

# STATE OF NEW YORK

8448--D

## IN SENATE

June 3, 2020

Introduced by Sens. THOMAS, BAILEY, CARLUCCI, GOUNARDES, HOYLMAN, MAY, RAMOS, STAVISKY -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged and said bill committed to the Committee on Health -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT in relation to the collection of emergency health data and personal information and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof

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

- 1 Section 1. For the purposes of this act:
- 2 1. "Collect" means to buy, rent, gather, obtain, receive, or access
- 3 any personal information pertaining to an individual by any means,
- 4 online or offline, including but not limited to, receiving information
- 5 from the individual or from a third party, actively or passively, or
- 6 obtaining information by observing an individual's behavior.
- 7 2. "Covered entity" means any person, including a government entity:
- 8 (a) that collects, processes, or discloses emergency health data, as
- 9 defined in this act, electronically or through communication by wire or
- 10 radio; or
- 11 (b) that develops or operates a website, web application, mobile
- 12 application, mobile operating system feature, or smart device applica-
- 13 tion for the purpose of tracking, screening, monitoring, contact trac-
- 14 ing, or mitigation, or otherwise responding to the COVID-19 public
- 15 health emergency.
- 16 3. "De-identified information" means information that cannot reason-
- 17 ably identify, relate to, describe, be capable of being associated with,

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

LBD16478-14-0

1 or be linked, directly or indirectly, to a particular individual, house-  
2 hold, or device. A covered entity that uses de-identified information:

3 (a) has implemented technical safeguards that prohibit re-identifica-  
4 tion of the individual to whom the information may pertain;

5 (b) has implemented business processes that specifically prohibit  
6 re-identification of the information;

7 (c) has implemented business processes that prevent inadvertent  
8 release of de-identified information; and

9 (d) makes no attempt to re-identify the information.

10 4. "Disclose" means any action, set of actions, or omission in which a  
11 covered entity makes personal information available to another person,  
12 intentionally or unintentionally, including but not limited to, sharing,  
13 publishing, releasing, transferring, disseminating, making available,  
14 selling, leasing, providing access to, failing to restrict access to, or  
15 otherwise communicating orally, in writing, electronically, or by any  
16 other means.

17 5. "Emergency health data" means data linked or reasonably linkable to  
18 an individual, household, or device, including data inferred or derived  
19 about the individual, household, or device from other collected data  
20 provided such data is still linked or reasonably linkable to the indi-  
21 vidual, household, or device, that concerns the public COVID-19 health  
22 emergency. Such data includes:

23 (a) Information that reveals the past, present, or future physical or  
24 behavioral health or condition of, or provision of healthcare to, an  
25 individual including:

26 (i) data derived from the testing or examination;

27 (ii) whether or not an individual has contracted or been tested for,  
28 or an estimate of the likelihood that a particular individual may  
29 contract, such disease or disorder; and

30 (iii) genetic data, biological samples and biometrics; and

31 (b) Other data collected in conjunction with other emergency health  
32 data that can be used to infer health status, health history, location  
33 or associations, including:

34 (i) geolocation data, when such term means data capable of determining  
35 the past or present precise physical location of an individual at a  
36 specific point in time, taking account of population densities, includ-  
37 ing cell-site location information, triangulation data derived from  
38 nearby wireless or radio frequency networks and global positioning  
39 system data;

40 (ii) proximity data, when such term means information that identifies  
41 or estimates the past or present physical proximity of one individual or  
42 device to another, including information derived from Bluetooth, audio  
43 signatures, nearby wireless networks, and near field communications;

44 (iii) demographic data;

45 (iv) contact information for identifiable individuals or a history of  
46 the individual's contacts over a period of time, such as an address book  
47 or call log; and

48 (v) any other data collected from a personal device.

49 6. "Individual" means a natural person whom the covered entity knows  
50 or has reason to know is located in New York state.

51 7. "Personal information" means information that identifies, relates  
52 to, describes, is capable of being associated with, or could reasonably  
53 be linked, directly or indirectly, with a particular individual or  
54 household, or device.

55 8. "Process" means any operation or set of operations that are  
56 performed on personal data by either automated or not automated means.

1 9. "Public health authority" means the New York state department of  
2 health, a county health department or the New York city department of  
3 health and mental hygiene, or a person or entity acting under a grant of  
4 authority from or contract with such public agency, including the  
5 employees or agents of such public agency or its contractors or persons  
6 to entities to whom it has granted authority, that is responsible for  
7 public health matters as part of its official mandate.

8 § 2. Individual rights.

9 1. The individual's right to opt-in. (a) A covered entity shall obtain  
10 freely given, specific, informed, and unambiguous opt-in consent from an  
11 individual to:

12 (i) process the individual's personal information or emergency health  
13 data; and

14 (ii) make any changes in the processing of the individual's personal  
15 information or emergency health data.

