



## 102ND GENERAL ASSEMBLY

### State of Illinois

2021 and 2022

HB4653

Introduced 1/21/2022, by Rep. Thaddeus Jones

#### SYNOPSIS AS INTRODUCED:

New Act  
5 ILCS 140/7.5

Creates the Insurance Data Security Law. Sets forth provisions concerning an information security program, investigations of cybersecurity events, and notifications of cybersecurity events. Provides that the Director of Insurance shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of the Act. Provides that whenever the Director has reason to believe that a licensee has been or is engaged in conduct in the State which violates the Act, the Director may take action that is necessary or appropriate to enforce the provisions of the Act. Provides that any documents, materials, or other information in the control or possession of the Department of Insurance that are furnished by a licensee or an employee or agent acting on behalf of a licensee or that are obtained by the Director in an investigation or examination shall be confidential by law and privileged, shall not be subject to the Freedom of Information Act, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. Sets forth provisions concerning exceptions, penalties, and severability. Provides that the Department may adopt rules necessary to carry out the provisions of the Act. Defines terms. Makes a conforming change in the Freedom of Information Act. Effective January 1, 2023.

LRB102 21459 BMS 30576 b

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 Insurance Data Security Law.

6 Section 2. Purpose and intent.

7 (a) The purpose and intent of this Act is to establish  
8 standards for data security and standards for the  
9 investigation of and notification to the Director of a  
10 cybersecurity event applicable to licensees.

11 (b) This Act shall not be construed to create or imply a  
12 private cause of action for a violation of its provisions nor  
13 shall it be construed to curtail a private cause of action  
14 which would otherwise exist in the absence of this Act.

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

16 "Authorized individual" means an individual known to and  
17 screened by the licensee and determined to be necessary and  
18 appropriate to have access to the nonpublic information held  
19 by the licensee and its information systems.

20 "Consumer" means an individual, including, but not limited  
21 to, an applicant, policyholder, insured, beneficiary,  
22 claimant, or certificate holder who is a resident of this

1 State and whose nonpublic information is in a licensee's  
2 possession, custody, or control.

3 "Cybersecurity event" means an event resulting in  
4 unauthorized access to, disruption, or misuse of an  
5 information system or information stored on such information  
6 system. "Cybersecurity event" does not include the  
7 unauthorized acquisition of encrypted nonpublic information if  
8 the encryption, process, or key is not also acquired,  
9 released, or used without authorization. "Cybersecurity event"  
10 does not include an event with regard to which the licensee has  
11 determined that the nonpublic information accessed by an  
12 unauthorized person has not been used or released and has been  
13 returned or destroyed.

14 "Department" means the Department of Insurance.

15 "Director" means the Director of Insurance.

16 "Encrypted" means the transformation of data into a form  
17 which results in a low probability of assigning meaning  
18 without the use of a protective process or key.

19 "Information security program" means the administrative,  
20 technical, and physical safeguards that a licensee uses to  
21 access, collect, distribute, process, protect, store, use,  
22 transmit, dispose of, or otherwise handle nonpublic  
23 information.

24 "Information system" means a discrete set of electronic  
25 information resources organized for the collection,  
26 processing, maintenance, use, sharing, dissemination, or

1 disposition of electronic information, as well as any  
2 specialized system such as industrial and process controls  
3 systems, telephone switching and private branch exchange  
4 systems, and environmental control systems.

5 "Licensee" means any person licensed, authorized to  
6 operate, or registered, or required to be licensed,  
7 authorized, or registered pursuant to the insurance laws of  
8 this State. "Licensee" does not include a purchasing group or  
9 a risk retention group chartered and licensed in a state other  
10 than this State or a licensee that is acting as an assuming  
11 insurer that is domiciled in another state or jurisdiction.

12 "Multi-factor authentication" means authentication  
13 through verification of at least 2 of the following types of  
14 authentication factors:

- 15 (1) knowledge factors, including a password;  
16 (2) possession factors, including a token or text  
17 message on a mobile phone; or  
18 (3) inherence factors, including a biometric  
19 characteristic.

