

Enrolled **House Bill 3284**

Sponsored by Representative HOLVEY; Representatives MARSH, REARDON (at the request of Attorney General Ellen Rosenblum)

CHAPTER

AN ACT

Relating to protecting the privacy of the personal health data of residents of this state; creating new provisions; amending ORS 646.607; and declaring an emergency.

Be It Enacted by the People of the State of Oregon:

SECTION 1. (1) As used in this section:

(a)(A) “Affirmative express consent” means an affirmative act by a resident individual that clearly and conspicuously communicates the resident individual’s authorization for a covered organization to perform an act or practice.

(B) “Affirmative express consent” does not include a resident individual’s acceptance of a general or broad terms of use document, or similar document, that contains descriptions of personal health data collection along with other unrelated information.

(b)(A) “Covered organization” means a person that collects, uses or discloses personal health data or that develops or operates a website, web application, mobile application, mobile operating system feature or other electronic method by means of which the person may collect, use or disclose personal health data.

(B) “Covered organization” does not include:

(i) A member of the resident individual’s household;

(ii) An agency, employee, agent, designee, affiliate, associate or contractor of a federal, state, local or tribal governmental body that under legal authorization and for public health purposes, including preventing disease, injury or disability, may collect, receive, observe, discover or investigate personal health data;

(iii) A health care provider, as defined in ORS 433.443; or

(iv) A covered entity or business associate, both as defined in 45 C.F.R. 160.103, as in effect on the effective date of this 2021 Act, to the extent that the covered entity or business associate is engaged in activities that are subject to regulation under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, or regulations adopted under the Act and codified as 45 C.F.R. parts 160 and 164, as in effect on the effective date of this 2021 Act.

(c) “Disclose” means to release, transfer, sell, share, provide access to, license or otherwise divulge to another person.

(d) “Emergency period” means a period that begins on the date on which the Governor has declared an emergency related to the COVID-19 pandemic and ends on a date 180 days after the Governor terminates the declaration or the declaration expires.

(e)(A) “Geolocation data” means information generated by or derived from technology that directly identifies the location of a natural person within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, including but not limited to:

- (i) Level latitude and longitude coordinates from a global positioning system;
- (ii) Cell site-location information; and
- (iii) Triangulation data derived from nearby wireless or radio frequency networks.

(B) “Geolocation data” does not include the content of communications.

(f)(A) “Personal health data” means information that is collected for the purpose of tracking, monitoring or tracing exposures to or infections by SARS-CoV-2 or development of disease conditions caused by or related to COVID-19 and that identifies or can reasonably be used to identify a resident individual and associate the resident individual’s personal identity with:

- (i) Exposure to or infection by SARS-CoV-2 or development of symptoms of or a disease condition caused by or related to COVID-19;
- (ii) Tests or examinations or requests for tests and examinations for exposure to SARS-CoV-2, including tests or examinations of body parts or bodily substances;
- (iii) Receipt of medical care or medical services related to exposure to SARS-CoV-2 or symptoms or development of COVID-19;
- (iv) Predisposition toward developing a disease condition that results from exposure to or infection by SARS-CoV-2;
- (v) Whether the resident individual has received a vaccination against COVID-19; or
- (vi) Other data, including geolocation data, that tracks, monitors or traces a resident individual’s exposure to or infection by SARS-CoV-2 or development of a disease condition caused by or related to COVID-19.

(B) “Personal health data” does not include information about a resident individual that:

- (i) Is lawfully available to the public from federal, state or local government records or widely available to the public from sources such as telephone directories, the internet, news media or similar or related sources;
- (ii) Was collected before the emergency period for purposes other than tracking, monitoring or tracing a resident individual’s exposure to or infection by SARS-CoV-2 or development of a disease condition caused by or related to COVID-19;
- (iii) Has been deidentified in accordance with 45 C.F.R. 164.514(b), as in effect on the effective date of this 2021 Act;

(iv) Was collected in an employment context; or

(v) Is collected after the expiration or termination of the emergency period.

(g) “Resident individual” means a natural person who resides in this state.

(h) “Service provider” means a person that collects, uses or discloses personal health data solely for the purpose of providing business services to, on behalf of, or for the benefit of a covered organization in accordance with instructions or direction from, or under the terms and conditions of a contract with, the covered organization.

(2)(a) Except as provided in paragraph (b) of this subsection, a covered organization may not collect, use or disclose personal health data about a resident individual who has not given affirmative express consent to the covered organization’s collection, use or disclosure of the resident individual’s personal health data. In obtaining affirmative express consent from a resident individual, a covered organization may not:

(A) Use a method that is designed with the purpose of, or that has the substantial effect of, subverting or impairing a resident individual’s decision-making or choice; and

(B) Infer consent from a resident individual’s inaction.

