1. **The law applies to more than health data and Washington residents.** The law embraces a very broad view of health data and applies to information about individuals who do not reside in Washington—but whose health data is processed there. But B2B and employee information is not covered under the law.

2. **Companies need to be ready by July 2023.** Due to drafting quirks, some provisions may be taking effect as soon as July 2023.

3. **Washington courts will play a large role in determining the scope of the law.** The private right of action will invariably lead to more litigation than a regulator-enforced law, as we have seen with Illinois' biometric privacy law.

4. **Pixels and third-party cookies are risky.** Given the broad definition of "sale" and impractical steps needed to

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Josh Hansen
Associate
303.285.5306
jahansen@shb.com

authorize a sale, companies should be extra leery of any online-tracking tools that transfer data to a third party.

5. **Data retention becomes complicated.** Companies arguably need the consumer's consent to retain *or* delete data that is no longer necessary to provide a service/product the consumer requests.

Applicability

The law applies to a "regulated entity" that processes (collects, uses, stores, infers, sells, shares, etc.) "consumer health data" (1) in Washington or (2) in another state when the information concerns Washington residents. The law does not apply to B2B or employee data. Consumer health data is broadly defined to include any information that is linked/linkable to a consumer and identifies their past, present or future physical/mental health status. The law provides a laundry list of examples, which generally fall into four categories: (1) traditional health data (treatments, diseases, medications, symptoms, etc.); (2) precise geolocation (within 2,000 feet) that could reasonably indicate a consumer's attempt to obtain healthcare services/supplies; (3) genetic & biometric data; and (4) data that identifies a consumer seeking healthcare services (services to assess, measures, improve or learn about their health). So, for example, a person searching for diet tips, purchasing workout clothes or visiting a gym could all be data points connected to a person seeking healthcare services because they are trying to improve or learn about their health.

Obligations

A company will often need to get consent before processing data (with more onerous obligations for selling it), and there are new privacy-policy requirements (maybe even a brand new policy) and restrictions on geofencing around healthcare facilities.

- **Processing.** A company must obtain affirmative (*opt-in*) consent before processing any consumer health data beyond what is necessary to provide the consumer's requested service/product. [Think of this as an obligation to get consent before using data for a secondary purpose.] When requesting consent, companies (1) must explain what consumer health data they are processing, why they are processing it, and how to revoke consent; and (2) cannot infer, bundle or incorporate the consent into terms of use.

- **Disclosures.** Companies must obtain affirmative consent before sharing consumer health data with affiliates or third parties (excluding processors) beyond what is required to provide the consumer's requested service/product. [Again, think of this as disclosing data for a secondary purpose.] The consent must be separate from the consent for collection or

Camila Tobón
Partner
303.285.5318
ctobon@shb.com

Colman McCarthy
Partner
816.559.2081
cdmccarthy@shb.com

sales.

- **Sales.** Before a company can sell data, the consumer must provide a *written* and *signed* authorization that expires one year from the signature and describes various details (including the purchaser, data elements, uses). This authorization must be separate from consent for processing or disclosures. The definition of sale tracks the California Consumer Privacy Act's broad language: exchange for money or valuable consideration—so advertising cookies likely require authorization.

- **Transparency.** A company must post a link on its website to a policy—the "Consumer Health Data Privacy Policy"—that largely repeats details that will be in the company's existing privacy policy. It is unclear whether a company can combine this with a preexisting privacy policy.

- **Geofencing.** There is an *absolute* prohibition on geofencing around a healthcare facility when the geofence is designed to identify/track consumers seeking healthcare, collect consumer health data, or send messages or advertisements to consumers related to consumer health data or health care services.

- **Security.** Companies must adopt reasonable security measures, with the caveat that there are defined limitations on internal access: employees and processors can only access consumer health data that is necessary (1) for the purposes that the consumer consented or (2) to provide the consumer's requested product/service.

- **Contracting.** Companies must enter into a data processing agreement with processors. But the contract requirements generally track what we see in other comprehensive state privacy laws.

Rights

Consumers have enhanced access and deletion rights, and companies must honor those requests within 45 days while also offering an appeal process. The expanded access right includes the right to confirmation of processing as well as a list (with contact information) of third parties and affiliates who received the data. For deletion, there are very limited exceptions (fewer than in other privacy laws) and no exception for legal claims/compliance. A company who receives a deletion request must pass it through to anyone with whom it shared the data (including affiliates, processors and third parties), who then must also delete the data.

Exemptions

The most pertinent exemptions are for deidentified data, publically available data and data subject to the Health Insurance

Portability and Accountability Act, Gramm–Leach–Bliley Act, and Fair Credit Reporting Act (notably, these are not entity-level exemptions). Notably, there is no general carve out for legal compliance. Instead, there is a provision allowing use and disclosures for activities related to preventing fraud, security incidents or violations of federal or Washington law (not other states' laws)—but the company bears the burden of proving the exemption applies.

Enforcement

Individuals (via a private right of action) and the Washington State Attorney General can enforce the My Health My Data Act by bringing a claim under the Washington Consumer Protection Act. A violation of the My Health My Data Act establishes the first three elements of a Consumer Protection Act claim, which is sufficient for the Attorney General to obtain an injunction and litigation costs as well as a civil penalty of up to $7,500 per violation. But when an individual sues, they must also prove an injury (not necessarily monetary damages) and demonstrate the violation of the My Health My Data Act caused their injury. Upon such a showing, the plaintiff can obtain an injunction, litigation costs and damages (but not civil penalties). The court can triple an individual's damages, so long as the total amount stays under $25,000.

Effective Date

For everyone but small businesses, some provisions will likely take effect on July 22, 2023 with the rest becoming effective on March 31, 2024. [A small business is any entity who either (1) processes consumer health data on fewer than 100,000 consumers (remember: this is Washington residents or someone who has their covered data processed in the state) per year *or* (2) derives less than 50% of its revenue from selling/processing such data and sells/processes consumer health data on fewer than 25,000 consumers.]

- **Non-Small Businesses.** The uncertainty on effective dates comes from what appears to be a drafting error. The Senate amended the bill (which the House later adopted) with the stated goal of creating a 2024 effective date. But the legislature actually just inserted the 2024 date into the first paragraph of most sections—which means the other provisions technically go into effect on July 22, 2023 (the default rule is that new laws take effect 90 days after the legislative session concludes). The provisions that arguably go into effect this year cover issues such as restricting geofencing, limiting disclosures, providing the right to delete or withdraw consent and posting a privacy policy (although the obligation to actually have such a policy doesn't apply

until March 2024).

- **Small Businesses.** The legislature specified in most sections that small businesses must comply with that portion starting on June 30, 2024. But there is no effective date for the geofencing restriction, which means that provision takes effect on July 22, 2023.

The state legislature has adjourned for the year. So, barring a special session, any legislative fixes will have to wait until after many of the provisions arguably take effect.