HB3494

LRB10411205BABAB21287b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

HB3494

Introduced 2/18/2025, by Rep. Ann M. Williams

SYNOPSIS AS INTRODUCED:

New Act
815 ILCS 505/2HHHH new

Creates the Protect Health Data Privacy Act. Provides that a regulated entity shall disclose and maintain a health data privacy policy that clearly and conspicuously discloses specified information. Sets forth provisions concerning health data privacy policies. Provides that a regulated entity shall not collect, share, or store health data, except in specified circumstances. Provides that it is unlawful for any person to sell or offer to sell health data concerning an individual without first obtaining valid authorization from the individual. Provides that a valid authorization to sell individual health data must contain specified information; a copy of the signed valid authorization must be provided to the individual; and the seller and purchaser of health data must retain a copy of all valid authorizations for sale of health data for 6 years after the date of its signature or the date when it was last in effect, whichever is later. Sets forth provisions concerning the consent required for collection, sharing, and storage of health data. Provides that an individual has the right to withdraw consent from the processing of the individual's health data. Provides that it is unlawful for a regulated entity to engage in discriminatory practices against individuals solely because they have not provided consent to the processing of their health data or have exercised any other rights provided by the provisions or guaranteed by law. Sets forth provisions concerning an individual's right to confirm whether a regulated entity is collecting, selling, sharing, or storing any of the individual's health data; an individual's right to have the individual's health data that is collected by a regulated entity deleted; prohibitions regarding geofencing; and individual health data security. Provides that any person aggrieved by a violation of the provisions shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. Provides that the Attorney General may enforce a violation of the provisions as an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Defines terms. Makes a conforming change in the Consumer Fraud and Deceptive Business Practices Act.

A BILL FOR

AN ACT concerning regulation.

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:

"Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this definition, "control" and "controlled" mean (A) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

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

"Consent" means a clear affirmative act by an individual that unambiguously communicates the individual's express, freely given, informed, opt-in, voluntary, specific, and unambiguous written agreement, including written consent provided by electronic means, to the processing 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.

"Deceptive design" means any user interface or element thereof that has the substantial 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 spatial or location detection to establish a virtual boundary around a specific physical location, or to locate an individual within a virtual boundary. For the purposes of this Act, "geofence" means a virtual boundary that is no more than 1,750 feet 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 an individual, 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) precise location information that could reasonably be used to determine an individual'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 non-health information, including by use of algorithms or machine learning, if such information is used or processed in connection with the advertising, marketing, or provision of health services.

"Health data" does not include:

(1) personal information collected with the individual's consent that is used in research conducted in accordance with the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, at Part 46 of Title 45 of the Code of Federal Regulations; the Good Clinical Practice Guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; or the United States Food and Drug Administration human subjects protection requirements under Parts 50 and 56 of Title 21 of the Code of Federal Regulations and 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; or

(2) deidentified data.

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

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, and any subsequent amendments thereto and any regulations promulgated thereunder, including the Privacy Rule, as specified in 45 CFR 164.500-534, the Security Rule, as specified in 45 CFR 164.302-318, and the Breach Notification rule, as specified in 45 CFR 164.400-414.

"Homepage" means the introductory page of a website 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" page, "Information" page, or settings page, and any other location that allows individuals to review the notice.

"Individual" means a person who is a resident of this State, however identified, including by any unique identifier. A person located in this State when the person's health data is collected by a regulated entity shall create a presumption that the person is a resident of this State for purposes of enforcing this Act. "Individual" does not include a person acting in a commercial or within an employment context.

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or linked, directly or indirectly, with a particular individual or household. "Personal information" does not include publicly available information or deidentified data.

"Precise location information" means information that identifies the location of an individual within a radius of 1,750 feet. "Precise location information" does not include: (i) the content of communications, or (ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "Processing" means any operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, whether alone or in combination with other data, such as the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, retrieval, modification, or deidentification of health data.

"Processor" means a person or legal entity that processes health data on behalf of a regulated entity pursuant to a written agreement or contract.

"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 this State or produces products or services that are available to individuals in this State; and (ii) for any purpose, processes or otherwise deals with health data. "Regulated entity" does not include government agencies, including the Illinois Insurance Guaranty Fund as described under Article XXXIV of the Illinois Insurance Code, tribal nations, a clerk of the court, or a judge or justice thereof, or contracted service providers or processors when processing an individual's health data on behalf of the governmental agency. "Regulated entity" does not include any entity that is a covered entity or a business associate, as defined in Section 160.103 of Title 45 of the Code of Federal Regulations, subject to and in substantial compliance with HIPAA to the extent such entity is acting as a covered entity or business associate under the Privacy and Security rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations. "Regulated entity" does not include any entity that is subject to and in compliance with restrictions on disclosure of records under Section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, to the extent such entity is acting in a capacity subject to such restrictions.

