HB3603

LRB10329143CPF55529b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB3603

Introduced 2/17/2023, by Rep. Ann M. Williams

SYNOPSIS AS INTRODUCED:

New Act

Amends the Protect Health Data Privacy Act. Provides that a regulated entity shall disclose and maintain a health data privacy policy that, in plain language, clearly and conspicuously disclosures specified information. Provides that a regulated entity shall prominently publish its health data privacy policy on its website homepage. Provides that a regulated entity shall not collect, share, sell, or store categories of health data not disclosed in the health data privacy policy without first disclosing the categories of health data and obtaining the consumer's consent prior to the collection, sharing, selling, or storing of such data. Prohibits the collection, sharing, selling, or storing of health data. Describes the regulated entity's duty to obtain consent; the consumer's right to withdraw consent; prohibitions on discrimination; prohibitions on geofencing; a private right of action; enforcement by the Attorney General; and conflicts with other laws. Makes other changes.

LRB103 29143 CPF 55529 b

A BILL FOR

AN ACT concerning safety.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Protect Health Data Privacy Act.

Section 5. Definitions. As used in this Act:

"Collect" means to buy, rent, lease, access, retain, receive, acquire, or otherwise process health data in any manner.

"Consent" means a clear affirmative act by a consumer that unambiguously communicates the consumer's express, freely given, informed, opt-in, voluntary, specific, and unambiguous written agreement, which may include written consent provided by electronic means, to the collection, sale, sharing or storage of health data. Consent may not be implied, and consent cannot be obtained by:

(1) acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other, unrelated information;

(2) hovering over, muting, pausing, or closing a given piece of digital content; or

(3) agreement obtained through the use of deceptive

designs.

"Consumer" means a person who is a resident of the State, however identified, including by any unique identifier. A person located in the State when the person's health data is collected by a regulated entity will create a presumption that the person is a resident of the State for purposes of enforcing this Act.

"Deceptive design" means any user interface or element thereof that has the effect of subverting, impairing, or impeding an individual's autonomy, decision-making, or choice.

"Deidentified data" means data that cannot be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual. A regulated entity that possesses deidentified data shall: (i) take reasonable measures to ensure that such data cannot be associated with an individual; (ii) publicly commit to process such data only in a deidentified fashion and not attempt to reidentify such data; and, (iii) contractually obligate any recipients of such data to satisfy the criteria set forth in items (i) and (ii).

"Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless Internet data, or any other form of location detection to establish a virtual boundary around a specific physical location.

"Health data" means information regarding, relating to,

derived, or extrapolated from the past, present, or future physical or mental health of a consumer, including, but not limited to, any information relating to:

(1) individual health conditions, treatment, status, diseases, or diagnoses;

(2) health related surgeries or procedures;

(3) use or purchase of medication;

(4) social, psychological, behavioral, and medical interventions;

(5) bodily functions, vital signs, measurements, or symptoms;

(6) diagnoses or diagnostic testing, treatment, or medication;

(7) efforts to research or obtain health services or supplies;

(8) health services or products that support or relate to lawful health care, as defined by Public Act 102-1117;

(9) location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; and

(10) any information described in paragraphs (1) through (9) that is derived or extrapolated from nonhealth information, including by use of algorithms or machine learning.

"Health data" does not include personal information collected with the consumer's consent that is used to engage

in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

"Health services" means any service, medical care, or information related to a consumer's health data provided to a consumer.

"Homepage" means the introductory page of an Internet website and any Internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice.

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or linked, directly or indirectly, with a particular consumer or household. "Personal information" does not include publicly available information or deidentified data. "Publicly available" means information that is lawfully made available from federal, State, or local government

records.

"Regulated entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized, that: (i) conducts business in the State or produces products or services that are available to consumers in the State, and (ii) for any purpose, handles, collects, shares, sells, stores or otherwise deals with health data. "Regulated entity" does not mean government agencies, tribal nations, a clerk of the court, or a judge or justice thereof.

"Sell" or "sale" means when a regulated entity, directly or indirectly, receives any form of remuneration or other valuable consideration from the use of health data or from the recipient of the health data in exchange for the health data. "Sell" does not include:

(1) the sharing of health data to a recipient where the regulated entity maintains control and ownership of the health data;

(2) the sharing of health data to comply with applicable laws or regulations;

(3) the recipient uses the health data only at the direction of the regulated entity and consistent with the purpose for which it was collected and disclosed to the consumer; and

(4) the transfer of health data to a third party as an asset as part of a merger, acquisition, bankruptcy, or

other transaction in which the third party assumes control of all or part of the regulated entity's assets that shall comply with the requirements and obligations in this Act.

