



## 103RD GENERAL ASSEMBLY

### State of Illinois

2023 and 2024

SB3080

Introduced 2/2/2024, by Sen. Celina Villanueva

#### SYNOPSIS AS INTRODUCED:

New Act  
815 ILCS 505/2EEEE new

Creates the Protect Health Data Privacy Act. Provides that a regulated entity shall disclose and maintain a health data privacy policy that clearly and conspicuously discloses specified information. Sets forth provisions concerning health data privacy policies. Provides that a regulated entity shall not collect, share, or store health data, except in specified circumstances. Provides that it is unlawful for any person to sell or offer to sell health data concerning a consumer without first obtaining valid authorization from the consumer. Provides that a valid authorization to sell consumer health data must contain specified information; a copy of the signed valid authorization must be provided to the consumer; and the seller and purchaser of health data must retain a copy of all valid authorizations for sale of health data for 6 years after the date of its signature or the date when it was last in effect, whichever is later. Sets forth provisions concerning the consent required for collection, sharing, and storage of health data. Provides that a consumer has the right to withdraw consent from the collection, sharing, sale, or storage of the consumer's health data. Provides that it is unlawful for a regulated entity to engage in discriminatory practices against consumers solely because they have not provided consent to the collection, sharing, sale, or storage of their health data or have exercised any other rights provided by the provisions or guaranteed by law. Sets forth provisions concerning a consumer's right to confirm whether a regulated entity is collecting, selling, sharing, or storing any of the consumer's health data; a consumer's right to have the consumer's health data that is collected by a regulated entity deleted; prohibitions regarding geofencing; and consumer health data security. Provides that any person aggrieved by a violation of the provisions shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. Provides that the Attorney General may enforce a violation of the provisions as an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Defines terms. Makes a conforming change in the Consumer Fraud and Deceptive Business Practices Act.

LRB103 38349 SPS 68484 b

A BILL FOR

1 AN ACT concerning regulation.

2 **Be it enacted by the People of the State of Illinois,**  
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the  
5 Protect Health Data Privacy Act.

6 Section 5. Definitions. As used in this Act:

7 "Collect" means to buy, rent, lease, access, retain,  
8 receive, or acquire health data in any manner.

9 "Consent" means a clear affirmative act by a consumer that  
10 unambiguously communicates the consumer's express, freely  
11 given, informed, opt-in, voluntary, specific, and unambiguous  
12 written agreement, including written consent provided by  
13 electronic means, to the collection, sale, sharing, or storage  
14 of health data. Consent may not be implied, and consent cannot  
15 be obtained by:

16 (1) acceptance of a general or broad terms of use  
17 agreement or a similar document that contains descriptions  
18 of personal data processing along with other, unrelated  
19 information;

20 (2) hovering over, muting, pausing, or closing a given  
21 piece of digital content; or

22 (3) agreement obtained through the use of deceptive  
23 designs.

1 "Consumer" means a person who is a resident of this State,  
2 however identified, including by any unique identifier. A  
3 person located in this State when the person's health data is  
4 collected by a regulated entity shall create a presumption  
5 that the person is a resident of this State for purposes of  
6 enforcing this Act. "Consumer" does not include an individual  
7 acting in a commercial or employment context.

8 "Deceptive design" means any user interface or element  
9 thereof that has the substantial effect of subverting,  
10 impairing, or impeding an individual's autonomy,  
11 decision-making, or choice.

12 "Deidentified data" means data that cannot be used to  
13 infer information about, or otherwise be linked to, an  
14 identified or identifiable individual, or a device linked to  
15 such individual. A regulated entity that possesses  
16 deidentified data shall: (i) take reasonable measures to  
17 ensure that such data cannot be associated with an individual;  
18 (ii) publicly commit to process such data only in a  
19 deidentified fashion and not attempt to reidentify such data;  
20 and (iii) contractually obligate any recipients of such data  
21 to satisfy the criteria set forth in items (i) and (ii).

22 "Geofence" means technology that uses global positioning  
23 coordinates, cell tower connectivity, cellular data, radio  
24 frequency identification, wireless Internet data, or any other  
25 form of spatial or location detection to establish a virtual  
26 boundary around a specific physical location or to locate a

1 consumer within a virtual boundary. For the purposes of this  
2 Act, "geofence" means a virtual boundary that is no more than  
3 1,750 feet around a specific physical location that provides  
4 health services.

5 "Health data" means information regarding, relating to,  
6 derived, or extrapolated from the past, present, or future  
7 physical or mental health of a consumer, including, but not  
8 limited to, any information relating to:

9 (1) individual health conditions, treatment, status,  
10 diseases, or diagnoses;

11 (2) health related surgeries or procedures;

12 (3) use or purchase of medication;

13 (4) social, psychological, behavioral, and medical  
14 interventions;

15 (5) bodily functions, vital signs, measurements, or  
16 symptoms;

17 (6) diagnoses or diagnostic testing, treatment, or  
18 medication;

19 (7) efforts to research or obtain health services or  
20 supplies;

21 (8) health services or products that support or relate  
22 to lawful health care, as defined by Public Act 102-1117;

23 (9) precise location information that could reasonably  
24 be used to determine a consumer's attempt to acquire or  
25 receive health services or supplies; and

26 (10) any information described in paragraphs (1)

1 through (9) that is derived or extrapolated from  
2 non-health information, including by use of algorithms or  
3 machine learning, if such information is used or processed  
4 in connection with the advertising, marketing, or  
5 provision of health services.

6 "Health data" does not include:

7 (1) personal information collected with the consumer's  
8 consent that is used to engage in public or peer-reviewed  
9 scientific, historical, or statistical research in the  
10 public interest that adheres to all other applicable  
11 ethics and privacy laws and is approved, monitored, and  
12 governed by an institutional review board, human subjects  
13 research ethics review board, or a similar independent  
14 oversight entity that determines that the regulated entity  
15 has implemented reasonable safeguards to mitigate privacy  
16 risks associated with research, including any risks  
17 associated with reidentification; or

18 (2) deidentified data.

19 "Health services" means any service, medical care, or  
20 information related to a consumer's health data provided to a  
21 consumer.

22 "HIPAA" means the Health Insurance Portability and  
23 Accountability Act of 1996, Public Law 104-191, the Health  
24 Information Technology for Economic and Clinical Health Act,  
25 and any subsequent amendments thereto and any regulations  
26 promulgated thereunder, including the Privacy Rule, as

1 specified in 45 CFR 164.500-534, the Security Rule, as  
2 specified in 45 CFR 164.302-318, and the Breach Notification  
3 rule, as specified in 45 CFR 164.400-414.

4 "Homepage" means the introductory page of a website where  
5 personal information is collected. In the case of an online  
6 service, such as a mobile application, "homepage" means the  
7 application's platform page or download page, such as from the  
8 application configuration, "About" page, "Information" page,  
9 or settings page, and any other location that allows consumers  
10 to review the notice.

11 "Personal information" means information that identifies,  
12 relates to, describes, is reasonably capable of being  
13 associated with, or linked, directly or indirectly, with a  
14 particular consumer or household. "Personal information" does  
15 not include publicly available information or deidentified  
16 data.

17 "Precise location information" means information that  
18 identifies the location of an individual within a radius of  
19 1,750 feet. "Precise location information" does not include:  
20 (i) the content of communications, or (ii) any data generated  
21 by or connected to advanced utility metering infrastructure  
22 systems or equipment for use by a utility.

23 "Processor" means an individual or legal entity that  
24 processes health data on behalf of a regulated entity pursuant  
25 to a written agreement or contract. "Process" or "processing"  
26 means arranging, storing, organizing, structuring, retrieving,

1 transmission, or the otherwise making available of data.

2 "Publicly available" means information that is lawfully  
3 made available from federal, State, or local government  
4 records.

