**Rep. Mary Beth Canty**

# Filed: 5/31/2026



AMENDMENT TO SENATE BILL 93

AMENDMENT NO. _____. Amend Senate Bill 93 by replacing everything after the enacting clause with the following:

"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 (1) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company, (2) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (3) the power to exercise controlling influence over the management of a company.

"Collect" means to buy, rent, lease, access, retain, receive, derive, or acquire health data in any manner, including receiving the data from an individual, either actively or passively, or by observing or tracking the individual's online activity or precise location.

"Consent" means a clear, affirmative act by an individual that unambiguously communicates the individual's express, freely given, informed, opted-into, voluntary, specific, and unambiguous written agreement, including written consent provided by electronic means to the processing or sale of health data. "Consent" does not include implied consent or consent 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.

"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 that is no more than 1,750 feet around a specific physical location.

"Health data" means (1) an individual's personal information that identifies a past or present health condition of that individual, or (2) information that is linked or can be reasonably linked to an individual that a regulated entity derives or extrapolates from nonhealth information that a regulated entity uses or processes to determine a past, present, or future health condition of that individual.

"Health data" includes any information relating to an individual's:

(1) health conditions, status, diseases, diagnoses, or testing;

(2) health-related treatment, surgeries, or procedures;

(3) use or purchase of medication;

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

(5) measurement or tracking of bodily functions, vital

signs, or symptoms;

(6) responses to and results from online screenings and online tests and quizzes regarding the individual's health conditions that are used to determine an individual's health condition;

(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 in Section 28-10 of the Lawful Health Care Activity Act; and

(9) precise location information used to determine an individual's attempt to acquire or receive health services or supplies.

"Health data" does not include:

(1) information about an individual's purchase or acquisition of retail goods or services that the regulated entity uses or processes for a purpose other than to determine an individual's past, present, or future physical or mental health condition; or

(2) deidentified data.

"Health services" means any service, medical care, or information related to an individual's health condition 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 natural person who is a resident of this State or whose health data is collected when present in this State, however identified, including by any unique identifier. "Individual" does not include a person acting within the scope of the person's duties as an employee, independent contractor, officer, board member, or sole proprietorship.

"Person" means, where applicable, natural persons, corporations, trusts, unincorporated associations, and partnerships. "Person" does not include (1) any branch of State government, unit of local government, or school district; (2) any tribal nation, or (3) any contractor, subcontractor, or agent that processes health data on behalf of, and in accordance with the terms and conditions of a

contract with, any branch of State government, tribal nation, unit of local government, or school district.

"Personal information" means information that identifies, is reasonably capable of being associated with, or is linked, directly or indirectly, with a particular individual or household. "Personal information" includes, but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier. "Personal information" does not include publicly available information or deidentified data.

"Precise location information" means information derived from technology, including, but not limited to, Global Positioning System level latitude and longitude coordinates or other mechanisms, that identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise location information" does not include: (1) the content of communications, or (2) 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, 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 made available to the general public from (1) federal, State, or local government records; (2) widely distributed media, including health data intentionally made available by the individual to the general public and in which the individual did not maintain a reasonable expectation of privacy; or (3) a disclosure that has been made to the general public as required by federal, State, or local law. "Publicly available information" does not include (1) personal information that is created through the combination of personal information with publicly available information; (2) information made available by an individual on a website or online service open to all members of the public, for free or for a fee, where the individual has maintained a reasonable expectation of privacy by restricting the information to a specific audience; or (3) any obscene visual depiction, as defined in 18 U.S.C. 1460.

"Regulated entity" means any individual, partnership, corporation, limited liability company, or association that: (1) conducts business in this State, or produces or provides products or services that are available to individuals in this

State; and (2) determines the purpose and means of processing or selling of health data.