(b) A covered organization may collect, use or disclose personal health data without a resident individual’s affirmative express consent if the collection, use or disclosure is necessary solely to comply with a legal obligation.

(3) A resident individual may give affirmative express consent to a collection, use or disclosure of personal health data on behalf of another resident individual who is younger than 14 years of age if the resident individual is a parent or legal guardian of the other resident individual.

(4)(a) Except as provided in paragraph (b) of this subsection, a covered organization may not retain, store or use and shall destroy, delete or, if appropriate, render inaccessible to any person in any manner personal health data that the covered organization collects, stores, uses, possesses or controls not later than 65 days after the covered organization collected, received or otherwise obtained the personal health data.

(b) A covered organization may use and need not destroy, delete or render inaccessible personal health data if:

(A) The personal health data consists of aggregations, statistical analyses, compilations or interpretations; and

(B) The covered organization deidentifies the personal health data in accordance with 45 C.F.R. 164.514(b), as in effect on the effective date of this 2021 Act.

(5) A covered organization shall collect, use, receive, process, examine, disclose or collate only personal health data that is reasonably necessary to provide services to the resident individual to whom the personal health data applies, and shall:

(a) Take reasonable measures to ensure the accuracy of the personal health data and provide an accessible and effective method for a resident individual to correct any inaccuracies, as appropriate for the nature of the personal health data and the context in which the covered organization collected or received the personal health data;

(b) Establish and implement safeguards for personal health data that comply, at a minimum, with the requirements of ORS 646A.622 and require service providers by contract to comply with this section and the requirements of ORS 646A.622;

(c) Establish and implement policies and procedures that prevent the covered organization from using personal health data for any discriminatory purpose;

(d) Provide an easily accessible and effective method by which a resident individual may revoke any affirmative express consent the resident individual gave previously;

(e) Adopt, implement and provide to each resident individual from whom the covered organization collects, or about whom the covered organization receives, personal health data a clear, understandable and conspicuous disclosure of policies and procedures in compliance with which the covered organization collects, receives or otherwise obtains personal health data that, at a minimum, must include:

(A) The manner in which and the purposes for which the covered organization collects, receives, processes, examines, analyzes, collates, discloses, transfers, stores, retains or makes use of personal health data;

(B) Categories of persons to which the covered organization does or may disclose personal health data or from which the covered organization does or may receive or obtain personal health data; and

(C) A statement that informs the resident individual that and how the resident individual may provide, refuse to provide or revoke affirmative express consent;

(f) Cease the covered organization's collection, receipt or use of a resident individual's personal health data not later than 21 days after receiving from the resident individual a revocation of affirmative express consent; and

(g) Compile, not later than 30 days after the effective date of this 2021 Act and during each period of 60 days thereafter, and retain for a period of not less than five years after the expiration or termination of the emergency period, subject to an audit by the Oregon Health Authority, a series of reports that:

(A) States the number of resident individuals from or about whom the covered organization collected, received or otherwise obtained personal health data;

(B) Describes the categories of personal health data the covered organization collected, received or otherwise obtained and the specific purpose for which the covered organization collected, received or obtained the personal health data; and

(C) Lists the persons to which the covered organization disclosed, sold or otherwise transferred personal health data.

(6) A covered organization may not collect, use or disclose personal health data for a purpose that this section does not expressly authorize, including for:

(a) Commercial advertising;

(b) Recommendations or reviews related to electronic commerce; or

(c) Training machine learning algorithms related to or for subsequent use in commercial advertising or electronic commerce.

(7) This section does not limit or prohibit:

(a) A university or other institution of higher education or a nonprofit corporation, as defined in ORS 65.001, from conducting scientific research or a public health program or from developing vaccinations, medications or treatments related to COVID-19 that are otherwise authorized by law;

(b) A covered organization from complying with a federal or state law, a court order, subpoena or other legal process that requires the covered organization or a service provider to disclose personal health data; or

(c) A covered organization from maintaining, retaining or storing other information in compliance with federal or state law.

(8) This section does not modify or affect a covered organization's obligation to comply with the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as in effect on the effective date of this 2021 Act, with regulations adopted under the Act or with ORS 192.553 to 192.581, if applicable.

(9) A covered organization's violation of a provision of this section is an unlawful practice under ORS 646.607.

