**103RD GENERAL ASSEMBLY**
**State of Illinois**
**2023 and 2024**
**HB3603**

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, or acquire, 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. “Consumer” does not include an individual acting in a commercial or employment context.

"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, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary. For the purposes of this definition, "geofence" means a virtual boundary that is no more than 1,750 feet around a specific physical location that provides health services.

"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 be used to determine 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 nonhealthy information, including by use of algorithms or machine learning.

"Health data" does not include (1) 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; or (2) deidentified data.

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

"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 164.500-34, the Security Rule, as specified in 45 CFR 164.302-18, and the Breach Notification rule as specified in 45 CFR 164.400-414.

"Homepage" means the introductory page of an Internet 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," "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.

“Processor” means an individual or legal entity that processes health data on behalf of a regulated entity pursuant to a written agreement or contract. “Process” or “processing” means arranging, storing, organizing, structuring, retrieving, transmission, or the otherwise making available of data.

"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, or contracted service providers when processing consumer health data on behalf of the government agency.

"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 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" 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" does not include:

(1) the disclosure 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 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.

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

"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 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 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 two (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 or link to its health data privacy policy on its website homepage, or in another manner that is clear and conspicuous to consumers. Such 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 consumers.

(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 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 processor to process consumer health data in a manner that is inconsistent with the regulated entity's consumer health data privacy policy.

(f) Exceptions. For the purposes of this Section 15 only, any regulated entity that is subject to and in compliance with HIPAA and provides consumers with a privacy notice pursuant to HIPAA prior to the collection of health data, shall be deemed to be in compliance with this Section.

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

(a) A regulated entity shall not collect, share, or store 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) This Section 20 shall not be construed to limit the collection, use and disclosure of protected health information by any regulated entity

that is subject to and in compliance with HIPAA, including as authorized under 45 CFR § 164.512.

**Section 25. Prohibition on sale of health data.**

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

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

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

(2) The name and contact information of any person(s) or entity collecting and selling the health data;

(3) The name and contact information of any person(s) or entity purchasing the health data from the seller identified in (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 (3) of this subsection when sold;

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

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

(7) A statement that the consumer 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 consumer signs the valid authorization; and

(9) The signature of the consumer 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 consumer;

(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 consumer signing the authorization.

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

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

**Section 30. Consent required for collection, sharing and storage.**

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

(b) Consent required under this Section must be obtained prior to the collection, sharing, 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, 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, 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.

(d) Exceptions. For the purposes of this Section, any regulated entity that is subject to and in compliance with HIPAA shall be deemed to be in compliance with consent requirements set forth in this Section.

**Section 35. Right to withdraw consent.**

(a) A consumer has the right to withdraw consent from the collection, sharing, sale or storage of the consumer's health data, consistent with the requirements of Section 30.

(b) Exceptions. Any regulated entity that is subject to and in compliance with HIPAA that collects, stores, or shares health data as protected health information pursuant to a valid HIPAA authorization from the consumer shall be deemed to be in compliance with this Section.

**Section 40. Prohibition on discriminatory practices.**

(a) It shall be unlawful for a regulated entity to engage in discriminatory practices against a consumer solely because they have not provided consent to the collection, sharing, sale, or storage of their 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 consumer;

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

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

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

(5) suggesting that the consumer 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 consumer to whom such health data relates has specifically requested from a regulated entity.

**Section 45. 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 50 of this Act. A regulated entity that receives a consumer request to confirm shall respond within 45 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 45 days of receipt of the consumer's request. The time period to provide the required confirmation may be extended once by an additional 45 calendar days when reasonably necessary, provided that the consumer is provided notice of the extension within the first 45-day period.

**Section 50. 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, except as provided in subsection (g).

(b) 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 45 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; 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.

(c) If a regulated entity stores any health data on archived or backup systems, it may delay compliance with the consumer’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 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.

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

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

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, provided that 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, when the entities' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided consent to such use of their health data;

(4) Comply with an applicable legal obligation, such as data retention requirements set forth in 210 ILCS 85/6 et seq., 45 CFR 164.316 and 45 CFR 164.530;

(5) Comply with an applicable legal obligation if the regulated entity has been notified, in writing by an attorney that there is litigation pending in court involving the consumer's health data as possible evidence and that the consumer is their client or is the person who has instituted such litigation against their client, then the regulated entity shall retain the record of that consumer 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 such record has been concluded or for a period of five (5) years from the date that the record was produced, whichever occurs first in time; or

(6) Otherwise use the consumer's health data, internally, in a lawful manner that is compatible with the context in which the consumer provided their health data. This includes quality assurance activities to the extent permissible under HIPAA.

**Section 55. Authentication of consumer identity.**

(a) A regulated entity that receives a consumer request to confirm or delete may take reasonable measures to authenticate the consumer's

identity to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three (3) pieces of personal information provided by the consumer with personal information maintained by the regulated entity that it has determined to be reliable for the purpose of authenticating the consumer together with a signed declaration under penalty of perjury that the consumer making the request is the consumer 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 a consumer's identity available to consumers, and shall maintain all signed declarations as part of its record-keeping obligations.

(b) A regulated entity is not required to comply with a consumer request to confirm or delete if the regulated entity, using commercially reasonable efforts, is unable to authenticate the identity of the consumer making the request. In the event a regulated entity is unable to authenticate the consumer's identity, the regulated entity shall inform the consumer that it was unable to authenticate the consumer's identity, and advise the consumer of other methods, if available, of authenticating their identity.

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

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

**Section 60. Consumer health data security and minimization.**

(a) A regulated entity shall restrict access to health data by the employees, processors, service providers, and contractors of such regulated entity to only those employees, processors, 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.

(c) For the purposes of this Section 60 only, any regulated entity that is subject to and in compliance with the Privacy, Security, and Breach Notification 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, established pursuant HIPAA, shall be deemed to be in compliance with this Section.

**Section 65. 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 70. 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 75. 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 80. Conflict with other laws.**

(a) Nothing in this Act shall be construed to conflict with HIPAA.

(b) 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, including 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.

(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.

(d) This Act shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations.