

# STATE OF NEW YORK

158--E

Cal. No. 76

2023-2024 Regular Sessions

## IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sens. KRUEGER, BROUK, COMRIE, FERNANDEZ, HINCHEY, HOYLMAN-SIGAL, JACKSON, LIU, MAY, WEBB -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, amended and ordered reprinted, retaining its place in the order of third reading -- again amended and ordered reprinted, retaining its place in the order of third reading -- recommitted to the Committee on Health in accordance with Senate Rule 6, sec. 8 -- reported favorably from said committee, ordered to first and second report, amended on second report, ordered to a third reading, and to be reprinted as amended, retaining its place in the order of third reading -- reported favorably from said committee to third reading, amended and ordered reprinted, retaining its place in the order of third reading -- passed by Senate and delivered to the Assembly, recalled, vote reconsidered, restored to third reading, amended and ordered reprinted, retaining its place in the order of third reading

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:

1 Section 1. The general business law is amended by adding a new article  
2 42 to read as follows:

### ARTICLE 42

#### NEW YORK HEALTH INFORMATION PRIVACY ACT

##### Section 1100. Definitions.

6 1101. Requirements for communications to individuals.

7 1102. Lawfulness of processing regulated health information.

8 1103. Individual rights.

9 1104. Security.

10 1105. Service providers.

11 1106. Exemptions.

12 1107. Enforcement.

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

LBD01105-16-4

1108. Contracts and waivers void and unenforceable.

§ 1100. 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 a particular 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;

(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; and

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

2. "Regulated health information" means any information that is reasonably linkable to an individual, or a device, and is collected or processed in connection with the physical or mental health of an individual. Location or payment information that relates to an individual's physical or mental health or any inference drawn or derived about an individual's physical or mental health that is reasonably linkable to an individual, or a device, shall be considered, without limitation, regulated health information. 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, disposal, licensing, destruction, deletion, modification, or deidentification of regulated health information.

4. "Regulated entity" means any entity that (a) controls the processing of regulated health information of an individual who is a New York resident, (b) controls the processing of regulated health information of an individual who is physically present in New York while that individual is in New York, or (c) is located in New York and controls the processing of regulated health information. A regulated entity may also be a service provider depending upon the context in which regulated health information is processed.

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, acquisition, 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.

1 § 1101. Requirements for communications to individuals. All notices,  
2 disclosures, forms, and other communications to individuals provided  
3 pursuant to this article shall comply with the following:

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

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

10 (a) utilizing digital accessibility tools;

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

15 (c) for other communications, providing information about how an indi-  
16 vidual with a disability may access the communication in an alternative  
17 format.

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

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

31 § 1102. Lawfulness of processing regulated health information. 1. In  
32 general, it shall be unlawful for a regulated entity to:

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

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

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

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

41 (A) providing or maintaining a specific product or service requested  
42 by such individual;

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

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

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

49 (E) protecting the vital interests of an individual;

50 (F) investigating, establishing, exercising, preparing for, or defend-  
51 ing legal claims; or

52 (G) complying with the regulated entity's legal obligations.

53 2. Unless processing of an individual's regulated health information  
54 is strictly necessary pursuant to subparagraph (ii) of paragraph (b) of  
55 subdivision one of this section, a regulated entity that processes regu-  
56 lated health information pursuant to valid authorization as required by

1 subparagraph (i) of paragraph (b) of subdivision one of this section  
2 shall comply with the following:

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

5 (i) be made separately from any other transaction or part of a trans-  
6 action;

7 (ii) be made at least twenty-four hours after an individual creates an  
8 account or first uses the requested product or service;

9 (iii) be made in the absence of any mechanism that has the purpose or  
10 substantial effect of obscuring, subverting, or impairing an individ-  
11 ual's decision-making regarding authorization for processing;

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

15 (v) not include any request for authorization for a processing activ-  
16 ity for which an individual has withheld or revoked authorization within  
17 the past calendar year.

18 (b) A valid authorization shall include:

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

20 (ii) the nature of the processing activity;

21 (iii) the specific purposes for such processing;

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

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

30 (vi) that failing to provide authorization will not affect the indi-  
31 vidual's experience of using the regulated entity's products or  
32 services;

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

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

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

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

41 (xi) the signature, which may be electronic, of the individual who is  
42 the subject of the regulated health information, or a parent or guardian  
43 authorized by law to take actions of legal consequence on behalf of the  
44 individual who is the subject of the regulated health information, and  
45 the date.

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

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

55 (iii) For individuals who have an online account with the regulated  
56 entity, the regulated entity must provide, in a conspicuous and easily

1 accessible place within the account settings, a list of all processing  
2 activities for which the individual has provided authorization and, for  
3 each processing activity, allow the individual to revoke authorization  
4 in the same place with one motion or action.

5 (d) Upon obtaining valid authorization from an individual, the regu-  
6 lated entity shall provide that individual a copy of the authorization.  
7 The authorization shall be provided in a manner that is capable of being  
8 retained by the individual.

9 (e) The regulated entity shall limit its processing to what was clear-  
10 ly disclosed to an individual pursuant to paragraph (b) of this subdivi-  
11 sion when the regulated entity received authorization from the individ-  
12 ual.

