

# STATE OF NEW YORK

158--D

Cal. No. 76

2023-2024 Regular Sessions

## IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sens. KRUEGER, COMRIE, HINCHEY, HOYLMAN-SIGAL, JACKSON, 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 -- reported favorably from said committee 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.

LBD01105-12-4

1 § 1100. Definitions. As used in this article, the following terms  
2 shall have the following meanings:

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

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

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

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

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

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

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

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

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

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

§ 1101. 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. In general, all communications shall use plain, straightforward language, avoiding technical or legal jargon, and must be provided through an interface regularly used in conjunction 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, the Web Content Accessibility Guidelines, from the World Web Consortium, incorporated herein by reference; 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 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 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.

§ 1102. Lawfulness of processing regulated health information. 1. In general, 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; or

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

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

(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 or the public interest in the area of public health;

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

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

2. 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:

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

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

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

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

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

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

16 (b) A valid authorization shall include:

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

18 (ii) the nature of the processing activity;

19 (iii) the specific purposes for such processing;

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

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

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

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

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

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

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

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

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

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

53 (iii) For individuals who have an online account with the regulated  
54 entity, the regulated entity must provide, in a conspicuous and easily  
55 accessible place within the account settings, a list of all processing  
56 activities for which the individual has provided authorization and, for

1 each processing activity, allow the individual to revoke authorization  
2 in the same place with one motion or action.

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

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

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

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

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

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

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

29 (ii) the nature of the processing activity;

30 (iii) the specific purposes for such processing;

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

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

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

45 § 1103. Individual rights. 1. (a) A regulated entity shall make avail-  
46 able an effective, efficient, and easy-to-use mechanism through an  
47 interface regularly used in conjunction with the regulated entity's  
48 product or service by which an individual may request access to their  
49 regulated health information.

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

54 2. (a) A regulated entity shall make available an effective, effi-  
55 cient, and easy-to-use mechanism through an interface regularly used in  
56 conjunction with the regulated entity's product or service by which an



1 individual may request the deletion of their regulated health informa-  
2 tion.

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

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

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

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

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

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

26 § 1104. Security. 1. In general, a regulated entity shall develop,  
27 implement, and maintain reasonable administrative, technical, and phys-  
28 ical safeguards to protect the security, confidentiality, and integrity  
29 of regulated health information.

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

36 § 1105. Service providers. 1. In general, any processing of regulated  
37 health information by a service provider on behalf of a regulated entity  
38 shall be governed by a written, binding agreement. Such agreement shall  
39 clearly set forth instructions for processing regulated health informa-  
40 tion, the nature and purpose of processing, the duration of processing,  
41 and the rights and obligations of both parties.

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

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

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

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

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

55 (e) comply with any exercises of an individual's rights under section  
56 eleven hundred three of this article upon the request of the regulated

1 entity and notify any service providers or third parties to which it  
2 disclosed regulated health information of the request;

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

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

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

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

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

29 § 1106. Exemptions. Nothing in this article shall apply to:

30 1. information processed by local, state, and federal governments, and  
31 municipal corporations;

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

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

48 4. information collected as part of a clinical trial subject to the  
49 Federal Policy for the Protection of Human Subjects, also known as the  
50 Common Rule, pursuant to good clinical practice guidelines issued by the  
51 International Council for Harmonisation or pursuant to human subject  
52 protection requirements of the United States Food and Drug Adminis-  
53 tration;

54 5. information processed pursuant to the federal Family Educational  
55 Rights and Privacy Act (20 U.S.C. Sec. 1232g) and its implementing regu-  
56 lations;

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

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

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

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

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

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

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

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

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

49 § 3. This act shall take effect July 1, 2025.