16 (b) It shall be unlawful for a covered entity to collect, process, or  
17 disclose emergency health data or personal information unless:

18 (i) the individual to whom the data pertains has freely given, specif-  
19 ic, informed, and unambiguous consent to such collection, processing, or  
20 disclosure; or

21 (ii) such collection, processing, or disclosure is necessary and for  
22 the sole purpose of:

23 (A) protecting against malicious, deceptive, fraudulent, or illegal  
24 activity; or

25 (B) detecting, responding to, or preventing security incidents or  
26 threats.

27 (c) To the extent that a covered entity must process internet protocol  
28 addresses, system configuration information, URLs of referring pages,  
29 locale and language preferences, keystrokes, and other personal informa-  
30 tion in order to obtain individuals' freely given, specific, informed,  
31 and unambiguous opt-in consent, the entity:

32 (i) shall only process the personal information necessary to request  
33 freely given, specific, informed, and unambiguous opt-in consent;

34 (ii) shall process the personal information solely to request freely  
35 given, specific, informed, and unambiguous opt-in consent; and

36 (iii) shall immediately delete the personal information if consent is  
37 withheld or withdrawn.

38 2. The individual's right to privacy. (a) All emergency health data  
39 and personal information shall be collected at a minimum level of iden-  
40 tifiability reasonably needed for the completion of the transaction  
41 disclosed to, affirmatively consented to, and requested by the individ-  
42 ual. For a covered entity using proximity tracing or exposure notifica-  
43 tion this includes changing temporary anonymous identifiers at least  
44 once in a 20 minute period.

45 (b) A covered entity shall not process personal information or emer-  
46 gency health data beyond what is adequate, relevant, and necessary for  
47 the completion of the transaction disclosed to, affirmatively consented  
48 to, and requested by the individual.

49 (c) A covered entity shall not process emergency health data or  
50 personal information for any purpose not authorized under this act,  
51 including:

52 (i) commercial advertising, recommendation for e-commerce, or the  
53 training of machine learning algorithms related to, or subsequently for  
54 use in, commercial advertising and e-commerce;

1 (ii) soliciting, offering, selling, leasing, licensing, renting,  
2 advertising, marketing, or otherwise commercially contracting for  
3 employment, finance, credit, insurance, housing, or education; or

4 (iii) segregating, discriminating in, or otherwise making unavailable  
5 the goods, services, facilities, privileges, advantages, or accommo-  
6 dations of any place of public accommodation (as such term is defined in  
7 section 301 of the Americans with Disabilities Act of 1990), except as  
8 authorized by a state or federal government entity for a public health  
9 purpose; provided that a covered entity shall not process emergency  
10 health data or personal information to make categorical decisions about  
11 the allocation of care based on disability.

12 3. Covered entity privacy policy. (a) A covered entity shall provide  
13 to the individual a privacy policy, at a fourth grade reading level or  
14 below and in the language the entity regularly uses to communicate with  
15 the individual, prior to or at the point of collection of emergency  
16 health data or personal information:

17 (i) detailing how and for what purpose the covered entity collects,  
18 processes, and discloses emergency health data and personal information;

19 (ii) describing the covered entity's data retention and data security  
20 policies and practices for emergency health data and personal informa-  
21 tion; and

22 (iii) describing how an individual may exercise rights under this  
23 section.

24 (b) A covered entity shall create transparency reports, at least once  
25 every 90 days, that include:

26 (i) the number of individuals whose emergency health data or personal  
27 information the covered entity collected or processed;

28 (ii) the categories of emergency health data and personal information  
29 collected, processed, or disclosed;

30 (iii) the purposes for which each category of emergency health data or  
31 personal information was collected, processed, or disclosed;

32 (iv) the number of requests for individuals' emergency health data or  
33 personal information, including information on who the emergency health  
34 data or personal information was disclosed to; and

35 (v) the number of instances where emergency health data or personal  
36 information was produced, in whole or in part, without prior, explicit  
37 consents by the individuals specified in the request.

38 (c) The covered entity shall make each transparency report persistent-  
39 ly available and readily accessible on such entity's website.

40 4. Time limitation on retention. (a) Emergency health data and  
41 personal information shall be deleted when the initial purpose for  
42 collecting or obtaining such data has been satisfied or within 30 days,  
43 whichever occurs first, except that proximity tracing or exposure  
44 notification data which shall be automatically deleted every 14 days.

45 (b) This subdivision shall not apply to de-identified information.

46 5. Access rights. (a) Emergency health data and personal information  
47 shall be disclosed only as necessary to provide the service requested by  
48 an individual.

49 (b) A covered entity may share aggregate, de-identified data with  
50 public health authorities.

