

STATE OF NEW YORK

8448--C

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

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

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

LBD16478-12-0

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

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

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

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

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

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

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

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

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

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

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

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

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

42 (iii) demographic data;

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

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

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

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

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

55 9. "Public health authority" means the New York state department of
56 health, a county health department or the New York city department of

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

6 § 2. Individual rights.

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

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

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

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

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

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

21 (A) protecting against malicious, deceptive, fraudulent, or illegal
22 activity; or

23 (B) detecting, responding to, or preventing security incidents or
24 threats.

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

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

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

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

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

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

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

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

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

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

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

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

(ii) describing the covered entity's data retention and data security policies and practices for emergency health data and personal information; and

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

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

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

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

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

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

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

(c) The covered entity shall make each transparency report persistently available and readily accessible on such entity's website.

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

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

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

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

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

(d) No covered entity in possession of emergency health data or personal information may disclose, redisclose, or otherwise disseminate an individual's emergency health data or personal information unless the subject of the emergency health data or personal information or the

1 subject's legally authorized representative consents in writing to the
2 disclosure or redisclosure.

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

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

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

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

22 § 3. 1. A covered entity shall implement reasonable measures to ensure
23 confidentiality, integrity, and availability of emergency health data
24 and personal information.

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

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

37 § 4. 1. All covered entities shall be subject to annual data
38 protection audits, conducted by a neutral third party auditor, evaluating
39 the technology utilized and the development processes for statistical
40 impacts on classes protected under section 296 of article 15 of
41 the executive law, as well as for impacts on privacy and security, that
42 includes at a minimum:

43 (a) a detailed description of the technology, its design, and its
44 purpose;

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

51 (c) an assessment of the risk of harm posed by the technology; the
52 risk that the technology may result in or contribute to inaccurate,
53 unfair, biased, or discriminatory decisions; the risk that the technology
54 may dissuade New Yorkers from participating in contact tracing or
55 obtaining medical testing or treatment; and the risk that personal
56 information or emergency health data can be accessed by third parties,

1 including, but not limited to law enforcement agencies and U.S. Immi-
2 gration and Customs Enforcement; and

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

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

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

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

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

14 § 5. 1. Private right of action.

15 (a) Any individual alleging a violation of this act or a regulation
16 promulgated under this act may bring a civil action in any court of
17 competent jurisdiction.

18 (b) A violation of this act or a regulation promulgated under this act
19 with respect to the personal information of an individual constitutes a
20 rebuttable presumption of harm to that individual.

21 (c) In a civil action in which the plaintiff prevails, the court may
22 award:

23 (i) liquidated damages of ten thousand dollars or actual damages,
24 whichever is greater;

25 (ii) punitive damages; and

26 (iii) any other relief, including an injunction, that the court deter-
27 mines is appropriate.

28 (d) In addition to any relief awarded pursuant to paragraph (c) of
29 this subdivision, the court shall award reasonable attorney's fees and
30 costs to any prevailing plaintiff.

31 2. The attorney general may bring an action in the name of the state,
32 or as parens patriae on behalf of persons residing in the state, to
33 enforce the provisions of this act. In an action brought by the attorney
34 general, the court may award injunctive relief, including preliminary
35 injunctions, to prevent further violations of and compel compliance with
36 this act; civil penalties up to twenty-five thousand dollars per
37 violation or up to four percent of annual revenue; other appropriate
38 relief, including restitution, to redress harms to individuals or to
39 mitigate all substantial risk of harm; and any other relief the court
40 determines.

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

50 § 7. This act shall take effect on the thirtieth day after it shall
51 have become a law and shall expire and be deemed repealed January 1,
52 2023.