20 "Nonpublic information" means information that is not  
21 publicly available information and that is:

- 22 (1) business-related information of a licensee the  
23 tampering with which, or unauthorized disclosure, access,  
24 or use of which, would cause a material adverse impact to  
25 the business, operations, or security of the licensee;  
26 (2) any information concerning a consumer which

1 because of name, number, personal mark, or other  
2 identifier can be used to identify such consumer, in  
3 combination with any one or more of the following data  
4 elements:

5 (A) social security number;

6 (B) driver's license number or nondriver  
7 identification card number;

8 (C) account number, credit card number, or debit  
9 card number;

10 (D) any security code, access code, or password  
11 that would permit access to a consumer's financial  
12 account; or

13 (E) biometric records; or

14 (3) any information or data, except age or gender, in  
15 any form or medium created by or derived from a health care  
16 provider or a consumer and that relates to:

17 (A) the past, present, or future physical, mental,  
18 or behavioral health or condition of any consumer or a  
19 member of the consumer's family;

20 (B) the provision of health care to any consumer;  
21 or

22 (C) payment for the provision of health care to  
23 any consumer.

24 "Person" means any individual or any nongovernmental  
25 entity, including, but not limited to, any nongovernmental  
26 partnership, corporation, branch, agency, or association.

1 "Publicly available information" means any information  
2 that a licensee has a reasonable basis to believe is lawfully  
3 made available to the general public from federal, State, or  
4 local government records; widely distributed media; or  
5 disclosures to the general public that are required to be made  
6 by federal, State, or local law. "Publicly available  
7 information" includes information that a consumer may direct  
8 not to be made available to the general public, but that the  
9 consumer has not directed not be made available.

10 "Risk assessment" means the risk assessment that each  
11 licensee is required to conduct under subsection (c) of  
12 Section 10.

13 "Third-party service provider" means a person, not  
14 otherwise defined as a licensee, that contracts with a  
15 licensee to maintain, process, store, or otherwise is  
16 permitted access to nonpublic information through its  
17 provision of services to the licensee.

18 Section 10. Information security program.

19 (a) Commensurate with the size and complexity of the  
20 licensee, the nature and scope of the licensee's activities,  
21 including its use of third-party service providers, and the  
22 sensitivity of the nonpublic information used by the licensee  
23 or in the licensee's possession, custody, or control, each  
24 licensee shall develop, implement, and maintain a  
25 comprehensive written information security program based on

1 the licensee's risk assessment and that contains  
2 administrative, technical, and physical safeguards for the  
3 protection of nonpublic information and the licensee's  
4 information system.

5 (b) A licensee's information security program shall be  
6 designed to:

7 (1) protect the security and confidentiality of  
8 nonpublic information and the security of the information  
9 system;

10 (2) protect against any threats or hazards to the  
11 security or integrity of nonpublic information and the  
12 information system;

13 (3) protect against unauthorized access to or use of  
14 nonpublic information;

15 (4) minimize the likelihood of harm to any consumer;  
16 and

17 (5) define and periodically reevaluate a schedule for  
18 retention of nonpublic information and a mechanism for its  
19 destruction when no longer needed.

20 (c) A licensee shall:

21 (1) designate one or more employees, an affiliate, or  
22 an outside vendor designated to act on behalf of the  
23 licensee who is responsible for the information security  
24 program;

25 (2) identify reasonably foreseeable internal or  
26 external threats that could result in unauthorized access,

1 transmission, disclosure, misuse, alteration, or  
2 destruction of nonpublic information, including the  
3 security of information systems and nonpublic information  
4 that are accessible to or held by third-party service  
5 providers;

6 (3) assess the likelihood and potential damage of  
7 these threats, taking into consideration the sensitivity  
8 of the nonpublic information;