51 (c) A covered entity shall not disclose emergency health data or  
52 personal information to a third party unless that third party is  
53 contractually bound to the covered entity to meet the same privacy and  
54 security obligations as the covered entity.

55 (d) No covered entity in possession of emergency health data or  
56 personal information may disclose, redisclose, or otherwise disseminate

1 an individual's emergency health data or personal information unless the  
2 subject of the emergency health data or personal information or the  
3 subject's legally authorized representative consents in writing to the  
4 disclosure or redisclosure.

5 (e) Without consent under subdivision one of this section, emergency  
6 health data, personal information, and any evidence derived therefrom  
7 shall not be subject to or provided in response to any legal process or  
8 be admissible for any purpose in any judicial or administrative action  
9 or proceeding.

10 (f) Individuals shall have the right to access the emergency health  
11 data and personal information collected on them and correct any inaccuracies.  
12

13 (i) A covered entity must comply with an individual's request to  
14 correct emergency health data or personal information not later than 30  
15 days after receiving a verifiable request from the individual or, in the  
16 case of a minor, the individual's parent or guardian.

17 (ii) Where the covered entity has reasonable doubts or cannot verify  
18 the identity of the individual making a request under this paragraph,  
19 the covered entity may request additional information necessary for the  
20 specific purpose of confirming the identity of the individual. In such  
21 cases, the additional information shall not be processed for any purpose  
22 other than verifying the identity of the individual and must be deleted  
23 immediately upon verification or failure to verify the individual.

24 § 3. 1. A covered entity shall implement reasonable measures to ensure  
25 confidentiality, integrity, and availability of emergency health data  
26 and personal information.

27 2. A covered entity that collects an individual's emergency health  
28 data or personal information shall implement and maintain reasonable  
29 security procedures and practices, including administrative, physical,  
30 and technical safeguards, appropriate to the nature of the information  
31 and the purposes for which that information will be processed, to  
32 protect that information from unauthorized processing, disclosure,  
33 access, destruction, or modification.

34 3. A covered entity shall limit access to emergency health data and  
35 personal information to authorized essential personnel whose use of the  
36 data is reasonably necessary to operate the program and record who has  
37 accessed emergency health data or personal information, the date of  
38 access, and for what purposes.

39 § 4. 1. All covered entities shall be subject to annual data  
40 protection audits, conducted by a neutral third party auditor, evaluating  
41 the technology utilized and the development processes for statistical  
42 impacts on classes protected under section 296 of article 15 of  
43 the executive law, as well as for impacts on privacy and security, that  
44 includes at a minimum:

45 (a) a detailed description of the technology, its design, and its  
46 purpose;

47 (b) an assessment of the relative benefits and costs of the technology  
48 in light of its purpose, taking into account relevant factors including  
49 data minimization practices; the duration for which personal information  
50 and emergency health data and the results of the data analysis are  
51 stored; what information about the technology is available to the  
52 public; and the recipients of the results of the technology;

53 (c) an assessment of the risk of harm posed by the technology; the  
54 risk that the technology may result in or contribute to inaccurate,  
55 unfair, biased, or discriminatory decisions; the risk that the technology  
56 may dissuade New Yorkers from participating in contact tracing or

1 obtaining medical testing or treatment; and the risk that personal  
2 information or emergency health data can be accessed by third parties,  
3 including, but not limited to law enforcement agencies and U.S. Immi-  
4 gration and Customs Enforcement; and

5 (d) the measures the covered entity will employ to minimize the risks  
6 described in paragraph (c) of this subdivision, including technological,  
7 legal and physical safeguards;

8 (e) an assessment of whether the covered entity has followed through  
9 on the promises made in its privacy notice regarding collection, access,  
10 sharing, retention, deletion and sunseting; and

11 (f) if the technology utilizes machine-learning systems, a description  
12 of the training data information.

13 2. The covered entity shall make the audit persistently available and  
14 readily accessible on such entity's website.

15 3. The cost of the audit shall be paid by the covered entity.

16 § 5. The attorney general may bring an action in the name of the  
17 state, or as *parens patriae* on behalf of persons residing in the state,  
18 to enforce the provisions of this act. In an action brought by the  
19 attorney general, the court may award injunctive relief, including  
20 preliminary injunctions, to prevent further violations of and compel  
21 compliance with this act; civil penalties up to twenty-five thousand  
22 dollars per violation or up to four percent of annual revenue; other  
23 appropriate relief, including restitution, to redress harms to individ-  
24 uals or to mitigate all substantial risk of harm; and any other relief  
25 the court determines.

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

35 § 7. This act shall take effect on the thirtieth day after it shall  
36 have become a law and shall expire and be deemed repealed January 1,  
37 2023.