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; amending RCW 42.56.360; adding a new chapter to Title 70 RCW; providing an expiration date; and declaring an emergency.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Sec. 1. (1) The legislature finds that the public health system must use all available and effective tools to prevent the spread of the novel coronavirus COVID-19 and save lives in Washington. Public health case investigation, testing, and contact tracing are traditional, trusted public health tools used to control the spread of communicable diseases and are subject to laws and policies protecting health information privacy. As the economy reopens, the staggering number of COVID-19 cases continue to test capacity of the public health system's ability to control COVID-19. In an effort to increase the system's capacity, academic institutions and technology companies have recently developed digital tools, including web and mobile applications, to assist local and state public health agencies with contact tracing efforts.

(2) The legislature finds that it is imperative to strike a balance between supporting innovative tools that increase the public
health system's capacity while also providing equitable protections for the privacy and security of individual's COVID-19 health data and assuring individuals that collected data will not be used for law enforcement or immigration purposes. Achieving this balance is critical to reassure every Washingtonian, that any data collected by digital tools will be used in a private, secure, and legitimate manner and to support the use of all available tools to reduce the spread of COVID-19, particularly among vulnerable populations, and save lives in Washington.

(3) Therefore, the legislature intends to establish privacy and security standards for these digital tools to provide protections for all Washingtonian's COVID-19 health data.

NEW SECTION. Sec. 2. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1)(a) "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:
   (i) 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
   (ii) 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.
   (b) For purposes of (a) of this subsection, affirmative express consent may not be inferred from the inaction of an individual or the individual's continued use of a service or product.
   (c) Affirmative express consent must be freely given and nonconditioned.

(2)(a) "Biometric data" means any information, regardless of how it is captured, converted, or stored, that is:
   (i) Based on an individual's unique biological characteristics, such as a retina or iris scan, fingerprint, voiceprint, a scan of hand or face geometry, or other unique biological patterns or characteristics; and
   (ii) Used to identify a specific individual.
   (b) "Biometric data" does not include:
Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, thermal images, or physical descriptions such as height, weight, hair color, or eye color;

(ii) Donated organ tissues or parts, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency;

(iii) Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996; or

(iv) X-ray, roentgen process, computed tomography, magnetic resonance imaging, positron emission tomography scan, mammography, or other image or film of the human anatomy used to diagnose, develop a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Collect" means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring COVID-19 health data in any manner by a covered organization, including by passively or actively observing the behavior of an individual.

"Covered organization" means any person, including a government entity, that:

(i) 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

(ii) 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.

"Covered organization" does not include:

(i) A health care provider;

(ii) A health care facility;

(iii) A public health agency;

(iv) The department of labor and industries and an employer that is self-insured under Title 51 RCW, if the department of labor and industries or employer is collecting data protected by RCW 51.28.070; or

(v) The state long-term care ombuds program;
A person or entity acting as a "covered entity" or "business associate," as those terms are defined in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996 or a person or entity acting in a similar capacity under chapter 70.02 RCW;

(vii) A service provider;

(viii) A person acting in their individual or household capacity;

or

(ix) A 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. A person or entity that provides such mobile application or mobile operating system feature to any person or entity other than a public health agency is a covered organization. A person or entity that transmits or uses deidentified proximity data for any purpose other than COVID-19 exposure notification is a covered organization.

(5) "COVID-19" means a respiratory disease caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).

(6)(a) "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.

(b) "COVID-19 health data" includes, but is not limited to:

(i) Information that reveals the past, present, or future physical or behavioral health or condition of, or provision of health care to, an individual;

(ii) Data derived from the testing or examination of a body or bodily substance, or a request for such testing;

(iii) 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;

(iv) Genetic data and biological samples;

(v) Biometric data;

(vi) Geolocation data;

(vii) Proximity data;

(viii) Demographic data; and

(ix) Contact information for identifiable individuals or a history of the individual's contacts over a period of time, such as an address book or call log.

(c) "COVID-19 health data" does not include:
(i) 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, 45 C.F.R. Part 46; the good clinical practice guidelines issued by the international council for harmonization; or the federal regulations on the protection of human subjects under 21 C.F.R. Parts 50 and 56;

(ii) Data that is deidentified in accordance with the deidentification requirements set forth in 45 C.F.R. Sec. 164.514 and that is derived from protected health information data subject to one of the standards set forth in (c)(i) of this subsection; or

(iii) Information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512.

