FINAL BILL REPORT
2SHB 1127

FULL VETO
Synopsis as Enacted

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: House Committee on Appropriations (originally sponsored by Representatives Slatter, Boehnke, Valdez, Kloba, Graham, Macri and Pollet).

House Committee on Health Care & Wellness
House Committee on Appropriations
Senate Committee on Health & Long Term Care
Senate Committee on Environment, Energy & Technology
Senate Committee on Ways & Means

Background:

Traditional Contact Tracing.
Case investigation and contact tracing are traditional 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 individuals with confirmed and probable diagnoses of a disease, which involves working with the individual who has been diagnosed with the disease to identify other people who may have been infected through exposure to the individual. Contact tracing is the subsequent identification, monitoring, and support of those contacts who have been exposed to, and possibly infected with, the virus. 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. During the COVID-19 pandemic, digital exposure notification applications and other digital

---

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.

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.

Summary:

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. 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 them 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 are retained longer than 30 days, they 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 a local, 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.

Other than the Department of Social and Health Services and the Medicaid Fraud Division of the Attorney General's Office, general authority and limited authority Washington law enforcement agencies and federal immigration authorities may not collect, use, or disclose COVID-19 health data for the purpose of enforcing criminal or civil law.

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), which must publish the report on the DOH's website. The report must:

- list the number of individuals whose COVID-19 health data were 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.

"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 or facility; a public health agency; the Department of Labor and Industries (L&I) and an employer that is self-insured if the L&I or employer is collecting confidential claims files and records; the L&I for purposes of administering the Washington Industrial Safety and Health Act; the Long-Term Care Ombuds program; a "covered entity" or "business associate," for purposes of the federal Health Insurance Portability and Accountability Act (HIPAA) 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 are collected, used, or disclosed in connection with COVID-19 or the related public health response and that are 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 are deidentified in accordance with federal HIPAA deidentification requirements and that are derived from protected health information data; or
- information used only for public health activities and purposes as defined by federal HIPAA rules.

"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 violation of the act is considered an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of the Consumer Protection Act, for which the Attorney General's has sole enforcement authority. The COVID-19 health data are 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; a good faith response to a valid subpoena, court order, or other legal process; or the Medicaid Fraud Division of the Attorney General's Office from collecting, using, or disclosing COVID-19 health data for the enforcement of criminal and civil law.

The act expires on December 31, 2022.

Votes on Final Passage:

House	76	21	
Senate	28	20	(Senate amended)
House	83	13	(House concurred)