"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" or "sale" 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 use of the health data by an entity exclusively at the direction of the regulated entity and consistent with the purpose for which it was collected and disclosed; 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" or "sharing" means to release, disclose, disseminate, divulge, loan, 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" or "sharing" does not include:

(1) the disclosure or transfer of health data to a processor that 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 processor maintains or uses the health data only for the regulated entity's distinct purposes pursuant to a contract;

(2) the disclosure or transfer of health data to a third party with whom the individual has a direct relationship for purposes of and only to the extent necessary for providing a product or service requested by the individual 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.

"Strictly necessary" means essential or required to be done.

"Substantial compliance" means a level of compliance with Title 45 of the Code of Federal Regulations Sections 164.502, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524,

164.526, 164.528, and 164.530 that does not arise from gross negligence, recklessness, or willful misconduct by the entity acting as a covered entity or business associate.

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

Section 10. Scope.

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

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

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 includes and 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) whether the regulated entity collects health data when the individual is not directly interacting with the

regulated entity or its services.

(4) the specific types of health data that are shared and sold;

(5) the categories of third parties with whom the regulated entity sells and processes health data, and the process to withdraw consent from having health data processed and sold;

(6) a list of the third parties with whom the regulated entity shares health data;

(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; however, 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 or as otherwise permitted by this Act;

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

(9) the process to opt out of having health data collected; and

(10) an active electronic mail address or other online mechanism that the individual may use to contact the

regulated entities free of charge.

(b) A regulated entity shall prominently publish or link to its health data privacy policy on its website homepage, mobile application, or in another manner that is clear and conspicuous to individuals. Its health data privacy policy must be distinguishable from other matters. Any regulated entity providing health services in a physical location shall also post its health data privacy policy in a conspicuous place that is readily available for viewing by individuals.

(c) A regulated entity shall not process or sell 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 individual's consent before the processing or selling of the health data.

(d) A regulated entity shall not process or sell health data for additional purposes not disclosed in the health data privacy policy without first disclosing the additional purposes and obtaining the individual's consent before the processing or selling of the health data.

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

Section 20. Prohibition on processing of health data.

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

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

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

(b) Consent required under this Section must be obtained before the use of any health data for any additional purpose that was not specified before obtaining an individual's consent for the use of the health data.

Section 25. Prohibition on sale of health data.

(a) It is unlawful for any person to sell or offer to sell health data concerning an individual without first obtaining valid authorization from the individual. The sale of individual health data must be consistent with the valid authorization signed by the individual.

(b) A valid authorization to sell an individual's health data is an agreement consistent with this Section and must be written in plain language. The valid authorization to sell the individual's health data must contain the following:

(1) the specific health data concerning the individual that the person intends to sell;

(2) the name and contact information of any person or

entity collecting and selling the health data;

(3) the name and contact information of any person or entity purchasing the health data from the seller identified in paragraph (2) of this subsection;

(4) a description of the purpose for the sale, including how the health data will be gathered and how it will be used by the purchaser identified in paragraph (3) of this subsection when sold;

(5) a statement that the provision of goods or services may not be conditioned on the individual signing the valid authorization;

(6) a statement that the individual has a right to revoke the valid authorization at any time and a description on how an individual may revoke the valid authorization;

(7) a statement that the individual health data sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by this Section;

(8) an expiration date for the valid authorization that expires one year from when the individual signs the valid authorization; and

(9) the signature of the individual and date.

(c) An authorization is not valid if the document has any of the following defects:

(1) the expiration date has passed;

(2) the authorization does not contain all the information required under this Section;

(3) the authorization has been revoked by the individual;

(4) the authorization has been combined with other documents to create a compound authorization; or

(5) the provision of goods or services is conditioned on the individual signing the authorization.

(d) A copy of the signed valid authorization must be provided to the individual.

(e) The seller and purchaser of health data must retain a copy of all valid authorizations for sale of health data for 6 years after the date of its signature or the date when it was last in effect, whichever is later.

Section 30. Consent required for processing health data.

(a) A regulated entity shall not seek consent to process health data without first disclosing its health data privacy policy as required under Section 15.

(b) Consent required under this Section must be obtained before the processing, 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 processed;

(2) the purpose of the processing of the health data,

including the specific ways in which it will be used; and

(3) how the individual can withdraw consent from future processing of their health data.

(c) Consent required under this Section must be obtained before the use of any health data for any additional purpose that was not specified before obtaining an individual's consent for the use of the health data.

(d) An individual may exercise rights under this Section by submitting a request to a regulated entity using the method the regulated entity specifies in the privacy policy under paragraph (8) of subsection (a) of Section 15.

