

STATE OF NEW YORK

687

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. L. ROSENTHAL, DICKENS, BARRON, SIMON, EPSTEIN, SEAWRIGHT -- read once and referred to the Committee on Health

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

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

LBD00299-01-1

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

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

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

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

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

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

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

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

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

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

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

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

40 (iii) demographic data;

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

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

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

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

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

53 9. "Public health authority" means the New York state department of
54 health, a county health department or the New York city department of
55 health and mental hygiene, or a person or entity acting under a grant of
56 authority from or contract with such public agency, including the

1 employees or agents of such public agency or its contractors or persons
2 to entities to whom it has granted authority, that is responsible for
3 public health matters as part of its official mandate.

4 § 2. Individual rights.

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

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

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

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

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

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

19 (A) protecting against malicious, deceptive, fraudulent, or illegal
20 activity; or

21 (B) detecting, responding to, or preventing security incidents or
22 threats.

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

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

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

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

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

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

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

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

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

54 (iii) segregating, discriminating in, or otherwise making unavailable
55 the goods, services, facilities, privileges, advantages, or accommo-
56 dations of any place of public accommodation (as such term is defined in

1 section 301 of the Americans with Disabilities Act of 1990), except as
2 authorized by a state or federal government entity for a public health
3 purpose; provided that a covered entity shall not process emergency
4 health data or personal information to make categorical decisions about
5 the allocation of care based on disability.

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

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

13 (ii) describing the covered entity's data retention and data security
14 policies and practices for emergency health data and personal informa-
15 tion; and

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

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

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

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

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

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

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

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

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

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

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

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

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

49 (d) No covered entity in possession of emergency health data or
50 personal information may disclose, redisclose, or otherwise disseminate
51 an individual's emergency health data or personal information unless the
52 subject of the emergency health data or personal information or the
53 subject's legally authorized representative consents in writing to the
54 disclosure or redisclosure.

55 (e) Without consent under subdivision one of this section, emergency
56 health data, personal information, and any evidence derived therefrom

1 shall not be subject to or provided in response to any legal process or
2 be admissible for any purpose in any judicial or administrative action
3 or proceeding.

4 (f) Individuals shall have the right to access the emergency health
5 data and personal information collected on them and correct any inaccuracies.
6

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

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

18 § 3. 1. A covered entity shall implement reasonable measures to ensure
19 confidentiality, integrity, and availability of emergency health data
20 and personal information.

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

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

33 § 4. 1. All covered entities shall be subject to annual data
34 protection audits, conducted by a neutral third party auditor, evaluating
35 the technology utilized and the development processes for statistical
36 impacts on classes protected under section 296 of article 15 of
37 the executive law, as well as for impacts on privacy and security, that
38 includes at a minimum:

39 (a) a detailed description of the technology, its design, and its
40 purpose;

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

47 (c) an assessment of the risk of harm posed by the technology; the
48 risk that the technology may result in or contribute to inaccurate,
49 unfair, biased, or discriminatory decisions; the risk that the technology
50 may dissuade New Yorkers from participating in contact tracing or
51 obtaining medical testing or treatment; and the risk that personal
52 information or emergency health data can be accessed by third parties,
53 including, but not limited to law enforcement agencies and U.S. Immigration
54 and Customs Enforcement; and

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

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

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

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

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

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

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

31 § 7. This act shall take effect on the thirtieth day after it shall
32 have become a law and shall expire and be deemed repealed January 1,
33 2024.