

# STATE OF NEW YORK

158--B

Cal. No. 429

2023-2024 Regular Sessions

## IN SENATE

(Prefiled)

January 4, 2023

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

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 to read as follows:

### ARTICLE 42

#### NEW YORK HEALTH INFORMATION PRIVACY ACT

##### Section 1100. Definitions.

1101. Requirements for communications to individuals.

1102. Lawfulness of processing regulated health information.

1103. Individual rights.

1104. Security.

1105. Service providers.

1106. Exemptions.

1107. Enforcement.

§ 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:

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

LBD01105-06-3

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

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

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

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

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

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

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

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

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

50 § 1101. Requirements for communications to individuals. All notices,  
51 disclosures, forms, and other communications to individuals provided  
52 pursuant to this article shall comply with the following:

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

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

3 (a) utilizing digital accessibility tools;

4 (b) for notices, complying with generally recognized industry stand-  
5 ards, including, but not limited to, the Web Content Accessibility  
6 Guidelines, version 2.1 of June 5, 2018, from the World Web Consortium,  
7 incorporated herein by reference; and

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

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

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

24 § 1102. Lawfulness of processing regulated health information. 1. In  
25 general, it shall be unlawful for a regulated entity to:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 (b) A valid authorization shall include:

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

12 (ii) the nature of the processing activity;

13 (iii) the specific purposes for such processing;

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

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

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

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

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

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

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

33 (xi) the signature, which may be electronic, of the individual who is  
34 the subject of the regulated health information, or a parent or guardian  
35 authorized by law to take actions of legal consequence on behalf of the  
36 individual who is the subject of the regulated health information, and  
37 the date.

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

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

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

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

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

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

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

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

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

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

23 (ii) the nature of the processing activity;

24 (iii) the specific purposes for such processing;

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

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

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

39 § 1103. Individual rights. 1. (a) A regulated entity shall make avail-  
40 able an effective, efficient, and easy-to-use mechanism through an  
41 interface regularly used in conjunction with the regulated entity's  
42 product or service by which an individual may request access to their  
43 regulated health information.

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

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

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



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

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

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

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

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

21 § 1104. Security. 1. In general, a regulated entity shall develop,  
22 implement, and maintain reasonable administrative, technical, and phys-  
23 ical safeguards to protect the security, confidentiality, and integrity  
24 of regulated health information.

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

31 § 1105. Service providers. 1. In general, any processing of regulated  
32 health information by a service provider on behalf of a regulated entity  
33 shall be governed by a written, binding agreement. Such agreement shall  
34 clearly set forth instructions for processing regulated health informa-  
35 tion, the nature and purpose of processing, the duration of processing,  
36 and the rights and obligations of both parties.

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

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

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

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

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

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

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

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

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

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

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

24 § 1106. Exemptions. Nothing in this article shall apply to:

25 1. information processed by local, state, and federal governments, and  
26 municipal corporations;

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

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

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

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

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

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

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

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

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

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

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

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

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

45     § 3. This act shall take effect July 1, 2024.