5 "Regulated entity" means any individual, partnership,  
6 corporation, limited liability company, association, or other  
7 group, however organized, that: (i) conducts business in this  
8 State or produces products or services that are available to  
9 consumers in this State; and (ii) for any purpose, handles,  
10 collects, shares, sells, stores or otherwise deals with health  
11 data. "Regulated entity" does not include government agencies,  
12 tribal nations, a clerk of the court, or a judge or justice  
13 thereof, or contracted service providers when processing  
14 consumer health data on behalf of the government agency.  
15 "Regulated entity" does not include any entity that is a  
16 covered entity or a business associate, as defined in Section  
17 160.103 of Title 45 of the Code of Federal Regulations,  
18 subject to and in compliance with HIPAA to the extent such  
19 entity is acting as a covered entity or business associate  
20 under the Privacy and Security rules issued by the United  
21 States Department of Health and Human Services, Parts 160 and  
22 164 of Title 45 of the Code of Federal Regulations. "Regulated  
23 entity" does not include any entity that is subject to and in  
24 compliance with restrictions on disclosure of records under  
25 Section 543 of the Public Health Service Act, 42 U.S.C.  
26 290dd-2, to the extent such entity is acting in a capacity

1 subject to such restrictions.

2 "Sell" or "sale" means when a regulated entity, directly  
3 or indirectly, receives any form of remuneration or other  
4 valuable consideration from the use of health data or from the  
5 recipient of the health data in exchange for the health data.

6 "Sell" does not include:

7 (1) the sharing of health data to a recipient where  
8 the regulated entity maintains control and ownership of  
9 the health data;

10 (2) the sharing of health data to comply with  
11 applicable laws or regulations;

12 (3) the use of the health data by an entity  
13 exclusively at the direction of the regulated entity and  
14 consistent with the purpose for which it was collected and  
15 disclosed; and

16 (4) the transfer of health data to a third party as an  
17 asset as part of a merger, acquisition, bankruptcy, or  
18 other transaction in which the third party assumes control  
19 of all or part of the regulated entity's assets that shall  
20 comply with the requirements and obligations in this Act.

21 "Share" means to release, disclose, disseminate, divulge,  
22 loan, make available, provide access to, license, or otherwise  
23 communicate orally, in writing, or by electronic or other  
24 means, health data by a regulated entity to a third party  
25 except where the regulated entity maintains exclusive control  
26 and ownership of the health data. "Share" does not include:



1           (1) the disclosure of health data to a processor that  
2           collects or processes the personal data on behalf of the  
3           regulated entity, when the regulated entity maintains  
4           control and ownership of the data and the processor  
5           maintains or uses the health data only for the regulated  
6           entity's distinct purposes pursuant to a contract;

7           (2) the disclosure of health data to a third party  
8           with whom the consumer has a direct relationship for  
9           purposes of and only to the extent necessary for providing  
10          a product or service requested by the consumer when the  
11          regulated entity maintains control and ownership of the  
12          data and the third party maintains or uses the health data  
13          only for the regulated entity's distinct purposes; or

14          (3) the disclosure or transfer of personal data to a  
15          third party as an asset that is part of a merger,  
16          acquisition, bankruptcy, or other transaction in which the  
17          third party assumes control of all or part of the  
18          regulated entity's assets and shall comply with the  
19          requirements and obligations in this Act.

20          "Strictly necessary" means essential or required to be  
21          done.

22          "Third party" means an entity other than a consumer,  
23          regulated entity, service provider, or affiliate of the  
24          regulated entity.

25          Section 10. Scope.

1 (a) This Act applies to consumers seeking, researching, or  
2 obtaining health services within this State, or information  
3 about health services available in this State and regulated  
4 entities.

5 (b) This Act does not affect an individual's right to  
6 voluntarily share the individual's own health care information  
7 with another person or entity.

8 Section 15. Health data privacy policy required.

9 (a) A regulated entity shall disclose and maintain a  
10 health data privacy policy that, in plain language, clearly  
11 and conspicuously discloses:

12 (1) the specific types of health data collected and  
13 the purpose for which the data is collected and used;

14 (2) the categories of sources from which the health  
15 data is collected;

16 (3) the specific types of health data that are shared,  
17 sold, and stored;

18 (4) the categories of third parties with whom the  
19 regulated entity collects, shares, sells, and stores  
20 health data, and the process to withdraw consent from  
21 having health data collected, shared, sold, and stored;

22 (5) a list of the specific third parties to which the  
23 regulated entity shares health data, and an active  
24 electronic mail address or other online mechanism that the  
25 consumer may use to contact these third parties free of

1 charge;

2 (6) how a consumer may exercise the rights provided in  
3 this Act, including, but not limited to, identifying 2 or  
4 more designated methods for a consumer to contact the  
5 regulated entity in connection with the exercise of any  
6 rights provided in this Act;

7 (7) the length of time the regulated entity intends to  
8 retain each category of health data, or if that is not  
9 possible, the criteria used to determine that period;  
10 however, a regulated entity shall not retain health data  
11 for each disclosed purpose for which the health data was  
12 collected for longer than is reasonably necessary to  
13 fulfill that disclosed purpose; and

14 (8) whether the regulated entity collects health data  
15 when the consumer is not directly interacting with the  
16 regulated entity or its services.

17 (b) A regulated entity shall prominently publish or link  
18 to its health data privacy policy on its website homepage, or  
19 in another manner that is clear and conspicuous to consumers.  
20 Its health data privacy policy must be distinguishable from  
21 other matters. Any regulated entity providing health services  
22 in a physical location shall also post its health data privacy  
23 policy in a conspicuous place that is readily available for  
24 viewing by consumers.

25 (c) A regulated entity shall not collect, share, sell, or  
26 store additional categories of health data not disclosed in

1 the health data privacy policy without first disclosing the  
2 additional categories of health data and obtaining the  
3 consumer's consent before the collection, sharing, selling, or  
4 storing of the health data.

5 (d) A regulated entity shall not collect, share, sell, or  
6 store health data for additional purposes not disclosed in the  
7 health data privacy policy without first disclosing the  
8 additional purposes and obtaining the consumer's consent  
9 before the collection, sharing, selling, or storing of the  
10 health data.

11 (e) It is a violation of this Act for a regulated entity to  
12 contract with a processor to process consumer health data in a  
13 manner that is inconsistent with the regulated entity's  
14 consumer health data privacy policy.

15 Section 20. Prohibition on collection, sharing, or storing  
16 of health data. A regulated entity shall not collect, share,  
17 or store health data, except:

18 (1) with the consent of the consumer to whom the  
19 information relates for a specified purpose; or

20 (2) as is strictly necessary to provide a product or  
21 service that the consumer to whom the health data relates  
22 has specifically requested from the regulated entity.

23 Section 25. Prohibition on sale of health data.

24 (a) It is unlawful for any person to sell or offer to sell

1 health data concerning a consumer without first obtaining  
2 valid authorization from the consumer. The sale of consumer  
3 health data must be consistent with the valid authorization  
4 signed by the consumer.

5 (b) A valid authorization to sell consumer health data is  
6 an agreement consistent with this Section and must be written  
7 in plain language. The valid authorization to sell consumer  
8 health data must contain the following:

9 (1) the specific consumer health data concerning the  
10 consumer that the person intends to sell;

11 (2) the name and contact information of any person or  
12 entity collecting and selling the health data;

13 (3) the name and contact information of any person or  
14 entity purchasing the health data from the seller  
15 identified in paragraph (2) of this subsection;

16 (4) a description of the purpose for the sale,  
17 including how the health data will be gathered and how it  
18 will be used by the purchaser identified in paragraph (3)  
19 of this subsection when sold;

20 (5) a statement that the provision of goods or  
21 services may not be conditioned on the consumer signing  
22 the valid authorization;

23 (6) a statement that the consumer has a right to  
24 revoke the valid authorization at any time and a  
25 description on how a consumer may revoke the valid  
26 authorization;

1           (7) a statement that the consumer health data sold  
2 pursuant to the valid authorization may be subject to  
3 redisclosure by the purchaser and may no longer be  
4 protected by this Section;

5           (8) an expiration date for the valid authorization  
6 that expires one year from when the consumer signs the  
7 valid authorization; and

8           (9) the signature of the consumer and date.

9           (c) An authorization is not valid if the document has any  
10 of the following defects:

11           (1) the expiration date has passed;

12           (2) the authorization does not contain all the  
13 information required under this Section;

14           (3) the authorization has been revoked by the  
15 consumer;

16           (4) the authorization has been combined with other  
17 documents to create a compound authorization; or

18           (5) the provision of goods or services is conditioned  
19 on the consumer signing the authorization.

20           (d) A copy of the signed valid authorization must be  
21 provided to the consumer.

22           (e) The seller and purchaser of health data must retain a  
23 copy of all valid authorizations for sale of health data for 6  
24 years after the date of its signature or the date when it was  
25 last in effect, whichever is later.

1 Section 30. Consent required for collection, sharing, and  
2 storage of health data.

3 (a) A regulated entity shall not seek consent to collect,  
4 share, or store health data without first disclosing its  
5 health data privacy policy as required under Section 15.

6 (b) Consent required under this Section must be obtained  
7 before the collection, sharing, or storing, as applicable, of  
8 any health data, and the request for consent must clearly and  
9 conspicuously disclose, separate and apart from its health  
10 data privacy policy:

11 (1) the categories of health data collected, sold,  
12 shared, or stored;

13 (2) the purpose of the collection, sharing, or storage  
14 of the health data, including the specific ways in which  
15 it will be used; and

16 (3) how the consumer can withdraw consent from future  
17 collection, sharing, or storage of their health data.

18 (c) Consent required under this Section must be obtained  
19 before the use of any health data for any additional purpose  
20 that was not specified before obtaining a consumer's consent  
21 for the use of the health data.

22 Section 35. Right to withdraw consent. A consumer has the  
23 right to withdraw consent from the collection, sharing, sale,  
24 or storage of the consumer's health data, consistent with the  
25 requirements of Section 30.

1 Section 40. Prohibition on discriminatory practices.

2 (a) It is unlawful for a regulated entity to engage in  
3 discriminatory practices against a consumer solely because the  
4 consumer has not provided consent to the collection, sharing,  
5 sale, or storage of the consumer's health data pursuant to  
6 this Act, or have exercised any other rights provided by this  
7 Act or guaranteed by law. Discriminatory practices include,  
8 but are not limited to:

9 (1) denying or limiting goods or services to the  
10 consumer;

11 (2) imposing additional requirements or restrictions  
12 on the individual that would not be necessary if the  
13 consumer provided their consent;

14 (3) providing materially different treatment to  
15 consumers who provide consent as compared to consumers who  
16 do not provide consent;

17 (4) providing or suggesting that the consumer will  
18 receive a lower level or quality of goods or services;

19 (5) suggesting that the consumer will receive a  
20 different price or rate for goods or services; or

21 (6) charging different prices or rates for goods or  
22 services, including using discounts or other benefits or  
23 imposing penalties.

24 (b) It shall not be a discriminatory practice under this  
25 Section to use health data as is strictly necessary to provide



1 a product or service that the consumer to whom the health data  
2 relates has specifically requested from a regulated entity.

3 Section 45. Right to confirm. A consumer has the right to  
4 confirm whether a regulated entity is collecting, selling,  
5 sharing, or storing any of the consumer's health data, and to  
6 confirm that a regulated entity has deleted the consumer's  
7 health data following a deletion request pursuant to Section  
8 50. A regulated entity that receives a consumer request to  
9 confirm shall respond within 45 calendar days after receiving  
10 the request to confirm from the consumer. The regulated entity  
11 shall, without reasonable delay, promptly take all steps  
12 necessary to verify the consumer's request, but this shall not  
13 extend the regulated entity's duty to respond within 45 days  
14 of receipt of the consumer's request. The time period to  
15 provide the required confirmation may be extended once by an  
16 additional 45 calendar days when reasonably necessary, if the  
17 consumer is provided notice of the extension within the first  
18 45-day period.

19 Section 50. Right to deletion.

20 (a) A consumer has the right to have the consumer's health  
21 data that is collected by a regulated entity deleted by  
22 informing the regulated entity of the consumer's request for  
23 deletion, except as provided in subsection (g).

24 (b) Except as otherwise specified in subsection (f), a

1 regulated entity that receives a consumer request to delete  
2 any of the consumer's health data shall without unreasonable  
3 delay, and no more than 45 calendar days from receiving the  
4 deletion request:

5 (1) delete the consumer's health data from its  
6 records, including from all parts of the regulated  
7 entity's network; and

8 (2) notify all service providers, contractors, and  
9 third parties with whom the regulated entity has shared  
10 the consumer's health data of the deletion request.

11 (c) If a regulated entity stores any health data on  
12 archived or backup systems, it may delay compliance with the  
13 consumer's request to delete with respect to the health data  
14 stored on the archived or backup system until the archived or  
15 backup system relating to that data is restored to an active  
16 system or is next accessed or used.

17 (d) Any processor, service provider, contractor, and other  
18 third party that receives notice of a consumer's deletion  
19 request from a regulated entity shall honor the consumer's  
20 deletion request and delete the health data from the regulated  
21 entity's records, including from all parts of its network or  
22 backup systems.

23 (e) A consumer or a consumer's authorized agent may  
24 exercise the rights set forth in this Act by submitting a  
25 request, at any time, to a regulated entity. Such a request may  
26 be made by:

1 (1) contacting the regulated entity through the manner  
2 included in its health data privacy policy;

3 (2) by designating an authorized agent who may  
4 exercise the rights on behalf of the consumer;

5 (3) in the case of collecting health data of a minor,  
6 the minor seeking health services may exercise their  
7 rights under this Act, or the parent or legal guardian of  
8 the minor may exercise the rights of this Act on the  
9 minor's behalf; or

10 (4) in the case of collecting health data concerning a  
11 consumer subject to guardianship, conservatorship, or  
12 other protective arrangement under the Probate Act of  
13 1975, the guardian or the conservator of the consumer may  
14 exercise the rights of this Act on the consumer's behalf.

15 (f) The time period to delete any of the consumer's health  
16 data may be extended once by an additional 30 calendar days  
17 when reasonably necessary, if the consumer is provided notice  
18 of the extension within the first 30-day period.

19 (g) Neither a regulated entity nor a processor shall be  
20 required to comply with a consumer's request to delete the  
21 consumer's health data if it is necessary for the regulated  
22 entity or the processor to maintain the consumer's health data  
23 to:

24 (1) complete the transaction for which the health data  
25 was collected, provide a good or service requested by the  
26 consumer, or otherwise fulfill the requirements of an

1 agreement between the regulated entity and the consumer;

2 (2) detect security incidents, protect against  
3 malicious, deceptive, fraudulent, or illegal activity, if  
4 the use of health data for such purposes is limited in time  
5 pursuant to a valid record retention schedule;

6 (3) engage in public or peer-reviewed scientific,  
7 historical, or statistical research in the public interest  
8 that adheres to all other applicable ethics and privacy  
9 laws, if the entities' deletion of the information is  
10 likely to render impossible or seriously impair the  
11 achievement of such research, and if the consumer has  
12 provided consent to such use of their health data;

13 (4) comply with an applicable legal obligation, such  
14 as data retention requirements set forth in Section 6 of  
15 the Hospital Licensing Act, 45 CFR 164.316, and 45 CFR  
16 164.530;

17 (5) comply with an applicable legal obligation if the  
18 regulated entity has been notified, in writing by an  
19 attorney, that there is litigation pending in court  
20 involving the consumer's health data as possible evidence  
21 and that the consumer is their client or is the person who  
22 has instituted the litigation against their client, then  
23 the regulated entity shall retain the record of that  
24 consumer until notified in writing by the plaintiff's  
25 attorney, with the approval of the defendant's attorney of  
26 record, that the case in court involving the record has

1           been concluded or for a period of 12 years after the date  
2           that the record was produced, whichever occurs first in  
3           time; or

4           (6) otherwise use the consumer's health data,  
5           internally, in a lawful manner that is compatible with the  
6           context in which the consumer provided their health data.

7           Section 55. Authentication of consumer identity.

8           (a) A regulated entity that receives a consumer request to  
9           confirm or delete may take reasonable measures to authenticate  
10          the consumer's identity to a reasonably high degree of  
11          certainty. A reasonably high degree of certainty may include  
12          matching at least 3 pieces of personal information provided by  
13          the consumer with personal information maintained by the  
14          regulated entity that it has determined to be reliable for the  
15          purpose of authenticating the consumer together with a signed  
16          declaration under penalty of perjury that the consumer making  
17          the request is the consumer whose health data is the subject of  
18          the request. If a regulated entity uses this method for  
19          authentication, the regulated entity shall make all forms  
20          necessary for authentication of a consumer's identity  
21          available to consumers, and shall maintain all signed  
22          declarations as part of its recordkeeping obligations.

23          (b) A regulated entity is not required to comply with a  
24          consumer request to confirm or delete if the regulated entity,  
25          using commercially reasonable efforts, is unable to

1 authenticate the identity of the consumer making the request.  
2 If a regulated entity is unable to authenticate the consumer's  
3 identity, the regulated entity shall inform the consumer that  
4 it was unable to authenticate the consumer's identity and  
5 advise the consumer of other methods, if available, of  
6 authenticating their identity.

