

STATE OF NEW YORK

158--C

Cal. No. 76

2023-2024 Regular Sessions

IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sens. KRUEGER, COMRIE, HINCHEY, HOYLMAN-SIGAL, MAY -- 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

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.

13 § 1100. Definitions. As used in this article, the following terms
14 shall have the following meanings:

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

LBD01105-10-4

1 1. "Deidentified information" means information that cannot reasonably
2 be used to infer information about, or otherwise be linked to a partic-
3 ular individual, household, or device, provided that the regulated enti-
4 ty or service provider that processes the information:

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

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

13 (c) Contractually obligates any recipient of the deidentified informa-
14 tion to comply with all requirements of this section.

15 2. "Regulated health information" means any information that is
16 reasonably linkable to an individual, or a device, and is collected or
17 processed in connection with the physical or mental health of an indi-
18 vidual. Location or payment information that relates to an individual's
19 physical or mental health or any inference drawn or derived about an
20 individual's physical or mental health that is reasonably linkable to an
21 individual, or a device, shall be considered, without limitation, regu-
22 lated health information. Regulated health information shall not include
23 deidentified information.

24 3. "Process" or "processing" means an operation or set of operations
25 performed on regulated health information, including but not limited to
26 the collection, use, access, sharing, sale, monetization, analysis,
27 retention, creation, generation, derivation, recording, organization,
28 structuring, storage, disclosure, transmission, disposal, licensing,
29 destruction, deletion, modification, or deidentification of regulated
30 health information.

31 4. "Regulated entity" means any entity that (a) controls the process-
32 ing of regulated health information of an individual who is a New York
33 resident, (b) controls the processing of regulated health information of
34 an individual who is physically present in New York while that individ-
35 ual is in New York, or (c) is located in New York and controls the proc-
36 essing of regulated health information of an individual. A regulated
37 entity may also be a service provider depending upon the context in
38 which regulated health information is processed.

39 5. "Sell" means to share regulated health information for monetary or
40 other valuable consideration. Selling does not include the sharing of
41 regulated health information for monetary or other valuable consider-
42 ation to a third party as an asset that is part of a merger, acquisi-
43 tion, bankruptcy, or other transaction in which the third party assumes
44 control of all or part of the regulated entity's assets.

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

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

54 § 1101. Requirements for communications to individuals. All notices,
55 disclosures, forms, and other communications to individuals provided
56 pursuant to this article shall comply with the following:

1 1. In general, all communications shall use plain, straightforward
2 language, avoiding technical or legal jargon, and must be provided
3 through an interface regularly used in conjunction with the regulated
4 entity's product or service.

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

7 (a) utilizing digital accessibility tools;

8 (b) for notices, complying with generally recognized industry stand-
9 ards, including, but not limited to, the Web Content Accessibility
10 Guidelines, from the World Web Consortium, incorporated herein by refer-
11 ence; and

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

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

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

28 § 1102. Lawfulness of processing regulated health information. 1. In
29 general, it shall be unlawful for a regulated entity to:

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

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

34 (i) The individual has provided valid authorization for such process-
35 ing; or

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

38 (A) providing a product or service requested by such individual;

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

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

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

45 (E) protecting the vital interests of an individual or the public
46 interest in the area of public health;

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

49 (G) complying with federal, state, or local laws, rules, or regu-
50 lations; or

51 (H) complying with a court order, valid subpoena, or similar process
52 authorized under law, provided that for any subpoena or other lawful
53 process that is not in connection with a law enforcement inquiry, the
54 party requesting the information must provide prior notice to the indi-
55 vidual who is the subject of the requested information.

1 2. A regulated entity that processes regulated health information
2 pursuant to valid authorization as required by subparagraph (i) of para-
3 graph (b) of subdivision one of this section shall comply with the
4 following:

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

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

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

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

14 (iv) if requesting authorization for multiple categories of processing
15 activities, allow the individual to provide/withhold authorization sepa-
16 rately for each category of processing activity; and

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

20 (b) A valid authorization shall include:

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

22 (ii) the nature of the processing activity;

23 (iii) the specific purposes for such processing;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33 (ii) the nature of the processing activity;

34 (iii) the specific purposes for such processing;

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

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

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

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

54 (b) Within thirty days of receiving an access request, the regulated
55 entity shall make available a copy of all regulated health information

1 about the individual that the regulated entity maintains or that service
2 providers maintain on behalf of the regulated entity.

3 2. (a) A regulated entity shall make available an effective, effi-
4 cient, and easy-to-use mechanism through an interface regularly used in
5 conjunction with the regulated entity's product or service by which an
6 individual may request the deletion of their regulated health informa-
7 tion.

8 (b) An individual's deletion or cancellation of their online account
9 shall be treated as a request to delete the individual's regulated
10 health information.

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

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

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

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

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

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

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

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

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

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

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

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

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

1 other personal information which the service provider receives from or
2 on behalf of another party or collects from its own relationship with
3 individuals;

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

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

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

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

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

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

34 § 1106. Exemptions. Nothing in this article shall apply to:

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

37 2. protected health information that is collected by a covered entity
38 or business associate governed by the privacy, security, and breach
39 notification rules issued by the United States Department of Health and
40 Human Services, Parts 160 and 164 of Title 45 of the Code of Federal
41 Regulations, established pursuant to the Health Insurance Portability
42 and Accountability Act of 1996 (Public Law 104-191) and the Health
43 Information Technology for Economic and Clinical Health Act (Public Law
44 111-5);

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

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

protection requirements of the United States Food and Drug Administration;

5. information processed pursuant to the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) and its implementing regulations;

6. information processed pursuant to section two-d of the education law; and

7. information processed pursuant to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq).

§ 1107. 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 or twenty percent of revenue obtained from New York consumers within the past fiscal year, whichever is greater, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

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 he or she 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.

§ 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 July 1, 2025.