SECTION 2. ORS 646.607 is amended to read:

646.607. A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person:

(1) Employs any unconscionable tactic in connection with selling, renting or disposing of real estate, goods or services, or collecting or enforcing an obligation.

(2) Fails to deliver all or any portion of real estate, goods or services as promised, and at a customer's request, fails to refund money that the customer gave to the person to purchase the undelivered real estate, goods or services and that the person does not retain pursuant to any right, claim or defense the person may assert in good faith. This subsection does not create a warranty obligation and does not apply to a dispute over the quality of real estate, goods or services delivered to a customer.

(3) Violates ORS 401.965 (2).

(4) Violates a provision of ORS 646A.725 to 646A.750.

(5) Violates ORS 646A.530.

(6) Employs a collection practice that is unlawful under ORS 646.639.

(7) Is a beneficiary that violates ORS 86.726 (1)(a) or (2), 86.729 (4) or 86.732 (1) or (2).

(8) Violates ORS 646A.093.

(9) Violates a provision of ORS 646A.600 to 646A.628.

(10) Violates ORS 646A.808 (2).

(11) Violates ORS 336.184.

(12) Publishes on a website related to the person's business, or in a consumer agreement related to a consumer transaction, a statement or representation of fact in which the person asserts that the person, in a particular manner or for particular purposes, will use, disclose, collect, maintain, delete or dispose of information that the person requests, requires or receives from a consumer and

the person uses, discloses, collects, maintains, deletes or disposes of the information in a manner that is materially inconsistent with the person's statement or representation.

(13) Violates ORS 646A.813 (2).

(14) Violates section 1 of this 2021 Act.

SECTION 3. ORS 646.607, as amended by section 2 of this 2021 Act, is amended to read:

646.607. A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person:

(1) Employs any unconscionable tactic in connection with selling, renting or disposing of real estate, goods or services, or collecting or enforcing an obligation.

(2) Fails to deliver all or any portion of real estate, goods or services as promised, and at a customer's request, fails to refund money that the customer gave to the person to purchase the undelivered real estate, goods or services and that the person does not retain pursuant to any right, claim or defense the person may assert in good faith. This subsection does not create a warranty obligation and does not apply to a dispute over the quality of real estate, goods or services delivered to a customer.

(3) Violates ORS 401.965 (2).

(4) Violates a provision of ORS 646A.725 to 646A.750.

(5) Violates ORS 646A.530.

(6) Employs a collection practice that is unlawful under ORS 646.639.

(7) Is a beneficiary that violates ORS 86.726 (1)(a) or (2), 86.729 (4) or 86.732 (1) or (2).

(8) Violates ORS 646A.093.

(9) Violates a provision of ORS 646A.600 to 646A.628.

(10) Violates ORS 646A.808 (2).

(11) Violates ORS 336.184.

(12) Publishes on a website related to the person's business, or in a consumer agreement related to a consumer transaction, a statement or representation of fact in which the person asserts that the person, in a particular manner or for particular purposes, will use, disclose, collect, maintain, delete or dispose of information that the person requests, requires or receives from a consumer and the person uses, discloses, collects, maintains, deletes or disposes of the information in a manner that is materially inconsistent with the person's statement or representation.

(13) Violates ORS 646A.813 (2).

[(14) Violates section 1 of this 2021 Act.]

SECTION 4. (1) **Section 1 of this 2021 Act and the amendments to ORS 646.607 by section 2 of this 2021 Act apply to acts to collect, receive, process, examine, analyze, collate, disclose, store or retain personal health data, as defined in section 1 of this 2021 Act, that occur on or after the effective date of this 2021 Act.**

(2) **A covered organization that collected, used or disclosed personal health data before the effective date of this 2021 Act may not store, retain or make use of personal health data later than, and shall destroy or render the personal health data inaccessible not later than, 65 days after the effective date of this 2021 Act.**

SECTION 5. Section 1 of this 2021 Act is repealed 270 days after the end of the emergency period, as defined in section 1 of this 2021 Act.

SECTION 6. The amendments to ORS 646.607 by section 3 of this 2021 Act become operative 270 days after the end of the emergency period, as defined in section 1 of this 2021 Act.

SECTION 7. This 2021 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2021 Act takes effect on its passage.

Passed by House April 27, 2021

Received by Governor:

.....M.,....., 2021

Approved:

.....M.,....., 2021

.....

Kate Brown, Governor

Passed by Senate June 7, 2021

Filed in Office of Secretary of State:

.....M.,....., 2021

Shemia Fagan, Secretary of State

Peter Courtney, President of Senate

Passed by Senate June 7, 2021

Enrolled House Bill 3284 (HB 3284-A)

Page 6