(7) "COVID-19 public health purpose" means a purpose that seeks to support or evaluate public health activities related to COVID-19 including, but not limited to, 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.

(8) "Demographic data" means information relating to the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity, sexual orientation, age, tribal affiliation, disability, domicile, employment status, familial status, immigration status, or veteran status of an individual or group of individuals.

(9) "Device" means any electronic equipment that is primarily designed for or marketed to consumers.

(10) "Disclose" or "disclosure" means the releasing, transferring, selling, providing access to, licensing, or divulging in any manner of COVID-19 health data by a covered organization to a third party.

(11) "Federal immigration authority" means any officer, employee, or person otherwise paid by or acting as an agent of the United States department of homeland security, including but not limited to its subagencies, immigration and customs enforcement and customs and border protection, and any present or future divisions thereof, charged with immigration enforcement.

(12) "Geolocation data" means data capable of determining the past or present precise physical location of an individual at a specific point in time, taking account of population densities,
including cell site location information, triangulation data derived from nearby wireless or radio frequency networks, and global positioning system data.

(13) "Health care facility" means a hospital, clinic, nursing home, psychiatric hospital, ambulatory surgical center, pharmacy, laboratory, testing site including a temporary or community-based site and locations where related samples are collected, office, or similar place where a health care provider provides health care to patients.

(14) "Health care provider" means a person who is licensed, certified, registered, or otherwise authorized by state law to provide health care in the ordinary course of business or practice of a profession.

(15) "Individual" means a natural person who is a Washington resident.

(16) "Law enforcement officer" means a law enforcement officer as defined in RCW 9.41.010 or a federal peace officer as defined in RCW 10.93.020.

(17) "Person" means a natural or legal person, or any legal, commercial, or governmental entity of any kind or nature.

(18) "Proximity data" means information that identifies or estimates the past or present physical proximity of one individual or device to another, including information derived from Bluetooth, audio signatures, nearby wireless networks, and near-field communications.

(19) "Public health agency" means an agency or authority of the state, political subdivision of the state, or an Indian tribe that is responsible for public health matters as part of its official mandate, or a person or entity acting under a grant of authority from or contract with such public agency. "Public health agency" includes the department of health, the state board of health, local health departments, local boards of health, health districts, and sovereign tribal nations.

(20)(a) "Service provider" means a person that collects, uses, or discloses COVID-19 health data for the purpose of performing a service or function on behalf of, for the benefit of, under instruction of, and under contractual agreement with a covered organization, but only to the extent that the collection, use, or disclosure relates to the performance of such service or function.
(b) "Service provider" excludes a person that develops or operates a website, web application, mobile application, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, mitigating, or otherwise responding to COVID-19.

(21)(a) "Third party" means a person to whom a covered organization discloses COVID-19 health data, or a corporate affiliate or a related party of a covered organization that does not have a direct relationship with an individual with whom the COVID-19 health data is linked or is reasonably linkable.

(b) "Third party" excludes a public health agency, the state long-term care ombuds program, or a service provider of a covered organization.

(22) "Use" means the processing, employment, application, utilization, examination, or analysis of COVID-19 health data by a covered organization.

NEW SECTION. Sec. 3. (1)(a) A covered organization shall provide to an individual a privacy policy that describes, at a minimum:

(i) The covered organization's data retention and data security policies and practices for COVID-19 health data;

(ii) How and for what purposes the covered organization collects, uses, and discloses COVID-19 health data;

(iii) The recipients to whom the covered organization discloses COVID-19 health data and the purpose of disclosure for each recipient; and

(iv) How an individual may exercise their rights under this chapter.

(b) A privacy policy required under (a) of this subsection must be disclosed to an individual in a clear and conspicuous manner, in the language in which the individual typically interacts with the covered organization, and prior to or at the point of the collection of COVID-19 health data.

(2)(a) A covered organization may not collect, use, or disclose COVID-19 health data unless the individual to whom the data pertains has given affirmative express consent to the collection, use, or disclosure.

(b) (a) of this subsection does not apply to the collection, use, or disclosure of COVID-19 health data that is necessary solely to
notify an employee or consumer of their 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.

(3) An affirmative express consent must be as easy to withdraw as it is to give. A covered organization shall provide an effective mechanism for an individual to revoke consent after it is given. After an individual revokes consent, the covered organization shall:

(a) Stop collecting, using, or disclosing the individual's COVID-19 health data no later than seven days after the receipt of the individual's revocation of consent;
(b) Destroy or render unlinkable the individual's COVID-19 health data under the same procedures as in section 4(4) of this act; and
(c) 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.

