STATE OF NEW YORK

10357

IN ASSEMBLY

February 26, 2026

Introduced by M. of A. ROSENTHAL, REYES, DINOWITZ, SIMON, GLICK, CUNNINGHAM, TAPIA, SHIMSKY, BICHOTTE HERMELYN, BURDICK, BRAUNSTEIN, LUCAS, SEAWRIGHT, STIRPE, KIM, DILAN, TAYLOR, SEPTIMO, GONZALEZ-ROJAS, LEVENBERG, MITAYNES, RAMOS, OTIS, WEPRIN, KELLES, LEE, O'PHARROW, PHEFFER AMATO, GALLAGHER, ROMERO -- read once and referred to the Committee on Science and Technology

AN ACT to amend the general business law, in relation to providing for the protection of health information

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The general business law is amended by adding a new article 42-A to read as follows:

ARTICLE 42-A

NEW YORK HEALTH INFORMATION PRIVACY ACT

Section 1120. Definitions.
1121. Requirements for communications to individuals.
1122. Lawfulness of processing regulated health information.
1123. Individual rights.
1124. Security.
1125. Service providers.
1126. Exemptions.
1127. Enforcement.
1128. Contracts and waivers void and unenforceable.
1129. Construction.

§ 1120. Definitions. As used in this article, the following terms shall have the following meanings:

1. "Deidentified information" means information that cannot reasonably be used to infer information about, or otherwise be linked to an identified or identifiable individual, household, or device, provided that the regulated entity or service provider that processes the information:

(a) Implements reasonable technical safeguards to ensure that the information cannot be associated with an individual, household, or device;

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD01741-06-6

(b) Publicly commits to process the information only as deidentified information and not attempt to reidentify the information, except that the regulated entity or service provider may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section;

(c) Contractually obligates any recipient of the deidentified information to comply with all requirements of this section; and

(d) Any deidentified information not otherwise exempt under this article, once subsequently reidentified shall not be considered deidentified.

2. "Regulated health information" means any information that:

(a) is reasonably linkable, directly or indirectly, to one or more identified or identifiable individuals, including by for example and without limitation, any 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; and

(b) is collected or processed in connection with an identified or identifiable individual's past, present, or future physical or mental health status. Such status includes but is not limited to:

(i) individual health conditions, treatments, diseases, or diagnoses;

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

(iii) surgeries or medical procedures;

(iv) use or purchase of medication;

(v) bodily functions, vital signs, symptoms, or measurements of the information;

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

(vii) gender-affirming care information;

(viii) reproductive or sexual health information;

(ix) biometric data;

(x) genetic data;

(xi) precise location information that could reasonably indicate an individual's attempt to acquire or receive health services or supplies;

(xii) data that identifies an individual seeking health care services; and

(xiii) any information that a regulated entity or their processor, processes to associate or identify an individual with a physical or mental health status, that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

Regulated health information shall not include deidentified information.

3. "Process" or "processing" means an operation or set of operations performed on regulated health information, including but not limited to the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, licensing, or modification of regulated health information.

4. "Regulated entity" means any entity that controls the processing of regulated health information of an individual (a) who is a New York resident or (b) is physically present in New York while that individual is in New York or (c) is seeking or receiving services in New York if the entity is located in New York.

5. "Sell" means to share regulated health information for monetary or other valuable consideration. Selling does not include the sharing of regulated health information for monetary or other valuable consideration to a third party as an asset that is part of a merger, acquisi-

tion, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets.

6. "Service provider" means any person or entity that processes regulated health information on behalf of a regulated entity. A service provider may also be a regulated entity depending upon the context in which regulated health information is processed.

7. "Third party" means a person or entity other than the individual, regulated entity, or service provider involved in a transaction or occurrence that involves regulated health information. A third party may also be a regulated entity or service provider depending upon the context in which regulated health information is processed.

8. "Individual" means a natural person acting in an individual or household context.

9. "Verifiable" means to use reasonable means to determine that a request to exercise any of the rights afforded in this act is being made by, or on behalf of, the individual who is entitled to exercise such rights with respect to the regulated health information at issue; provided that any additional personal information a regulated entity requests for the purpose of verification must be strictly necessary for the purpose of confirming the identity of such individual and shall not be processed or used for any purpose other than verifying the identity of the individual and shall be deleted immediately upon verification or failure to verify the individual. Such verification shall not extend the maximum allowable time within which the regulated entity may satisfy a request by an individual.