"Share" means to release, disclose, disseminate, divulge, loans, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, health data by a regulated entity to a third party except where the regulated entity maintains exclusive control and ownership of the health data. "Share" does not include:

(1) the disclosure of health data to an entity who collects or processes the personal data on behalf of the regulated entity, when the regulated entity maintains control and ownership of the data and the third party maintains or uses the health data only for the regulated entity's distinct purposes;

(2) the disclosure of health data to a third party with whom the consumer has a direct relationship for purposes of and only to the extent necessary for providing a product or service requested by the consumer when the regulated entity maintains control and ownership of the data and the third party maintains or uses the health data only for the regulated entity's distinct purposes; or

(3) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the

regulated entity's assets and shall comply with the requirements and obligations in this Act.

"Third party" means an entity other than a consumer, regulated entity, service provider, or affiliate of the regulated entity.

Section 10. Scope.

(a) This Act applies to consumers seeking, researching, or obtaining health services within the State, or information about health services available in the State and regulated entities.

(b) This Act does not affect an individual's right to voluntarily share the individual's own health care information with another person.

Section 15. Health data privacy policy required.

(a) A regulated entity shall disclose and maintain a health data privacy policy that, in plain language, clearly and conspicuously discloses:

(1) the specific types of health data collected and the purpose for which the data is collected and used;

(2) the categories of sources from which the health data is collected;

(3) the specific types of health data that are shared, sold, and stored;

(4) the categories of third parties with whom the

regulated entity collects, shares, sells, and stores health data, and the process to withdraw consent from having health data collected, shared, sold, and stored;

(5) a list of the specific third parties to which the regulated entity shares health data, and an active electronic mail address or other online mechanism that the consumer may use to contact these third parties free of charge;

(6) how a consumer may exercise the rights provided in this Act, including, but not limited to, identifying 2 or more designated methods for a consumer to contact the regulated entity in connection with the exercise of any rights provided in this Act;

(7) the length of time the regulated entity intends to retain each category of health data, or if that is not possible, the criteria used to determine that period provided that a regulated entity shall not retain health data for each disclosed purpose for which the health data was collected for longer than is reasonably necessary to fulfill that disclosed purpose; and

(8) whether the regulated entity collects health data when the consumer is not directly interacting with the regulated entity or its services.

(b) A regulated entity shall prominently publish its health data privacy policy on its website homepage. Such health data privacy policy must be distinguishable from other

matters.

(c) A regulated entity shall not collect, share, sell, or store additional categories of health data not disclosed in the health data privacy policy without first disclosing the additional categories of health data and obtaining the consumer's consent prior to the collection, sharing, selling, or storing of such health data.

(d) A regulated entity shall not collect, share, sell, or store health data for additional purposes not disclosed in the health data privacy policy without first disclosing the additional purposes and obtaining the consumer's affirmative consent prior to the collection, sharing, selling, or storing of such health data.

(e) It is a violation of this Act for a regulated entity to contract with a service provider to process consumer health data in a manner that is inconsistent with the regulated entity's consumer health data privacy policy.

Section 20. Prohibition on collection, sharing, selling, or storing of health data.

(a) A regulated entity shall not collect health data, except:

(1) with the consent of the consumer to whom such information relates for a specified purpose; or

(2) as is strictly necessary to provide a product or service that the consumer to whom such health data relates

has specifically requested from such regulated entity.

(b) A regulated entity shall not share any health data except:

(1) with consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect health data; or

(2) to the extent strictly necessary to provide a product or service that the consumer to whom such health data relates has specifically requested from such regulated entity.

(c) A regulated entity shall not sell health data to any third party without entering into a separate written agreement with the consumer to whom such health data relates, in which the consumer expressly consents to and authorizes the regulated entity to sell such health data.

(d) A regulated entity shall not store any health data except:

(1) with consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect health data; or

(2) to the extent strictly necessary to provide a product or service that the consumer to whom such health data relates has specifically requested from such regulated entity.

Section 25. Consent required.

(a) A regulated entity shall not seek consent to collect, share, sell, or store health data without first disclosing its health data privacy policy as required under Section 15.

(b) Consent obtained prior to collection, sharing, selling, or storing. Consent required under this Section must be obtained prior to the collection, sharing, selling, or storing, as applicable, of any health data, and the request for consent must clearly and conspicuously disclose, separate and apart from its health data privacy policy:

(1) the categories of health data collected, sold, shared, or stored;

(2) the purpose of the collection, selling, sharing, or storage of the health data, including the specific ways in which it will be used; and

(3) how the consumer can withdraw consent from future collection, selling, sharing or storage of their health data.

(c) Consent required under this Section must be obtained prior to the use of any health data for any purpose not specified prior to obtaining a consumer's consent for the use of such health data for any new purpose.

Section 30. Right to withdraw consent. A consumer has the right to withdraw consent from the collection and sharing of the consumer's health data.

Section 35. Prohibition on discrimination. It shall be unlawful for a regulated entity to discriminate against a consumer solely because they have not provided consent pursuant to this Act, or have exercised any other rights provided by this Act or guaranteed by law. Discrimination includes, but is not limited to:

(1) providing different, or a different level or quality of, goods or services to the consumer;

(2) denying or limiting goods or services to the consumer;

(3) imposing additional requirements or restrictions on the individual that would not be necessary if the consumer provided their consent;

(4) providing materially different treatment to consumers who provide consent as compared to consumers who do not provide consent;

(5) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services; or

(6) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

Section 40. Right to confirm. A consumer has the right to confirm whether a regulated entity is collecting, selling, sharing, or storing any of the consumer's health data, and to

confirm that a regulated entity has deleted the consumer's health data following a deletion request pursuant to Section 45 of this Act. A regulated entity that receives a consumer request to confirm shall respond within 30 calendar days from receiving the request to confirm from the consumer. The regulated entity shall, without reasonable delay, promptly take all steps necessary to verify the consumer's request, but this shall not extend the regulated entity's duty to respond within 30 days of receipt of the consumer's request. The time period to provide the required confirmation may be extended once by an additional 30 calendar days when reasonably necessary, provided the consumer is provided notice of the extension within the first 30-day period.

Section 45. Right to deletion.

(a) A consumer has the right to have the consumer's health data that is collected by a regulated entity deleted by informing the regulated entity of the consumer's request for deletion.

(b) A regulated entity that collects health data about consumers shall disclose the consumer's rights to request the deletion of the consumer's health data.

(c) Except as otherwise specified in subsection (f), a regulated entity that receives a consumer request to delete any of the consumer's health data shall without unreasonable delay, and no more than 30 calendar days from receiving the

deletion request:

(1) delete the consumer's health data from its records, including from all parts of the regulated entity's network or backup systems; and

(2) notify all service providers, contractors, and third parties with whom the regulated entity has shared the consumer's health data of the deletion request.

(d) Any service provider, contractor, and other third party that receives notice of a consumer's deletion request from a Regulated Entity shall honor the consumer's deletion request and delete the health data from the regulated entity's records, including from all parts of its network or backup systems.

(e) A consumer or a consumer's authorized agent may exercise the rights set forth in this Act by submitting a request, at any time, to a regulated entity. Such a request may be made by:

(1) contacting the regulated entity through the manner included in its health data privacy policy;

(2) by designating an authorized agent who may exercise the rights on behalf of the consumer;

(3) in the case of collecting health data of a minor, the minor seeking health services may exercise their rights under this Act, or the parent or legal guardian of the minor, may exercise the rights of this Act on the minor's behalf; or

(4) in the case of collecting health data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under the Probate Act of 1975, the guardian or the conservator of the consumer may exercise the rights of this Act on the consumer's behalf.

(f) The time period to delete any of the consumer's health data may be extended once by an additional 30 calendar days when reasonably necessary, provided the consumer is provided notice of the extension within the first 30-day period.

Section 50. Consumer health data security and minimization.

(a) A regulated entity shall restrict access to health data by the employees, service providers, and contractors of such regulated entity to only those employees, services providers, and contractors for which access is necessary to provide a product or service that the consumer to whom such health data relates has requested from such regulated entity.

(b) A regulated entity shall establish, implement, and maintain administrative, technical, and physical data security practices that at least satisfy a reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of health data appropriate to the volume and nature of the personal data at issue.

Section 55. Prohibition on geofencing.

(a) It shall be unlawful for any person to implement a geofence that enables the sending of a notification, message, alert, or other pieces of information to a consumer that enters the perimeter around any entity that provides health services.

(b) It shall be unlawful for any person to implement a geofence around any entity that provides in-person health care services where such geofence is used to identify, track, or collect data from a consumer that enters the virtual perimeter.

Section 60. Private right of action. Any person aggrieved by a violation of this Act shall have a right of action in a state circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against any offending party that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against any offending party that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the

State or federal court may deem appropriate.

Section 65. Enforcement by the Attorney General. The Attorney General may enforce a violation of this Act as an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. All rights and remedies provided the Attorney General under the Consumer Fraud and Deceptive Business Practices Act shall be available for enforcement of a violation of this Act.

Section 70. Conflict with other laws.

(a) Nothing in this Act shall be construed to conflict with the Health Insurance Portability and Accountability Act of 1996.

(b) Nothing in this Act shall be construed to prohibit disclosure as required under the Adult Protective Services Act, the Abused and Neglected Child Reporting Act, the Criminal Code of 2012, and the Disclosure of Offenses Against Children Act.

(c) If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the remainder of this Act and the application of such provision to other persons not similarly situated or to other circumstances shall not be affected by the invalidation.