HOUSE BILL REPORT
HB 1127

As Reported by House Committee On:
Health Care & Wellness

Title: An act relating to protecting the privacy and security of COVID-19 health data collected by entities other than public health agencies, health care providers, and health care facilities.

Brief Description: Protecting the privacy and security of COVID-19 health data collected by entities other than public health agencies, health care providers, and health care facilities.

Sponsors: Representatives Slatter, Boehnke, Valdez, Kloba, Graham, Macri and Pollet.

Brief History:
Committee Activity:
Health Care & Wellness: 1/28/21, 2/10/21 [DPS].

Brief Summary of Substitute Bill

- Restricts a covered organization's ability to collect, use, or disclose Coronavirus Disease 2019 (COVID-19) health data.
- Specifies prohibited purposes for collecting, using, or disclosing COVID-19 health data.
- Exempts COVID-19 health data from disclosure under the Public Records Act.

HOUSE COMMITTEE ON HEALTH CARE & WELLNESS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 13 members: Representatives Cody, Chair; Bateman, Vice Chair; Caldier, Assistant Ranking Minority Member; Bronoske, Davis, Harris, Macri, Riccelli, Rude, Simmons, Stonier, Tharinger and Ybarra.

Minority Report: Without recommendation. Signed by 2 members: Representatives Schmick, Ranking Minority Member; Maycumber.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Staff: Kim Weidenaar (786-7120).

Background:

Traditional Contact Tracing.
Case investigation and contact tracing are core public health strategies used to reduce the spread of communicable diseases, such as Coronavirus Disease 2019 (COVID-19), a novel acute respiratory syndrome coronavirus. Case investigation is the identification and investigation of patients with confirmed and probable diagnoses of a disease, which involves working with the patient who has been diagnosed with the disease to identify other people who may have been infected through exposure to the patient. Contact tracing is the subsequent identification, monitoring, and support of those contacts who have been exposed to, and possibly infected with, the virus. In Washington, local health departments, with the support of the Department of Health (DOH), are responsible for performing case investigations and contact tracing.

Use of Digital Technologies in Public Health Response.
A range of digital data sources have been used to enhance and interpret epidemiological data gathered by public-health authorities for COVID-19. Digital tools have been developed to track symptoms, individual locations, and notify individuals of exposure. These tools reduce reliance on human recall and may facilitate a pandemic response without relying on the resource constraints of traditional contact tracing. In the COVID-19 pandemic, digital exposure notification applications and other digital health tools have been developed for use in several countries and states.

In December 2020 the DOH launched an exposure notification technology known as WA Notify. Google and Apple jointly developed this smartphone technology, which will anonymously notify a user who has been in close contact with another user who tests positive for COVID-19. The technology does not know or track the identity of an individual or where they go, instead it uses message keys, which are exchanged as random anonymous codes with no identification or global positioning system (GPS) location data.

Consumer Protection Act.
The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General is authorized to investigate and prosecute claims under the CPA on behalf of the state or individuals in the state. A person injured by a violation of the CPA may bring a civil action for injunctive relief, recovery of actual damages, and reasonable attorneys' fees. The courts may increase awarded damages up to three times the actual damages sustained.

Uniform Health Care Information Act.
The state Uniform Health Care Information Act (UHCIA) governs the disclosure of health care information by health care providers and their agents or employees. The UHCIA provides that a health care provider may not disclose health care information about a patient

unless there is a statutory exception or written authorization by the patient.

Disclosure of Public Records.
The Public Records Act (PRA) requires state and local agencies to make all public records available for public inspection and copying, unless a record falls within an exemption in the PRA or another statute that exempts or prohibits disclosure of specific information or records. To the extent required to prevent an unreasonable invasion of personal privacy interests, an agency must delete identifying details when it makes a public record available. A person's right to privacy is violated only if disclosure would be highly offensive to a reasonable person and is not of legitimate concern to the public. The PRA is liberally construed and its exemptions narrowly construed.

Summary of Substitute Bill:

Limitations on Collection, Use, and Disclosure.
A covered organization must only collect, use, or disclose Coronavirus Disease 2019 (COVID-19) health data that is necessary, proportionate, and limited for a good-faith COVID-19 public health purpose. A covered organization must limit the collection, use, or disclosure of COVID-19 health data to the minimum level of identifiability and the amount necessary for a good faith COVID-19 public health purpose. A covered organization may only disclose COVID-19 health data to a government agency if the disclosure is to a public health agency and for a good-faith COVID-19 public health purpose, unless the information disclosed is protected under a state or federal privacy law that restricts redisclosure. A covered organization may not collect, use, or disclose an individual's COVID-19 health data unless the individual has given affirmative express consent. The COVID-19 health data may be collected, used, or disclosed to notify an employee or consumer of a potential exposure to COVID-19 while on a covered organization's premises or through an interaction with an employee or person acting on behalf of a covered organization without affirmative express consent.

Within 30 days of collecting COVID-19 health data, a covered organization must destroy the data or render it unlinkable in such a manner that is it impossible or demonstrably impracticable to identify any individual from the COVID-19 health data, unless required to retain data longer than 30 days by state or federal law. If data is retained longer than 30 days, it must be maintained in a confidential and secure manner and may not be redisclosed except as required by state or federal law.

A covered organization must also take reasonable measures to ensure the accuracy of COVID-19 health data and provide an easily accessible mechanism for an individual to correct the data within 30 days of receiving a request.

A covered organization may not collect, use, or disclose COVID-19 health data for any unauthorized purpose, including:

- commercial advertising or recommendation for electronic commerce;
- soliciting, selling, leasing, advertising, licensing, marketing, or otherwise commercially contracting for employment, finance, credit, insurance, housing, or education opportunities in a way that discriminates or makes opportunities unavailable on the basis of COVID-19 health data;
- segregating, discriminating, or otherwise making unavailable goods, services, facilities, privileges, or accommodations of any place of accommodation, except as authorized by the state or federal government for a COVID-19 public health purpose; and
- disclosing COVID-19 health data to any law enforcement or federal immigration authority or using COVID-19 health data for any law enforcement or immigration purpose.

A covered organization or service provider must establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of COVID-19 health data. A covered organization may not disclose identifiable COVID-19 health data to a service provider or a third party unless the service provider or third party is contractually bound to the same data privacy and security obligations as the covered organization.

Privacy Policy.
A covered organization must provide an individual a privacy policy that describes:
- the covered organization's data retention and security policies and practices;
- how and for what purposes the covered organization collects, uses, and discloses COVID-19 health data;
- recipients of COVID-19 health data and the purpose of the disclosure for each recipient; and
- how an individual may exercise their rights under the act.

The privacy policy must be disclosed to the individual before collecting COVID-19 health data and in a clear and conspicuous manner that is in the language in which the individual typically interacts with the covered organization.

Affirmative consent must be as easy to withdraw as it is to give. After an individual revokes consent, the covered organization must:
- stop collecting, using, or disclosing the individual's COVID-19 health data no later than seven days after receiving the revocation of consent;
- destroy or render unlinkable the individual's COVID-19 health data; and
- notify the individual if and for what purposes the covered organization collected, used, or disclosed the individual's COVID-19 health data before honoring the individual's revocation of consent.

Report.
A covered organization that collects, uses, or discloses COVID-19 health data of at least

30,000 individuals over 60 days must issue a public report at least once every 90 days. The report must be provided to the Department of Health (DOH), who must publish the report on the DOH's website. The report must:

- list the number of individuals whose COVID-19 health data was collected, used, or disclosed;
- describe the categories of COVID-19 data collected, used, and disclosed and the purpose for each category;
- describe the categories of recipients of the data and specific recipients; and
- not include any information that is linked or reasonably linked to a specific individual or device.