§ 1121. Requirements for communications to individuals. All notices, disclosures, forms, and other communications to individuals provided pursuant to this article shall comply with the following:

1. All communications shall use plain, straightforward language, avoiding technical or legal jargon, and must be provided through an interface the individual regularly uses in connection with the regulated entity's product or service.

2. All communications shall be reasonably accessible to individuals with disabilities, including by:

(a) utilizing digital accessibility tools;

(b) for notices, complying with generally recognized industry standards, including, but not limited to, current standards set by standards setting bodies such as the World Web Consortium, or other similar standards setting bodies as determined by the attorney general; and

(c) for other communications, providing information about how an individual with a disability may access the communication in an alternative format.

3. All communications shall be available in the languages in which the regulated entity provides information via its website and services. Any direct communication to an individual shall be provided in the language in which the individual ordinarily interacts with the regulated entity or its service provider.

4. A regulated entity shall make any notice for processing pursuant to a permissible purpose, pursuant to subparagraph (ii) of paragraph (b) of subdivision one of section eleven hundred twenty-two of this article, or form for processing pursuant to authorization, pursuant to subparagraph (i) of paragraph (b) of subdivision one of section eleven hundred twenty-two of this article, publicly available on its website. If an authorization form is customized for each individual, the regulated entity may instead publicly post a sample authorization form on its website.

§ 1122. Lawfulness of processing regulated health information. 1. It shall be unlawful for a regulated entity to:

(a) sell an individual's regulated health information to a third party; or

(b) otherwise process an individual's regulated health information unless:

(i) The individual has provided valid authorization for such processing as set forth in paragraph (b) of subdivision two of this section; or

(ii) Processing of an individual's regulated health information is strictly necessary for the purpose of:

(A) providing, maintaining, developing, improving, or repairing a specific product, feature, or service requested by such individual, or functionality thereof;

(B) conducting the regulated entity's internal business operations, which exclude any activities related to marketing, advertising, research and development, or providing products or services to third parties;

(C) protecting against malicious, fraudulent, or illegal activity;

(D) detecting, responding to, or preventing security incidents or threats;

(E) protecting the vital interests of an individual;

(F) investigating, establishing, exercising, preparing for, or defending legal claims; or

(G) complying with the regulated entity's legal obligations pursuant to federal, state or local law or regulation.

2. Unless processing of an individual's regulated health information is strictly necessary pursuant to subparagraph (ii) of paragraph (b) of subdivision one of this section, a regulated entity that processes regulated health information pursuant to valid authorization as required by subparagraph (i) of paragraph (b) of subdivision one of this section shall comply with the following:

(a) A request for authorization to process an individual's regulated health information shall:

(i) be made separately from any other transaction or part of a transaction;

(ii) be written in plain language and in no less than twelve point font;

(iii) clearly and conspicuously state that the processing for which the consent is requested is not strictly necessary, and that the user may decline without preventing continued use of the website, online service, online application, mobile device, connected device, or any other service the user is requesting or signing up for;

(iv) be made in the absence of any mechanism that has the purpose or substantial effect of obscuring, subverting, or impairing an individual's decision-making regarding authorization for processing;

(v) if requesting authorization for multiple categories of processing activities, allow the individual to provide or withhold authorization separately for each category of processing activity; and

(vi) not include any request for authorization for a processing activity for which an individual has withheld or revoked authorization within the past nine months.

(b) A valid authorization shall include:

(i) the types of regulated health information to be processed;

(ii) the nature of the processing activity;

(iii) the specific purposes for such processing;

(iv) the names where readily available, or categories of service providers and third parties to which the regulated entity may disclose

the individual's regulated health information and the purposes for such disclosure, including the circumstances under which the regulated entity may disclose regulated health information to law enforcement;

(v) any monetary or other valuable consideration the regulated entity may receive in connection with processing the individual's regulated health information, where applicable;

(vi) that failing to provide authorization will not affect the individual's experience of using the regulated entity's products or services;

(vii) the expiration date of the authorization, which may be up to one year from the date authorization was provided;

(viii) the mechanism by which the individual may revoke authorization prior to expiration;

(ix) the mechanism by which the individual may request access to and deletion of their regulated health information;

(x) any other information material to an individual's decision-making regarding authorization for processing; and

(xi) the signature or other form of unambiguous affirmative consent, which may be electronic, of the individual who is the subject of the regulated health information, or a parent or guardian authorized by law to take actions of legal consequence on behalf of the individual who is the subject of the regulated health information, and the date.

(c) (i) A regulated entity that receives authorization for processing shall provide an effective, efficient, and easy-to-use mechanism by which an individual may revoke authorization at any time through an interface the individual regularly uses in connection with the regulated entity's product or service.

(ii) Upon an individual's verifiable revocation of authorization, the regulated entity shall immediately cease all processing activities for which authorization was revoked, except to the extent necessary to comply with the regulated entity's legal obligations.

(iii) For individuals who have an online account with the regulated entity, the regulated entity must provide, in a conspicuous and easily accessible place within the account settings, a list of all processing activities for which the individual has provided authorization and, for each processing activity, allow the individual to revoke authorization in the same place with one motion or action.

(d) Upon obtaining valid authorization from an individual, the regulated entity shall provide that individual a copy of the authorization. The authorization shall be provided in a manner that is capable of being retained by the individual.

(e) The regulated entity shall limit its processing to what was clearly disclosed to an individual pursuant to paragraph (b) of this subdivision when the regulated entity received authorization from the individual.

(f) If the regulated entity seeks to materially alter its processing activities for regulated health information collected pursuant to authorization, the regulated entity shall obtain a new authorization for the new or altered processing activity.

(g) Providing a product or service requested by an individual must not be made contingent on providing authorization. The regulated entity must not discriminate against an individual for withholding authorization, such as by charging different prices or rates for products or services, including through the use of discounts or other benefits, imposing penalties, or providing a different level or quality of services or goods to the individual.

3. A regulated entity that processes regulated health information pursuant to a permissible purpose pursuant to subparagraph (ii) of paragraph (b) of subdivision one of this section shall comply with the following:

(a) A regulated entity shall provide clear and conspicuous notice that describes:

(i) the types of regulated health information to be processed;

(ii) the nature of the processing activity;

(iii) the specific purposes for such processing;

(iv) the names where readily available, or categories of service providers and third parties to which the regulated entity may disclose the individual's regulated health information and the purposes for such disclosure, including the circumstances under which the regulated entity may disclose regulated health information to law enforcement; and

(v) the mechanism by which the individual may request access to and deletion of their regulated health information.

(b) If the regulated entity materially alters its processing activities for regulated health information collected pursuant to a permissible purpose, the regulated entity must provide a clear and conspicuous notice in plain language, separate from a privacy policy, terms of service, or similar document, that describes any material changes to the processing activities and provide the individual with an opportunity to request deletion of their regulated health information.

§ 1123. Individual rights. 1. (a) A regulated entity shall make available an effective, efficient, and easy-to-use mechanism through an interface the individual regularly uses in connection with the regulated entity's product or service by which an individual may make verifiable requests under this section.

(b) The regulated entity shall, without undue delay and no later than within thirty days of receiving a verifiable access request, make available a copy of all regulated health information about the individual that the regulated entity maintains or that service providers maintain on behalf of the regulated entity. A regulated entity may extend the period within which to make available such copy one time by thirty additional days when reasonably necessary, as long as the regulated entity provides notice of such extension to the individual during the original thirty day period.

2. (a) A regulated entity shall make available an effective, efficient, and easy-to-use mechanism through an interface the individual regularly uses in connection with the regulated entity's product or service by which an individual may request the deletion of their regulated health information.

(b) An individual's request to delete or cancel their online account shall be treated as a request to delete the individual's regulated health information.

(c) The regulated entity shall, without undue delay and no later than within thirty days of receiving a verifiable deletion request:

(i) Delete all regulated health information associated with the individual in the regulated entity's possession or control, except to the extent necessary to comply with the regulated entity's legal obligations; and

(ii) Unless it proves impossible or involves disproportionate effort that is documented in writing by the regulated entity, communicate such request to each service provider or third party that processed the individual's regulated health information in connection with a transaction

involving the regulated entity occurring within one year preceding the individual's request.