Section 35. Right to withdraw consent. An individual has the right to withdraw consent from the sale or processing of the individual's health data, consistent with the requirements of Section 30.

Section 40. Prohibition on discriminatory practices.

(a) It is unlawful for a regulated entity to engage in discriminatory practices against an individual solely because the individual has not provided consent to the sale or processing of the individual's health data pursuant to this Act, or have exercised any other rights provided by this Act or guaranteed by law. Discriminatory practices include, but are not limited to:

(1) denying or limiting goods or services to the

individual;

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

(3) providing materially different treatment to individuals who provide consent as compared to individuals who do not provide consent;

(4) providing or suggesting that the individual will receive a lower level or quality of goods or services;

(5) suggesting that the individual will receive a different price or rate for goods or services; or

(6) charging different prices or rates for goods or services, including using discounts or other benefits or imposing penalties.

(b) It shall not be a discriminatory practice under this Section to use health data as is strictly necessary to provide a product or service that the individual to whom the health data relates has specifically requested from a regulated entity.

Section 45. Right to confirm. (a) An individual has the right to confirm whether a regulated entity is collecting, selling, sharing, or storing any of the individual's health data, and to confirm that a regulated entity has deleted the individual's health data following a deletion request pursuant to Section 50.

(b) A regulated entity that receives an individual's request to confirm shall respond within 45 calendar days after receiving the request to confirm from the individual.

(c) The regulated entity shall, without reasonable delay, promptly take all steps necessary to verify the individual's request, but this shall not extend the regulated entity's duty to respond within 45 days of receipt of the individual's request.

(d) The time period to provide the required confirmation may be extended once by an additional 45 calendar days when reasonably necessary, if the individual is provided notice of the extension within the first 45-day period.

Section 50. Right to deletion.

(a) An individual whose health data is collected by a regulated entity has the right to have the individual's health data that is collected by a regulated entity deleted by informing the regulated entity of the individual's request for deletion, except as provided in subsection (g).

(b) Except as otherwise specified in subsection (f), a regulated entity that receives an individual's request to delete any of the individual's health data shall without unreasonable delay, and no more than 45 calendar days from receiving the deletion request:

(1) delete the individual's health data from its records, including from all parts of the regulated

entity's network; and

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

(c) If a regulated entity stores any health data on archived or backup systems, it may delay compliance with the individual's request to delete with respect to the health data stored on the archived or backup system until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(d) Any processor, service provider, contractor, and other third party that receives notice of an individual's deletion request from a regulated entity shall honor the individual'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) An individual or an individual'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 individual;

(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 an individual subject to guardianship, conservatorship, or other protective arrangement under the Probate Act of 1975, the guardian or the conservator of the individual may exercise the rights of this Act on the individual's behalf.

(f) The time period to delete any of the individual's health data may be extended once by an additional 45 calendar days when reasonably necessary, if the individual is provided notice of the extension within the first 45-day period.

(g) Neither a regulated entity nor a processor shall be required to comply with an individual's request to delete the individual's health data if it is necessary for the regulated entity or the processor to maintain the individual's health data to:

(1) complete the transaction for which the health data was collected, provide a good or service requested by the individual, or otherwise fulfill the requirements of an agreement between the regulated entity and the individual;

(2) prevent or detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, if the use of health data for such purposes is limited in time pursuant to a valid record retention

schedule;

(3) 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, if the entities' deletion of the information is likely to render impossible or seriously impair the achievement of such research, and if the individual has provided consent to such use of their health data;

(4) comply with any applicable data retention requirements in accordance with State and federal law, including the data retention requirements set forth in Section 6 of the Hospital Licensing Act, 45 CFR 164.316, and 45 CFR 164.530; or

(5) retain the health data if the regulated entity has been notified, in writing by an attorney, that there is litigation pending in court involving the individual's health data as possible evidence and that the individual is the attorney's client or is the person who has instituted the litigation against their client, then the regulated entity shall retain the record of that individual until notified in writing by the plaintiff's attorney, with the approval of the defendant's attorney of record, that the case in court involving the record has been concluded or for a period of 12 years after the date that the record was produced, whichever occurs first in time.

Section 55. Authentication of identity.

(a) A regulated entity that receives an individual's request to confirm or delete may take reasonable measures to authenticate the individual's identity or an authorized agent's identity to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least 3 pieces of personal information provided by the individual or the individual's authorized agent with personal information maintained by the regulated entity that it has determined to be reliable for the purpose of authenticating the individual or the individual's authorized agent together with a signed declaration under penalty of perjury that the individual or the individual's authorized agent making the request is the individual or the individual's authorized agent whose health data is the subject of the request. If a regulated entity uses this method for authentication, the regulated entity shall make all forms necessary for authentication of an individual's or the individual's authorized agent's identity available to the individual or the individual's authorized agent, and shall maintain all signed declarations as part of its recordkeeping obligations.

(b) A regulated entity is not required to comply with an individual's or the individual's authorized agent's request to confirm or delete if the regulated entity, using commercially reasonable efforts, is unable to authenticate the identity of

the individual or the individual's authorized agent making the request. If a regulated entity is unable to authenticate the individual's or the individual's authorized agent's identity, the regulated entity shall inform the individual or the individual's authorized agent that it was unable to authenticate the individual's or the individual's authorized agent's identity and advise the individual or the individual's authorized agent of other methods, if available, of authenticating their identity.

(c) If a regulated entity denies an authenticated individual's request to delete that individual's health data, in whole or in part, because of a conflict with federal or State law, the regulated entity shall inform the requesting individual and explain the basis for the denial, unless prohibited from doing so by law.

(d) Any information provided by an individual or the individual's authorized agent to a regulated entity for the purpose of authenticating the individual's or the individual's authorized agent's identity shall not be used for any purpose other than authenticating the individual's identity and shall be destroyed immediately following the authentication process.

Section 60. Individual health data security and minimization.

(a) A regulated entity shall restrict access to health data by the employees, processors, service providers, and

contractors of the regulated entity to only those employees, processors, services providers, and contractors for whom access is necessary to provide a product or service that the individuals to whom the health data relates have requested from the 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 65. Prohibition on geofencing.

(a) It shall be unlawful for any person to implement a geofence that enables the sending of notifications, messages, alerts, advertisements, or other pieces of information to an individual that enters the perimeter around any entity that provides health services or products, unless such messages are directly related to an individual's appointment in the facility or the provision of requested health services or products by the regulated entity.

(b) It shall be unlawful for any person to implement a geofence around any entity that provides in-person health care services and products where the geofence is used to:

(1) identify or track individuals seeking health care

services or products or to determine whether the individual is seeking health care services or products; or

(2) collect data from an individual who enters the virtual perimeter.

Section 70. Limits on access to an individual's health information by government agencies, officials, and law enforcement.

(a) A regulated entity shall not disclose an individual's health data to a federal, state, or local governmental agency, official, or law enforcement agent or agency unless: (1) disclosure is requested by the individual to whom the health data pertains or (2) the governmental entity or official serves the regulated entity with a valid warrant, except as prohibited under the laws of this State, including, but not limited to, Section 3.5 of the Uniform Interstate Depositions and Discovery Act.

(b) A regulated entity shall not sell, share, allow access to, or disclose an individual's health data to any State or local jurisdiction for the purpose of investigating or enforcing a law that denies or interferes with an individual's right to obtain any lawful health care services, as defined by the Lawful Health Care Activity Act.

Section 75. 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 attorney's 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 80. 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 to the Attorney General under the Consumer Fraud and Deceptive Business Practices Act shall be available for enforcement of a violation of this Act.

Section 85. Conflict with other laws.

(a) Nothing in this Act shall be construed to prohibit the lawful and authorized disclosure of health data by regulated entities to local health departments or State government

agencies or by or among local health departments and State government agencies as may be required by State and federal law, including 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.

(b) 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.

(c) This Act shall not apply to:

(1) personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations; and

(2) entities subject to, and in compliance with, the Insurance Information and Privacy Protection Act, the Insurance Data Security Law in the Illinois Insurance Code, and any corresponding privacy protection rules adopted by the Director of Insurance.

(d) This Act shall not be construed to conflict with, or limit the application of, any of the following laws, rules, or regulations governing the sharing, collection, processing, or disclosure of personal information or health data: the Medical Patient Rights Act; the Hospital Licensing Act; Sections 2, 4, 5, 6, 7, 8, 9, 9.3, 9.8, and 11 the Mental Health and Developmental Disabilities Confidentiality Act; subsections

(c) through (f) of Section 10 of the Mental Health and Developmental Disabilities Confidentiality Act; and Sections 8-2001 and 8-2001.5 of the Code of Civil Procedure.

(e) In the event of a conflict between the provisions of this Act and any other law, rule, or regulation listed in subsections (c) and (d), the law, rule, or regulation that provides the greater right, benefit, or protection to individuals shall apply. Nothing in this Act shall be construed to diminish or limit any rights, benefits, or protections afforded under the laws, rules, or regulations referenced in subsections (c) and (d).

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

Section 100. The Consumer Fraud and Deceptive Business Practices Act is amended by adding Section 2HHHH as follows:

(815 ILCS 505/2HHHH new)

Sec. 2HHHH. Violations of the Protect Health Data Privacy Act. Any person who violates the Protect Health Data Privacy Act commits an unlawful practice within the meaning of this Act.