ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

HB 3284: Contact Tracing & Exposure Notification Privacy

Background:

As technology continues to develop in new and innovative ways, it is our responsibility to update our privacy laws. That is why, in June of 2019, the Attorney General formed a Consumer Privacy Task Force to answer the growing call for comprehensive state consumer privacy legislation.

This Task Force has worked diligently on the development of comprehensive privacy legislation, and we will continue that work post-session. However, emerging issues related to COVID-19 created a pressing need for our task force to pivot our focus to data collection for contact tracing and exposure notification purposes. Thankfully, a subset of our task force members was willing to put in significant work over the last several months to develop policy that strictly protects our personal health data in this context.

While Oregon and federal law protect health information privacy in a variety of ways, those laws have limited application to contact tracing and exposure notification that occurs in the private sector. Without such protections, there's no assurance that this sensitive data won't end up in the hands of insurance companies, employers, creditors, identity thieves, or stalkers, to be used in ways that could harm individuals. That is why HB 3284 is a crucial bill for Oregonians, and one that we hope will serve as a model for other states.

Bill Summary:

Personal Health Data

HB 3284 provides a broad definition of personal health data. Personal health data is any information that identifies or can reasonably be used to identify an individual that is collected for the purpose of detecting, tracking, monitoring, or tracing an individual's exposure to or infection by COVID-19.

This includes information that can associate an individual with:

- Exposure to a person who has COVID-19;
- Development of symptoms;
- COVID-19 tests or examinations;
- Receipt of COVID-19-related medical care;
- Predisposition toward developing a disease condition that results from the exposure to or infection by COVID-19;

- Vaccine status; and
- Geolocation data and other data that can be used to track our exposure or infection.

Covered Organizations

HB 3284 applies to anyone who collects, uses or discloses personal health data or develops or operates a website, web application, mobile application to collect, use or disclose "personal health data" (as defined above).

Public health authorities, health care providers, and entities covered by HIPAA for HIPAA-covered activities are exempted from HB 3284.

Consent

HB 3284 prohibits covered organizations from collecting, using or disclosing personal health data without affirmative express consent. Affirmative express consent must be a clear and conspicuous act that specifically does not include acceptance of a general or broad terms of use document.

Additional provisions prohibit obtaining consent through the use of "dark patterns." A dark pattern is a user interface that has been designed to trick users into doing things, like buying or signing up for something they didn't mean to.

Covered organizations must provide a way to revoke consent once it has been given, after which personal health data may no longer be collected.

A parent or legal guardian may provide consent on behalf of a child under 14 years of age.

Limitations on Use

Under HB 3284, only the personal health data that is reasonably necessary to provide services to the consumer can be collected, used and disclosed. To put this into context, if you sign up to use a contact tracing application and provide affirmative express consent for your information to be used for contact tracing and exposure notification services, your personal health data can only be used to provide those services to you.

Additional provisions clarify that this data can only be used for the expressly authorized purpose. Here, HB 3284 provides some examples of prohibited uses of data, such as commercial advertising and the use of algorithms that are used to advertise to you in the future.

Protecting/Deleting Data

HB 3284 requires personal health data to be deleted 65 days after it has been collected, on a rolling basis. However, data can be retained if it has been deidentified and converted into statistical analyses, compilations, or interpretations (so the data cannot be traced back to an individual).

Additional provisions require covered organizations to:

- Take reasonable measures to ensure the accuracy of the data;
- Provide a method for correcting inaccuracies;
- Establish safeguards to protect the data from a data breach;
- Establish and implement policies that prevent the data from being used for a discriminatory purpose;
- Provide information to the consumer, including information about how to revoke consent, in transparent policies; and
- Maintain recordkeeping about how they have complied with the requirements of this law.

Exceptions

The Task Force recognized that there are circumstances where an organization is required to turn over data or information. For example, in response to a court order, a subpoena or a warrant. There are also circumstances where organizations must retain certain data to comply with a different federal or state law. HB 3284 includes exemptions for those situations.

Enforcement

Violation of this law is enforceable solely by the Attorney General under the Unlawful Trade Practices Act, ORS 646.605, *et. seq*.

Contact:
Kimberly McCullough, Legislative Director, 503-931-0418, kimberly.mccullough@doj.state.or.us
Kate Denison, Deputy Legislative Director, 971-599-9851, kate.e.denison@doj.state.or.us