(d) Any service provider or third party that receives notice of an individual's deletion request shall within thirty days delete all regulated health information associated with the individual in its possession or control, except to the extent necessary to comply with its legal obligations.

3. Any right set forth in this section may be exercised at any time by the individual who is the subject of the regulated health information or an agent authorized by such individual.

§ 1124. Security. 1. A regulated entity shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of regulated health information.

2. A regulated entity must securely dispose of an individual's regulated health information pursuant to a publicly available retention schedule within a reasonable time, and in no event later than sixty days, after it is no longer necessary to maintain for the permissible purpose or purposes identified in the notice or for which the individual provided valid authorization.

§ 1125. Service providers. 1. Any processing of regulated health information by a service provider on behalf of a regulated entity shall be governed by a written, binding agreement. Such agreement shall clearly set forth instructions for processing regulated health information, the nature and purpose of processing, the duration of processing, and the rights and obligations of both parties.

2. An agreement pursuant to subdivision one of this section shall require that the service provider:

(a) ensure that each person processing regulated health information is subject to a duty of confidentiality with respect to such information;

(b) protect regulated health information in a manner consistent with the requirements of this article;

(c) process regulated health information only when and to the extent necessary to comply with its obligations to the regulated entity;

(d) not combine the regulated health information which the service provider receives from or on behalf of the regulated entity with any other personal information which the service provider receives from or on behalf of another party or collects from its own relationship with individuals;

(e) comply with any exercises of an individual's rights under section eleven hundred twenty-three of this article upon the request of the regulated entity and notify any service providers or third parties to which it disclosed regulated health information of the request;

(f) delete or return all regulated health information to the regulated entity at the end of the provision of services, unless retention of the regulated health information is required by law;

(g) upon the reasonable request of the regulated entity, make available to the regulated entity all data in its possession necessary to demonstrate the service provider's compliance with the obligations in this section;

(h) allow, and cooperate with, reasonable assessments by the regulated entity or the regulated entity's designated assessor for purposes of evaluating compliance with the obligations of this article. Alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations

under this article using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The service provider shall provide a report of such assessment to the regulated entity upon request;

(i) notify the regulated entity a reasonable time in advance before disclosing or transferring regulated health information to any further service providers, which may be in the form of a regularly updated list of further service providers that may access regulated health information; and

(j) engage any further service provider pursuant to a written, binding agreement that includes the contractual requirements provided in this section, containing at minimum the same obligations that the service provider has entered into with regard to regulated health information.

§ 1126. Exemptions. Nothing in this article shall apply to the following, and the attorney general may promulgate rules and regulations specifying additional exceptions for regulated health information that is subject to and processed in compliance with any federal law that is as protective or more protective of individual privacy than this chapter:

1. local, state, or federal governments and their agencies, authorities or public corporations as defined in section sixty-six of the general construction law or information processed by or on behalf of such governmental entities provided that the information is only processed for governmental purposes;

2. information that meets the definition of protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and implementing regulations as well as the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5) and implementing regulations;

3. any covered entity governed by 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 (CFR), established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191);

4. any business associate governed by 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 (CFR), established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) to the extent the business associate maintains the information in the same manner as described in subdivision two of this section for protected health information or deidentifies such information in accordance with requirements for deidentification set forth in section eleven hundred twenty of this article;

5. a program or qualified service organization or records subject to 42 USC Section 290dd-2 and 42 CFR Part 2;

6. information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration;

7. information and documents lawfully subject to the federal Health Care Quality Improvement Act of 1986 (42 USC Sections 11101 - 11152), and implementing federal regulations;

8. patient safety work product subject to 42 CFR Part 3, established pursuant to 42 USC Sections 299b-21 through 299b-26;

9. deidentified protected health information, as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), that is deidentified in accordance with the requirements for deidentification set forth in 45 CFR Section 164.514;

10. identifiable private information for purposes of the federal policy for the protection of human subjects, 45 C.F.R. Part 46; 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; the protection of human subjects under 21 C.F.R. Parts 50 and 56; data used or shared in research, as defined in 45 CFR 164.501, and subject to 45 CFR 164.512(i); or data used or shared in research conducted in accordance with one or more of the requirements set forth in this section;

11. data used or disclosed only for one or more of the following:

(a) product registration and tracking consistent with applicable United States Food and Drug Administration regulations and guidance;