"Regulated entity" does not include:

(1) any branch of State government, a tribal nation, a unit of local government, or a school district;

(2) a contractor, subcontractor, or agent that processes health data on behalf of, and in accordance with the terms and conditions of a contract with, any branch of State government, a tribal nation, a unit of local government, or a school district;

(3) a processor that processes health data on behalf of a regulated entity;

(4) a not-for-profit legal entity that is subject to and in compliance with the Illinois Insurance Guaranty Fund Article of the Illinois Insurance Code or the Life and Health Insurance Guaranty Association Article of the Illinois Insurance Code, to the extent such entity is acting in a capacity subject to the supervision of the Department of Insurance;

(5) a covered entity or a business associate, as defined in 45 CFR 160.103, 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;

(6) 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; or

(7) an entity that is subject to and in compliance with the Insurance Information and Privacy Protection Article of the Illinois Insurance Code, the Insurance Data Security Law, and any corresponding privacy protection rules adopted by the Director of Insurance to the extent such entity is acting in a capacity subject to such laws and rules.

"Sell" or "sale" means the exchange of health data for monetary or other valuable consideration.

"Sell" or "sale" does not include:

(1) the sharing or transfer of an individual's health data by a regulated entity to a processor that processes the individual's health data on behalf of the regulated entity;

(2) the sharing or transfer of an individual's health data to an affiliate of the regulated entity;

(3) the sharing or transfer of an individual's health data by a regulated entity to a third party with whom the individual has a direct relationship when the sharing is for the purpose of, and only to the extent necessary for providing a product or service requested by the

individual, and the third party maintains or uses the individual's health data consistent with the purpose for which it was collected and consented to by the individual;

(4) the sharing or transfer of an individual's health data when the individual directs the regulated entity to disclose the individual's health data or intentionally uses the regulated entity to interact with a third party;

(5) the sharing or transfer of an individual's health 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 complies with the requirements and obligations in this Act, but only if the regulated entity, within a reasonable time before the exchange, provides the affected individual with:

(A) a notice describing the transfer, including the name of the entity receiving the individual's health data and the applicable privacy policies of the entity; and

(B) a reasonable opportunity to withdraw previously provided consent related to the individual's health data and request the deletion of the individual's health data; and

(6) the sharing or transfer of an individual's publicly available health data.

"Share" or "sharing" means to release, disclose,

disseminate, divulge, loan, make available, provide access to, license, transfer, or otherwise communicate orally, in writing, or by electronic or other means, an individual's 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 sharing or transfer of an individual's health data by a regulated entity to a processor that processes the individual's health data on behalf of the regulated entity;

(2) the sharing or transfer of an individual's health data to an affiliate of the regulated entity;

(3) the sharing or transfer of an individual's health data by a regulated entity to a third party with whom the individual has a direct relationship when the sharing is for the purpose of, and only to the extent necessary for providing a product or service requested by the individual, and the third party maintains or uses the individual's health data consistent with the purpose for which it was collected and consented to by the individual;

(4) the sharing or transfer of an individual's health data when the individual directs the regulated entity to disclose the individual's health data or intentionally uses the regulated entity to interact with a third party;

(5) the sharing or transfer of an individual's health

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 complies with the requirements and obligations in this Act, but only if the regulated entity, within a reasonable time before the exchange, provides the affected individual with:

(A) a notice describing the transfer, including the name of the entity receiving the individual's health data and the applicable privacy policies of the entity; and

(B) a reasonable opportunity to withdraw previously provided consent related to the individual's health data and request the deletion of the individual's health data; and

(6) the sharing or transfer of an individual's publicly available health data.

"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, processor, or affiliate of the regulated entity.

"Unit of local government" means a county, municipality, township, special district, or any other unit designated as a unit of local government by law.

Section 10. 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 categories of health data processed, including the specific categories of health data collected, the purposes for which the health data is collected, and how the health data will be used;

(2) the categories of sources from which 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 categories of health data shared and sold;

(5) the categories of third parties to whom the regulated entity shares and sells health data, if applicable;

(6) the process for opt-in consent to collection of health data;

(7) how to withdraw consent from the collection, processing, and selling of an individual's health data;

(8) the process to withdraw consent from having health data collected;

(9) 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;

(10) 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;

(11) an active email address or other online mechanism that the individual may use to contact the regulated entities, free of charge; and

(12) the date the health data privacy notice was last updated.

(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. A regulated entity's 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 15. Processing of health data.

(a) Except as provided in subsection (c), a regulated entity shall not process an individual's health data unless it first obtains consent of the individual to whom the data relates. Before a regulated entity processes an individual's

health data, it shall first:

(1) disclose its health data privacy policy as required under Section 10; and

(2) separate from the health data privacy policy, request the individual's consent to process the information for a specified purpose and clearly and conspicuously disclose within the request the following information:

(A) the categories of health data processed;

(B) the regulated entity's specific purpose for processing the health data, including the specific ways in which the individual's health data will be used;

(C) the categories of entities with whom the health data is shared; and

(D) how the individual can withdraw consent from future processing of the individual's health data.

(b) A regulated entity shall not process an individual's health data for any additional purpose that was not specifically disclosed and consented to by the individual in accordance with this Act.

(c) Consent to process an individual's health data is not required if the individual's health data is processed only for one or more of the following permissible purposes:

(1) as is strictly necessary to provide a product, service, or service feature that the individual to whom

the health data relates has specifically requested from the regulated entity;

(2) to initiate, manage, execute, or complete a financial or commercial transaction or to fulfill an order for a specific product or service requested by an individual to whom the individual health data pertains, including, but not limited to, associated routine administrative, operational, or account-servicing activity, such as billing, shipping, storage, or accounting;

(3) to comply with an obligation under a law of this State or federal law;

(4) to protect public safety or public health;

(5) to prevent, detect, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activities, or activities that are illegal under the laws of this State;

(6) to preserve the integrity or security of systems; or

(7) to investigate, report, or prosecute persons responsible for activities that are illegal under the laws of this State.

(d) For purposes of this Act, the processing of precise location information or health data to provide transportation services by private entities regulated under the Transportation Network Providers Act is strictly necessary to

the extent that the private entity uses the precise location information or health data for the sole purpose of providing a service requested by the individual or the use is otherwise consistent with that individual's reasonable expectations, considering the context in which the individual provided the precise location information to the private entity.

Section 20. Sale of health data.

(a) It is unlawful for any regulated entity to sell or offer to sell health data concerning an individual without first obtaining consent required under Section 15 and valid authorization from the individual. The sale of individual health data must be consistent with the valid authorization signed or electronically documented by the individual.

(b) A valid authorization to sell an individual's health data is an agreement consistent with this Section and must be provided 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 regulated entity intends to sell;

(2) the name and contact information of the regulated entity collecting and selling the health data;

(3) the name and contact information of the regulated 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 after the individual signs the valid authorization, unless the individual extends the valid authorization before it expires. The individual may renew the individual's valid authorization annually if the regulated entity provides the individual with a notice that alerts the individual that the valid authorization will expire within 30 days before the expiration date and provides the individual with a mechanism that allows the individual to renew the valid authorization for an additional year or withdraw consent; 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 and the individual did not sign an updated valid authorization before the expiration date passed;

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

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

(4) the valid 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 the 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 25. Rights and requests

(a) An individual has the right to confirm: (i) whether a regulated entity has, or is, processing or selling the individual's health data and to access such data, including a list of all third parties and affiliates with whom the regulated entity shared or sold the individual's health data,

and an active email address or other online mechanism that the individual may use to contact these third parties; and (ii) that a regulated entity has deleted the individual's health data following a deletion request pursuant to subsection (c).

(1) 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.

(2) 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 calendar days after receipt of the individual's request.

(3) 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.

(b) An individual has the right to withdraw (i) consent for processing, including collection and sharing, and (ii) authorization for the sale of health data consistent with the requirements of Sections 15 and 20, respectively.