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

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

24 3. A regulated entity that processes regulated health information  
25 pursuant to a permissible purpose pursuant to subparagraph (ii) of para-  
26 graph (b) of subdivision one of this section shall comply with the  
27 following:

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

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

31 (ii) the nature of the processing activity;

32 (iii) the specific purposes for such processing;

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

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

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

47 § 1103. Individual rights. 1. (a) A regulated entity shall make avail-  
48 able an effective, efficient, and easy-to-use mechanism through an  
49 interface the individual regularly uses in connection with the regulated  
50 entity's product or service by which an individual may request access to  
51 their regulated health information.

52 (b) Within thirty days of receiving an access request, the regulated  
53 entity shall make available a copy of all regulated health information  
54 about the individual that the regulated entity maintains or that service  
55 providers maintain on behalf of the regulated entity.

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

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

9 (c) Within thirty days of receiving a deletion request, the regulated  
10 entity shall:

11 (i) Delete all regulated health information associated with the indi-  
12 vidual in the regulated entity's possession or control, except to the  
13 extent necessary to comply with the regulated entity's legal obli-  
14 gations; and

15 (ii) Unless it proves impossible or involves disproportionate effort  
16 that is documented in writing by the regulated entity, communicate such  
17 request to each service provider or third party that processed the indi-  
18 vidual's regulated health information in connection with a transaction  
19 involving the regulated entity occurring within one year preceding the  
20 individual's request.

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

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

29 § 1104. Security. 1. In general, a regulated entity shall develop,  
30 implement, and maintain reasonable administrative, technical, and phys-  
31 ical safeguards to protect the security, confidentiality, and integrity  
32 of regulated health information.

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

39 § 1105. Service providers. 1. In general, any processing of regulated  
40 health information by a service provider on behalf of a regulated entity  
41 shall be governed by a written, binding agreement. Such agreement shall  
42 clearly set forth instructions for processing regulated health informa-  
43 tion, the nature and purpose of processing, the duration of processing,  
44 and the rights and obligations of both parties.

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

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

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

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

53 (d) not combine the regulated health information which the service  
54 provider receives from or on behalf of the regulated entity with any  
55 other personal information which the service provider receives from or

1 on behalf of another party or collects from its own relationship with  
2 individuals;

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

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

10 (g) upon the reasonable request of the regulated entity, make avail-  
11 able to the regulated entity all data in its possession necessary to  
12 demonstrate the service provider's compliance with the obligations in  
13 this section;

14 (h) allow, and cooperate with, reasonable assessments by the regulated  
15 entity or the regulated entity's designated assessor for purposes of  
16 evaluating compliance with the obligations of this article. Alterna-  
17 tively, the service provider may arrange for a qualified and independent  
18 assessor to conduct an assessment of the service provider's policies and  
19 technical and organizational measures in support of the obligations  
20 under this article using an appropriate and accepted control standard or  
21 framework and assessment procedure for such assessments. The service  
22 provider shall provide a report of such assessment to the regulated  
23 entity upon request;

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

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

33 § 1106. Exemptions. Nothing in this article shall apply to:

34 1. information processed by local, state, and federal governments, and  
35 municipal corporations;

36 2. protected health information that is collected by a covered entity  
37 or business associate governed by the privacy, security, and breach  
38 notification rules issued by the United States Department of Health and  
39 Human Services, Parts 160 and 164 of Title 45 of the Code of Federal  
40 Regulations, established pursuant to the Health Insurance Portability  
41 and Accountability Act of 1996 (Public Law 104-191) and the Health  
42 Information Technology for Economic and Clinical Health Act (Public Law  
43 111-5);

44 3. any covered entity governed by the privacy, security, and breach  
45 notification rules issued by the United States Department of Health and  
46 Human Services, Parts 160 and 164 of Title 45 of the Code of Federal  
47 Regulations, established pursuant to the Health Insurance Portability  
48 and Accountability Act of 1996 (Public Law 104-191), to the extent the  
49 covered entity maintains patient information in the same manner as  
50 protected health information as described in subdivision two of this  
51 section; and

52 4. information collected as part of a clinical trial subject to the  
53 Federal Policy for the Protection of Human Subjects, also known as the  
54 Common Rule, pursuant to good clinical practice guidelines issued by the  
55 International Council for Harmonisation or pursuant to human subject

1 protection requirements of the United States Food and Drug Adminis-  
2 tration.

3 § 1107. Enforcement. 1. Whenever it appears to the attorney general,  
4 either upon complaint or otherwise, that any person or persons, within  
5 or outside the state, has engaged in or is about to engage in any of the  
6 acts or practices stated to be unlawful under this article, the attorney  
7 general may bring an action or special proceeding in the name and on  
8 behalf of the people of the state of New York to enjoin any violation of  
9 this article, to obtain restitution of any moneys or property obtained  
10 directly or indirectly by any such violation, to obtain disgorgement of  
11 any profits obtained directly or indirectly by any such violation, to  
12 obtain civil penalties of not more than fifteen thousand dollars per  
13 violation or twenty percent of revenue obtained from New York consumers  
14 within the past fiscal year, whichever is greater, and to obtain any  
15 such other and further relief as the court may deem proper, including  
16 preliminary relief.

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

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

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

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

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

38 § 1108. Contracts and waivers void and unenforceable. 1. Any contrac-  
39 tual provision inconsistent with this article shall be void and unen-  
40 forceable.

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

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

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