9 (4) assess the sufficiency of policies, procedures,  
10 information systems, and other safeguards in place to  
11 manage these threats, including consideration of threats  
12 in each relevant area of the licensee's operations,  
13 including:

14 (A) employee training and management;

15 (B) information systems, including network and  
16 software design, as well as information  
17 classification, governance, processing, storage,  
18 transmission, and disposal; and

19 (C) detecting, preventing, and responding to  
20 attacks, intrusions, or other systems failures; and

21 (5) implement information safeguards to manage the  
22 threats identified in its ongoing assessment, and, no less  
23 than annually, assess the effectiveness of the safeguards'  
24 key controls, systems, and procedures.

25 (d) Based on its risk assessment, the licensee shall:

26 (1) design its information security program to



1 mitigate the identified risks, commensurate with the size  
2 and complexity of the licensee's activities, including its  
3 use of third-party service providers, and the sensitivity  
4 of the nonpublic information used by the licensee or in  
5 the licensee's possession, custody, or control;

6 (2) select and implement appropriate security measures  
7 from the following:

8 (A) place access controls on information systems,  
9 including controls to authenticate and permit access  
10 only to authorized individuals to protect against the  
11 unauthorized acquisition of nonpublic information;

12 (B) identify and manage the data, personnel,  
13 devices, systems, and facilities that enable the  
14 organization to achieve business purposes in  
15 accordance with their relative importance to business  
16 objectives and the organization's risk strategy;

17 (C) restrict access at physical locations  
18 containing nonpublic information only to authorized  
19 individuals;

20 (D) protect, by encryption or other appropriate  
21 means, all nonpublic information while being  
22 transmitted over an external network and all nonpublic  
23 information stored on a laptop computer or other  
24 portable computing or storage device or media;

25 (E) adopt secure development practices for  
26 in-house-developed applications utilized by the

1 licensee and procedures for evaluating, assessing, or  
2 testing the security of externally developed  
3 applications utilized by the licensee;

4 (F) modify the information system in accordance  
5 with the licensee's information security program;

6 (G) utilize effective controls, including  
7 multifactor authentication procedures for any  
8 individual accessing nonpublic information;

9 (H) regularly test and monitor systems and  
10 procedures to detect actual and attempted attacks on  
11 or intrusions into information systems;

12 (I) include audit trails within the information  
13 security program designed to detect and respond to  
14 cybersecurity events and designed to reconstruct  
15 material financial transactions sufficient to support  
16 normal operations and obligations of the licensee;

17 (J) implement measures to protect against  
18 destruction, loss, or damage of nonpublic information  
19 due to environmental hazards, including fire and water  
20 damage, other catastrophes, or technological failures;  
21 and

22 (K) develop, implement, and maintain procedures  
23 for the secure disposal of nonpublic information in  
24 any format;

25 (3) include cybersecurity risks in the licensee's  
26 enterprise risk management process;

1           (4) stay informed regarding emerging threats or  
2 vulnerabilities and utilize reasonable security measures  
3 when sharing information relative to the character of the  
4 sharing and the type of information shared; and

5           (5) provide its personnel with cybersecurity awareness  
6 training that is updated as necessary to reflect risks  
7 identified by the licensee in the risk assessment.

8           (e) If the licensee has a board of directors, the board or  
9 an appropriate committee of the board shall, at a minimum:

10           (1) require the licensee's executive management or its  
11 delegates to develop, implement, and maintain the  
12 licensee's information security program;

13           (2) require the licensee's executive management or its  
14 delegates to report in writing, at least annually, the  
15 following information:

16           (A) the overall status of the information security  
17 program and the licensee's compliance with this Act;  
18 and

19           (B) material matters related to the information  
20 security program, addressing issues such as risk  
21 assessment, risk management and control decisions,  
22 third-party service provider arrangements, results of  
23 testing, cybersecurity events or violations and  
24 management's responses thereto, and recommendations  
25 for changes in the information security program; and

26           (3) if executive management delegates any of its

1           responsibilities under this Section, it shall oversee the  
2           development, implementation, and maintenance of the  
3           licensee's information security program prepared by the  
4           delegate and shall receive a report from the delegate  
5           complying with the requirements of the report to the board  
6           of directors.