(b) public health activities and purposes as described in and subject to 45 CFR Section 164.512;

(c) part of a limited data set, as defined, and is used, disclosed, and maintained in the manner required by 45 CFR Section 164.514; or

(d) activities related to quality, safety, or effectiveness regulated by the United States Food and Drug Administration;

12. information subject to the Trusted Exchange Framework and Common Agreement (TEFCA) created by the U.S. Department of Health & Human Services Assistant Secretary for Technology Policy (ASTP), or through other networks that exchange information about individuals, including but not limited to health information or social services information, and are approved in accordance with the statewide common participation agreement and policies and procedures adopted pursuant to 10 NYCRR Part 300;

13. information specifically for a quality assurance committee, peer review committee, or quality improvement committee for purposes of section twenty-eight hundred five-j, twenty-eight hundred five-k, or twenty-eight hundred five-l of the public health law;

14. health information collected, used, or disclosed subject to section eighteen of the public health law;

15. directory information subject to the Family Educational Rights and Privacy Act, 20 U.S.C. §§ 1232g et seq., as amended from time to time;

16. personal information subject to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and implementing regulations when used for the purpose of furnishing a consumer credit report under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and implementing regulations;

17. data used for research and development only if deidentified in accordance with the requirements for deidentification set forth in section eleven hundred twenty of this article, and reviewed and approved by an Institutional Review Board;

18. any other information, which may be deemed to be regulated health information under this section, but which is subject to, and which is processed in compliance with, any other privacy laws or regulations that are as or more protective of individual privacy than this chapter;

19. information that:

(a) is collected by a business about an individual in the course of the individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the individual's personal information is collected and used by the business solely within

the context of the individual's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business;

(b) is collected by a business that is emergency contact information of the individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the information is collected and used solely within the context of having an emergency contact on file; or

(c) is necessary for the business to retain to administer benefits for another individual relating to the individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the information is collected and used solely within the context of administering those benefits;

20. information collected, created or maintained pursuant to sections 33.13 and 33.16 of the mental hygiene law; or

21. entities licensed, registered or certified by the office of children and family services, which are required to process information by the regulations of such office.

§ 1127. Enforcement. 1. Whenever it appears to the attorney general, either upon complaint or otherwise, that any person or persons, within or outside the state, has engaged in or is about to engage in any of the acts or practices stated to be unlawful under this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits obtained directly or indirectly by any such violation, to obtain civil penalties of not more than fifteen thousand dollars per violation and to obtain any such other and further relief as the court may deem proper, including preliminary relief. In determining the penalty, the court shall consider the severity of the violation and the regulated entity's good faith effort to comply with the requirements of this article.

2. The remedies provided by this section shall be in addition to any other lawful remedy available.

3. Any action or special proceeding brought by the attorney general pursuant to this section must be commenced within six years of the date on which the attorney general became aware of the violation.

4. In connection with any proposed action or special proceeding under this section, the attorney general is authorized to take proof and make a determination of the relevant facts, and to issue subpoenas in accordance with the civil practice law and rules. The attorney general may also require such other data and information as they may deem relevant and may require written responses to questions under oath. Such power of subpoena and examination shall not abate or terminate by reason of any action or special proceeding brought by the attorney general under this article.

5. This section shall apply to all acts declared to be unlawful in this article, whether or not subject to any other law of this state, and shall not supersede, amend or repeal any other law of this state under which the attorney general is authorized to take any action or conduct any inquiry.

6. The attorney general may promulgate such rules and regulations as are necessary to effectuate and enforce the provisions of this section.

§ 1128. Contracts and waivers void and unenforceable. 1. Any contractual provision inconsistent with this article shall be void and unenforceable.

2. Any waiver by any individual of the provisions of this article shall be void and unenforceable.

§ 1129. Construction. Nothing in this article shall be construed to restrict, invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or disclosures to the New York State Department of Health for public health activities, or health oversight activities, including, but not limited to, any disclosures permitted by 45 CFR 164.512(b) and (d).

§ 2. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. It is hereby declared to be the intent of the legislature that this act would have been enacted even if such invalid provisions had not been included herein.

§ 3. This act shall take effect 6 months after it shall have become a law. Effective immediately, the addition, amendment and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized to be made and completed on or before such effective date.