(1) An individual may exercise rights under this subsection (b) by submitting a request to a regulated entity using the method the regulated entity specifies in the privacy policy under paragraph (10) of subsection (a)

of Section 10.

(2) A regulated entity may cease providing a product, service, or service feature upon the withdrawal of consent for collection if the collection of health data is strictly necessary to provide that product, service, or service feature.

(c) 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 paragraph (6) of this subsection.

(1) Except as otherwise specified in paragraph (5), 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 after receiving the deletion request:

(A) delete the individual's health data from its records, including from all parts of the regulated entity's network; and

(B) notify all processors, affiliates, and third parties with whom the regulated entity has shared the individual's health data of the deletion request.

(2) 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.

(3) Any processors, affiliates, or other third parties that receive 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.

(4) 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. This request may be made by:

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

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

(C) 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 minor's rights of this Act on the minor's behalf; or

(D) 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.

(5) 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.

(6) 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:

(A) provide a product, service, or service feature to the individual to whom the health data pertains when requested by that individual. In such cases, the regulated entity shall confirm whether the individual wishes the request for deletion to be treated as a request to terminate the associated product, service, or feature;

(B) execute or complete a financial or commercial transaction, or to fulfill an order for a specific product, good, or service requested by an individual to whom the individual health data pertains, including, but not limited to, associated routine administrative, operational, and account-servicing activity, such as billing, shipping, storage, and

accounting, or otherwise fulfill the requirements of an agreement between the regulated entity and the individual;

(C) prevent, detect, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activities, or activities that are illegal under the laws of this State, or investigate, report, or prosecute those responsible for any such activity;

(D) comply with an obligation under a law of this State or federal law, including 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;

(E) 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 regulated entity's or processor's 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 the individual's health data;

(F) 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

(G) investigate, establish, exercise, prepare for, or defend legal claims.

(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 (10) of subsection (a) of Section 10.

(e) A regulated entity shall not 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 has exercised any other rights provided by this Act or guaranteed by law. Discriminatory practices include, but are not limited to:

(1) denying 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.

For the purposes of this subsection, discriminatory practices do not prohibit a regulated entity from suggesting that the individual will receive a different price or rate for

goods or services or charging different prices or rates for goods or services, including using discounts or other benefits, when done in connection with an individual's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Section 30. Processors.

(a) A processor may process an individual's health data only pursuant to a binding contract between the processor and the regulated entity that sets forth the processing instructions and limits the actions the processor may take with respect to the individual health data it processes on behalf of the regulated entity. A processor may process individual health data only in a manner that is consistent with the binding instructions set forth in the contract with the regulated entity.

(b) A processor shall assist the regulated entity using appropriate technical and organizational measures, whenever possible, in fulfilling the regulated entity's obligations under this Act.

(c) If a processor fails to adhere to the regulated entity's instructions or processes individual health data in a manner that is outside the scope of the processor's contract with the regulated entity, the processor is considered a regulated entity with regard to such data and is subject to all the requirements of this Act with regard to such data.

(d) Determining whether a person is acting as a regulated entity or processor with respect to a specific processing of health data is a fact-based determination that depends upon the context in which health data is to be processed. A processor that continues to adhere to a regulated entity's instructions with respect to a specific processing of health data remains a processor.

(e) A regulated entity or processor that discloses health data to a processor or third party in accordance with this Act shall not be liable under this Act if the processor or third party receiving the health data violates this Act, so long as the disclosing regulated entity or processor did not have actual knowledge that the receiving processor or third-party controller would violate this Act. A third party or processor receiving personal data from a regulated entity or processor in compliance with this Act is not liable under this Act for violations committed by the regulated entity or processor that disclosed the health data.

Section 35. Authentication of an individual's 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 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 the regulated entity 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 the individual's or the individual's authorized agent's 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 40. Individual health data security and minimization.