NEW SECTION. Sec. 4. (1) A covered organization shall:

(a) Collect, use, or disclose only COVID-19 health data that is necessary, proportionate, and limited for a good-faith COVID-19 public health purpose, including a service or feature to support a good-faith COVID-19 public health purpose;
(b) Limit the collection, use, or disclosure of COVID-19 health data to the minimum level of identifiability and the amount of data necessary for a good-faith COVID-19 public health purpose;
(c) Take reasonable measures to ensure the accuracy of COVID-19 health data, provide an easily accessible and effective mechanism for an individual to correct inaccurate information, and comply with an individual's request to correct COVID-19 health data no later than 30 days after receiving the request;
(d) Adopt reasonable safeguards to prevent unlawful discrimination on the basis of COVID-19 health data; and
(e) Only disclose COVID-19 health data to a government entity when the disclosure is to a public health agency and is made solely for good-faith COVID-19 public health purposes, unless the information disclosed is protected under a state or federal privacy law that restricts redisclosure.

(2) A covered organization may not collect, use, or disclose COVID-19 health data for any purpose not authorized in this act, including:
(a) Commercial advertising, recommendation for e-commerce, or the training of machine-learning algorithms related to, or subsequently for use in, commercial advertising or e-commerce;

(b) Soliciting, offering, selling, leasing, licensing, renting, advertising, marketing, or otherwise commercially contracting for employment, finance, credit, insurance, housing, or education opportunities in a manner that discriminates or otherwise makes opportunities unavailable on the basis of COVID-19 health data;

c) Segregating, discriminating in, or otherwise making unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation, except as authorized by a federal or state government entity for a COVID-19 public health purpose; and

d) Disclosing COVID-19 health data to any law enforcement officer or federal immigration authority or using COVID-19 health data for any law enforcement or immigration purpose.

(3) A law enforcement officer or a federal immigration authority may not collect or use COVID-19 health data when acting in their official, rather than individual or household, capacity.

(4) No later than 30 days after collection, COVID-19 health data must be destroyed or rendered unlinkable in such a manner that it is impossible or demonstrably impracticable to identify any individual from the COVID-19 health data, unless data retention beyond 30 days is required by state or federal law. All COVID-19 health data retained beyond 30 days must be maintained in a confidential and secure manner and may not be redisclosed except as required by state or federal law.

(5) A covered organization may not disclose identifiable COVID-19 health data to a service provider or a third party unless that service provider or third party is contractually bound to the covered organization to meet the same data privacy obligations as the covered organization.

NEW SECTION. Sec. 5. (1) A covered organization or service provider shall establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of COVID-19 health data.

(2) A covered organization may not disclose identifiable COVID-19 health data to a third party unless that third party is contractually
bound to the covered organization to meet the same data security obligations as the covered organization.

NEW SECTION.  Sec. 6.  (1) A covered organization that collects, uses, or discloses COVID-19 health data of at least 30,000 individuals over 60 calendar days shall issue a public report at least once every 90 days. The public report must:

(a) State in aggregate terms the number of individuals whose COVID-19 health data the covered organization collected, used, or disclosed to the extent practicable;

(b) Describe the categories of COVID-19 health data collected, used, or disclosed and the purposes for which each category of COVID-19 health data was collected, used, or disclosed;

(c) Describe the categories of recipients to whom COVID-19 health data was disclosed and list specific recipients of COVID-19 health data within each category.

(2) The public report required under subsection (1) of this section may not contain any information that is linked or reasonably linkable to a specific individual or device or that may be used to identify or reidentify a specific individual or device.

(3) A covered organization subject to the public report requirement under subsection (1) of this section shall provide a copy of the public report to the department of health. The department of health shall publish all received reports on its public website.

(4) Nothing in this section requires a covered organization to:

(a) Take an action that would convert data that is not COVID-19 health data into COVID-19 health data;

(b) Collect or maintain COVID-19 health data that the covered organization would otherwise not maintain; or

(c) Maintain COVID-19 health data longer than the covered organization would otherwise maintain such data.

NEW SECTION.  Sec. 7.  (1) Nothing in this act limits or prohibits a public health agency from administering programs or activities to identify individuals who have contracted, or may have been exposed to, COVID-19 through interviews, outreach, case investigation, and other recognized investigatory measures by a public health agency or its designated agent intended to monitor and mitigate the transmission of a disease or disorder.
(2) Nothing in this act limits or prohibits public health or scientific research conducted for COVID-19 public health purposes by:
   (a) A public health agency;
   (b) A nonprofit corporation or a public benefit nonprofit corporation, as defined in RCW 24.03.005; or
   (c) An institution of higher education, as defined in RCW 28B.92.030.