7 (c) If a regulated entity denies an authenticated consumer  
8 request to delete that consumer's health data, in whole or in  
9 part, because of a conflict with federal or State law, the  
10 regulated entity shall inform the requesting consumer and  
11 explain the basis for the denial, unless prohibited from doing  
12 so by law.

13 (d) Any information provided by a consumer to a regulated  
14 entity for the purpose of authenticating the consumer's  
15 identity shall not be used for any purpose other than  
16 authenticating the consumer's identity and shall be destroyed  
17 immediately following the authentication process.

18 Section 60. Consumer health data security and  
19 minimization.

20 (a) A regulated entity shall restrict access to health  
21 data by the employees, processors, service providers, and  
22 contractors of the regulated entity to only those employees,  
23 processors, services providers, and contractors for which  
24 access is necessary to provide a product or service that the  
25 consumer to whom the health data relates has requested from

1 the regulated entity.

2 (b) A regulated entity shall establish, implement, and  
3 maintain administrative, technical, and physical data security  
4 practices that at least satisfy a reasonable standard of care  
5 within the regulated entity's industry to protect the  
6 confidentiality, integrity, and accessibility of health data  
7 appropriate to the volume and nature of the personal data at  
8 issue.

9 Section 65. Prohibition on geofencing.

10 (a) It shall be unlawful for any person to implement a  
11 geofence that enables the sending of a notification, message,  
12 alert, or other piece of information to a consumer that enters  
13 the perimeter around any entity that provides health services.

14 (b) It shall be unlawful for any person to implement a  
15 geofence around any entity that provides in-person health care  
16 services where the geofence is used to identify, track, or  
17 collect data from a consumer that enters the virtual  
18 perimeter.

19 Section 70. Private right of action. Any person aggrieved  
20 by a violation of this Act shall have a right of action in a  
21 State circuit court or as a supplemental claim in federal  
22 district court against an offending party. A prevailing party  
23 may recover for each violation:

24 (1) against any offending party that negligently

1 violates a provision of this Act, liquidated damages of  
2 \$1,000 or actual damages, whichever is greater;

3 (2) against any offending party that intentionally or  
4 recklessly violates a provision of this Act, liquidated  
5 damages of \$5,000 or actual damages, whichever is greater;

6 (3) reasonable attorney's fees and costs, including  
7 expert witness fees and other litigation expenses; and

8 (4) other relief, including an injunction, as the  
9 State or federal court may deem appropriate.

10 Section 75. Enforcement by the Attorney General. The  
11 Attorney General may enforce a violation of this Act as an  
12 unlawful practice under the Consumer Fraud and Deceptive  
13 Business Practices Act. All rights and remedies provided the  
14 Attorney General under the Consumer Fraud and Deceptive  
15 Business Practices Act shall be available for enforcement of a  
16 violation of this Act.

17 Section 80. Conflict with other laws.

18 (a) Nothing in this Act shall be construed to prohibit the  
19 lawful and authorized disclosure of health data by regulated  
20 entities to local health departments or State government  
21 agencies or by or among local health departments and State  
22 government agencies as may be required by State and federal  
23 law, including under the Adult Protective Services Act, the  
24 Abused and Neglected Child Reporting Act, the Criminal Code of



1 2012, and the Disclosure of Offenses Against Children Act.

2 (b) If any provision of this Act, or the application  
3 thereof to any person or circumstance, is held invalid, the  
4 remainder of this Act and the application of such provision to  
5 other persons not similarly situated or to other circumstances  
6 shall not be affected by the invalidation.

7 (c) This Act shall not apply to personal information  
8 collected, processed, sold, or disclosed subject to the  
9 federal Gramm-Leach-Bliley Act, Public Law 106-102, and  
10 implementing regulations.

11 Section 900. The Consumer Fraud and Deceptive Business  
12 Practices Act is amended by adding Section 2EEEE as follows:

13 (815 ILCS 505/2EEEE new)

14 Sec. 2EEEE. Violations of the Protect Health Data Privacy  
15 Act. Any person who violates the Protect Health Data Privacy  
16 Act commits an unlawful practice within the meaning of this  
17 Act.