Definitions.

"Affirmative express consent" means an affirmative act by an individual that clearly and conspicuously communicates the individual's authorization of an act or practice and is made in the absence of any mechanism in the user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decision making or choice to obtain consent; and taken after the individual has been presented with a clear and conspicuous disclosure that is separate from other options or acceptance of general terms and that includes a concise and easy-to-understand description of each act or practice for which the individual's consent is sought.

"Covered organization" means any natural or legal person, or any legal, commercial, or governmental entity that:

- collects, uses, or discloses COVID-19 health data of Washington residents electronically or through communication by wire or radio for a COVID-19 public health purpose; or
- develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, mitigating, or otherwise responding to COVID-19 or the related public health response.

A "covered organization" does not include: a health care provider; a health care facility; a public health agency; the Department of Labor and Industries and an employer that is self-insured under Title 51 RCW, if the department or employer is collecting confidential claims files and records; the Long-Term Care Ombuds program; a "covered entity" or "business associate," for purposes of the federal Health Insurance Portability and Accountability Act of 1996 or person or entity acting in a similar capacity under the state's Uniform Health Care Information Act; a service provider; a person acting in their individual or household capacity; or person or entity that provides to a public health agency a mobile application or mobile operating system feature that transmits deidentified proximity data solely for the purpose of digitally notifying an individual who may have become exposed to COVID-19.

"COVID-19 health data" means data that is collected, used, or disclosed in connection with COVID-19 or the related public health response and that is linked to an individual or device

and includes:

- information that reveals the past, present, or future physical or behavioral health or condition of, or provision of health care to, an individual;
- data derived from the testing or examination of a body or bodily substance, or a request for such testing;
- information as to whether or not an individual has contracted or been tested for, or an estimate of the likelihood that a particular individual may contract, a disease or disorder;
- genetic data, biological samples, and biometric data;
- geolocation data and proximity data; and
- demographic data and contact information for identifiable individuals or a history of the individual's contacts over a period of time.

"COVID-19 health data" does not include:

- identifiable personal data collected and used for the purposes of human subjects research conducted in accordance with: the federal policy for the protection of human subjects; the good clinical practice guidelines issued by the international council for harmonization; or the federal regulations on the protection of human subjects;
- data that is deidentified in accordance with the deidentification requirements set forth in federal regulation and that is derived from protected health information data; or
- information used only for certain public health activities and purposes.

"COVID-19 public health purpose" means a purpose that seeks to support or evaluate public health activities related to COVID-19 including: preventing, detecting, and responding to COVID-19; creating emergency response plans; identifying population health trends; health surveillance; health assessments; implementing educational programs; program evaluation; developing and implementing policies; and determining needs for access to services and administering services.

Other.
A new chapter is created in Title 70 RCW. A violation of the chapter is considered an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of the Consumer Protection Act. The COVID-19 health data is exempt from public disclosure.

The act does not limit or prohibit a public health agency from administering contact tracing programs or activities, public health or scientific research conducted for a COVID-19 public health purpose, research, development, manufacture, or distribution of a drug, biological product, or vaccine associated with COVID-19, or a good faith response to a valid subpoena, court order, or other legal process.

The act expires on December 31, 2022.

Substitute Bill Compared to Original Bill:

The substitute bill:

- modifies the definition of "covered organization," so that for purposes of applying the provisions to a covered organization that collects, uses, or discloses COVID-19 health data electronically or through communication by wire or radio, the data must be collected, used, or disclosed for a COVID-19 public health purpose;
- exempts the following from a "covered organization" in addition to those that were already exempted: the Department of Labor and Industries and an employer that is self-insured under Title 51 RCW, if the department or employer is collecting data protected by specific statutory confidentiality provisions; the state Long-Term Care Ombuds program (also excluded from the definition of third party); and persons or entities acting in a similar capacity to a federal Health Insurance Portability and Accountability Act covered entity or business associate under the state Uniform Health Care Information Act;
- modifies the definition of "COVID-19 health data" so that it no longer includes data that is reasonably linked to an individual or device and data inferred or derived about the individual or device where such data is still linked or reasonably linked to the individual or device;
- exempts certain data that is deidentified in compliance with federal law and information that is only used for public health activities and purposes from the definition of "COVID-19 health data";
- modifies the definition of "health care facility" to include locations where related samples are collected;
- excludes the collection, use, and disclosure of COVID-19 health data from the express consent requirements if the data is necessary solely to notify an employee or consumer of their potential exposure;
- allows a covered organization to disclose COVID-19 health data if the disclosure is protected by a state or federal privacy law that restricts redisclosure;
- allows a covered organization to retain COVID-19 health data if data retention beyond 30 days is required by state or federal law, but requires that all data retained beyond 30 days must be maintained in a confidential and secure manner; and
- removes the provision that requires consent for any data that is provided in response to a legal or judicial process and provides that the act does not prohibit a good faith response to a valid subpoena or court order.

Appropriation: None.

Fiscal Note: Requested on January 19, 2021.

Effective Date of Substitute Bill: The bill contains an emergency clause and takes effect immediately.

Staff Summary of Public Testimony:

(In support) This bill is about saving lives by building trust so that we can use all tools to combat this virus. This bill is not intended to be a precedent-setting privacy bill. Throughout the process, many different groups have been consulted as this bill was written. The COVID-19 virus thrives on social connection and digital tools can help us recognize when we have been exposed so that we can isolate ourselves and stop the spread.

The protections included in the WA Notify application have been built into this bill as other digital tools may not include these protections. One of the biggest barriers to people using these digital tools is a lack of trust in government and big tech and without this trust the tools will not be used. If this bill can offer reassurance to one person that their data is protected and will not be used for other purposes, then this bill has the power to save lives. This is a time when we need to be extra vigilant. This bill tries to strike a balance between encouraging the use of all tools while also protecting civil liberties. This bill is narrowly targeted and ends in 2022. There have been some amendment requests for those that are already covered by a privacy law.

We are all in this together to try to stop this virus and save lives. Bringing in parties of all sides when it comes to privacy regulation is very important and the sponsor has done that on this bill. This bill is will build trust and ensure that individuals' information will not continue to be tracked. An individual can limit what information they want to share, but it also allows information to be tracked and shared with those that can quickly respond to the outbreak.

This is a common-sense privacy bill that gives consumers confidence that their data will be kept private. However, the Long-Term Care Ombuds program requests a small amendment. Long-term care has significant COVID-19 health data because it has been hit particularly hard by COVID-19. The Long-Term Care Ombuds program is not a state agency, but is already governed by stricter state and federal privacy laws and so requests that it be exempted from the provisions of this bill.

(Opposed) None.

(Other) The sponsor reached out to the business community early on this bill, which is appreciated. This bill attempts to strike a balance between innovative tools and public safety. However, it creates a unique problem for employers. If an employee is exposed to COVID-19 the employer will want to notify the employee of the exposure. However, requiring affirmative consent is burdensome and if consent is not given the employer likely cannot remove the person from the workplace, which creates an unsafe workplace. This also creates a problem when dealing with customers. Oregon has a similar contact tracing bill that recognizes the idea that employers are in a different situation with consent and that it makes sense to provide workplaces an exemption so that employees and consumers may

be notified of any exposure. Accordingly, the business community would like an exemption for employer and customer safety.

This bill also excludes public health authorities who are the primary holders of this data.

Persons Testifying: (In support) Representative Slatter, prime sponsor; Representative Boehnke; and Melanie Smith, Washington State Long-Term Care Ombuds Program.

(Other) Robert Battles, Association of Washington Business; and Andrew Kingman, State Privacy and Security Coalition.

Persons Signed In To Testify But Not Testifying: None.