(3) Nothing in this chapter limits or prohibits research, development, manufacture, or distribution of a drug, biological product, or vaccine that relates to a disease or disorder that is associated or potentially associated with COVID-19.

(4) Nothing in this act prohibits a good faith response to, or compliance with, otherwise valid subpoenas, court orders, or other legal processes.

NEW SECTION. Sec. 8. (1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

   (2) This chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

Sec. 9. RCW 42.56.360 and 2020 c 323 s 2 are each amended to read as follows:

   (1) The following health care information is exempt from disclosure under this chapter:

   (a) Information obtained by the pharmacy quality assurance commission as provided in RCW 69.45.090;
   (b) Information obtained by the pharmacy quality assurance commission or the department of health and its representatives as provided in RCW 69.41.044, 69.41.280, and 18.64.420;
   (c) Information and documents created specifically for, and collected and maintained by a quality improvement committee under RCW 43.70.510, 70.230.080, or 70.41.200, or by a peer review committee under RCW 4.24.250, or by a quality assurance committee pursuant to RCW 74.42.640 or 18.20.390, or by a hospital, as defined in RCW
43.70.056, for reporting of health care-associated infections under
RCW 43.70.056, a notification of an incident under RCW 70.56.040(5),
and reports regarding adverse events under RCW 70.56.020(2)(b),
regardless of which agency is in possession of the information and
documents;

(d)(i) Proprietary financial and commercial information that the
submitting entity, with review by the department of health,
specifically identifies at the time it is submitted and that is
provided to or obtained by the department of health in connection
with an application for, or the supervision of, an antitrust
exemption sought by the submitting entity under RCW 43.72.310;

(ii) If a request for such information is received, the
submitting entity must be notified of the request. Within ten
business days of receipt of the notice, the submitting entity shall
provide a written statement of the continuing need for
confidentiality, which shall be provided to the requester. Upon
receipt of such notice, the department of health shall continue to
treat information designated under this subsection (1)(d) as exempt
from disclosure;

(iii) If the requester initiates an action to compel disclosure
under this chapter, the submitting entity must be joined as a party
to demonstrate the continuing need for confidentiality;

(e) Records of the entity obtained in an action under RCW
18.71.300 through 18.71.340;

(f) Complaints filed under chapter 18.130 RCW after July 27,
1997, to the extent provided in RCW 18.130.095(1);

(g) Information obtained by the department of health under
chapter 70.225 RCW;

(h) Information collected by the department of health under
chapter 70.245 RCW except as provided in RCW 70.245.150;

(i) Cardiac and stroke system performance data submitted to
national, state, or local data collection systems under RCW
70.168.150(2)(b);

(j) All documents, including completed forms, received pursuant
to a wellness program under RCW 41.04.362, but not statistical
reports that do not identify an individual;

(k) Data and information exempt from disclosure under RCW
43.371.040; and

(l) Medical information contained in files and records of members
of retirement plans administered by the department of retirement
systems or the law enforcement officers' and firefighters' plan 2 retirement board, as provided to the department of retirement systems under RCW 41.04.830.

(2) Chapter 70.02 RCW applies to public inspection and copying of health care information of patients.

(3)(a) Documents related to infant mortality reviews conducted pursuant to RCW 70.05.170 are exempt from disclosure as provided for in RCW 70.05.170(3).

(b)(i) If an agency provides copies of public records to another agency that are exempt from public disclosure under this subsection (3), those records remain exempt to the same extent the records were exempt in the possession of the originating entity.

(ii) For notice purposes only, agencies providing exempt records under this subsection (3) to other agencies may mark any exempt records as "exempt" so that the receiving agency is aware of the exemption, however whether or not a record is marked exempt does not affect whether the record is actually exempt from disclosure.

(4) Information and documents related to maternal mortality reviews conducted pursuant to RCW 70.54.450 are confidential and exempt from public inspection and copying.

(5) COVID-19 health data, as defined in section 2 of this act, is exempt from disclosure under this chapter.

NEW SECTION. Sec. 10. Sections 1 through 8 of this act constitute a new chapter in Title 70 RCW.

NEW SECTION. Sec. 11. This act expires December 31, 2022.

NEW SECTION. Sec. 12. This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately.

--- END ---