(a) A regulated entity shall restrict access to health data to only the employees, processors, and contractors, subcontractors, agents, and third parties of the regulated entity for whom access is necessary to provide a product or service that the individual to whom the health data relates has 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.

(c) A regulated entity in possession of deidentified data shall:

(1) take reasonable measures to ensure that such data cannot be associated with an individual;

(2) publicly commit to process such data only in a deidentified fashion and not attempt to reidentify such data; and

(3) contractually obligate any recipients of such data to satisfy the criteria set forth in items (1) and (2).

Section 45. Prohibition on geofencing. It is unlawful for a regulated entity 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 50. 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 collect, 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 55. 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, damages in the amount of $1,000 or compensatory damages, whichever is greater;

(2) against any offending party that intentionally or recklessly violates a provision of this Act, damages in the amount of $5,000 or compensatory 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 60. 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 by the Attorney General under the Consumer Fraud and Deceptive Business Practices Act shall be available for enforcement of a violation of this Act.

Section 65. Conflicts 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) 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 of 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.

(c) In the event of a conflict between the provisions of this Act and any other law, rule, or regulation listed in subsection (b), 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 subsection (b).

Section 70. Exemptions.

(a) This Act shall not apply to:

(1) information that meets the definition of:

(A) protected health information, as defined by, and for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(B) patient identifying information collected,

used, or disclosed in accordance with 42 CFR Part 2, established pursuant to 42 U.S.C. 290dd-2;

(C)(i) identifiable private information for purposes of the federal policy for the protection of human subjects, 45 CFR Part 46;

(ii) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the Good Clinical Practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(iii) the protection of human subjects under 21 CFR Parts 50 and 56; or

(iv) personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this subparagraph (C);

(D) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, Public Law 99-660, and related regulations;

(E) patient safety work product for purposes of 42 CFR Part 3, established pursuant to 42 U.S.C. 299b-21 through 42 U.S.C. 299b-26; or

(F) information that is deidentified in accordance with the requirements for deidentification set forth in 45 CFR Part 164, and derived from any of the health care-related information listed under this paragraph;

(2) information originating from and intermingled to be indistinguishable with information under paragraph (1) that is maintained by:

(A) a covered entity or a business associate, as defined in 45 CFR 160.103, subject to and in substantial compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and 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;

(B) a health care facility, including a private hospital, clinic, center, medical school, medical training institution, laboratory or diagnostic facility, physician's office, infirmary, dispensary, ambulatory surgical treatment center, or other institution or location wherein health care services are provided to any person, including physician organizations and associations, networks, joint ventures, and all other combinations of those organizations;

(C) a health care provider, including a physician, hospital facility, or other person that is licensed or otherwise authorized to deliver health care services; or

(D) a program or a qualified service organization as defined in 42 CFR 2.11; or

(3) information used only for public health activities and purposes as described in 45 CFR 164.512 or that is part of a limited data set, as defined in 45 CFR 164.514, and is used, disclosed, and maintained in the manner required, by 45 CFR 164.514.

(b) Personal information that is governed by and collected, used, or disclosed pursuant to the following laws or regulations is exempt from this Act: (1) the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., and implementing regulations; (2) Part C of Title XI of the Social Security Act, 42 U.S.C. 1320d et seq.; (3) The Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.; (4) the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; Part 99 of Title 34 of the Code of Federal Regulations; or (5) the Insurance Information and Privacy Protection Article of the Illinois Insurance Code, the Insurance Data Security Law, and any corresponding privacy protection rules adopted by the Department of Insurance.

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

Section 500. The Consumer Fraud and Deceptive Business Practices Act is amended by adding Section 2MMMM as follows:

(815 ILCS 505/2MMMM new)

Sec. 2MMMM. Violations of the Protect Health Data Privacy Act. Only for purposes of enforcing Section 60 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.

Section 999. Effective date. This Act takes effect August 1, 2027, except that Section 55 takes effect February 1, 2028.".