7           (f) A licensee shall exercise due diligence in selecting  
8           its third-party service provider and a licensee shall require  
9           a third-party service provider to implement appropriate  
10          administrative, technical, and physical measures to protect  
11          and secure the information systems and nonpublic information  
12          that are accessible to or held by the third-party service  
13          provider.

14          (g) The licensee shall monitor, evaluate, and adjust, as  
15          appropriate, the information security program consistent with  
16          any relevant changes in technology, the sensitivity of its  
17          nonpublic information, internal or external threats to  
18          information, and the licensee's own changing business  
19          arrangements, including mergers and acquisitions, alliances  
20          and joint ventures, outsourcing arrangements, and changes to  
21          information systems.

22          (h) As part of its information security program, a  
23          licensee shall establish a written incident response plan  
24          designed to promptly respond to and recover from any  
25          cybersecurity event that compromises the confidentiality,  
26          integrity, or availability of nonpublic information in its

1 possession, the licensee's information systems, or the  
2 continuing functionality of any aspect of the licensee's  
3 business or operations. The incident response plan shall  
4 address the following areas:

5 (1) the internal process for responding to a  
6 cybersecurity event;

7 (2) the goals of the incident response plan;

8 (3) the definition of clear roles, responsibilities,  
9 and levels of decision-making authority;

10 (4) external and internal communications and  
11 information sharing;

12 (5) identification of requirements for the remediation  
13 of any identified weaknesses in information systems and  
14 associated controls;

15 (6) documentation and reporting regarding  
16 cybersecurity events and related incident response  
17 activities; and

18 (7) the evaluation and revision of the incident  
19 response plan following a cybersecurity event, as  
20 necessary.

21 (i) Annually, an insurer domiciled in this State shall  
22 submit to the Director a written statement by February 15  
23 certifying that the insurer is in compliance with the  
24 requirements set forth in this Section. Each insurer shall  
25 maintain for examination by the Department all records,  
26 schedules, and data supporting this certificate for a period

1 of 5 years. To the extent an insurer has identified areas,  
2 systems, or processes that require material improvement,  
3 updating, or redesign, the insurer shall document the  
4 identification and the remedial efforts planned and underway  
5 to address such areas, systems, or processes. The  
6 documentation of identified areas, systems, or processes must  
7 be available for inspection by the Director.

8 (j) Licensees shall comply with subsection (f) 2 years  
9 after the effective date of this Act, and shall comply with all  
10 other subsections of this Section one year after the effective  
11 date of this Act.

12 Section 15. Investigation of a cybersecurity event.

13 (a) If the licensee learns that a cybersecurity event has  
14 occurred or may have occurred, the licensee, or an outside  
15 vendor or service provider designated to act on behalf of the  
16 licensee, shall conduct a prompt investigation.

17 (b) During the investigation the licensee, or an outside  
18 vendor or service provider designated to act on behalf of the  
19 licensee, shall, at a minimum, comply with as many of the  
20 following as possible:

21 (1) determine whether a cybersecurity event has  
22 occurred;

23 (2) assess the nature and scope of the cybersecurity  
24 event;

25 (3) identify any nonpublic information that may have

1           been involved in the cybersecurity event; and

2           (4) perform or oversee reasonable measures to restore  
3           the security of the information systems compromised in the  
4           cybersecurity event in order to prevent further  
5           unauthorized acquisition, release, or use of nonpublic  
6           information in the licensee's possession, custody, or  
7           control.

8           (c) If the licensee learns that a cybersecurity event has  
9           occurred or may have occurred in a system maintained by a  
10          third-party service provider, the licensee will complete the  
11          steps listed in subsection (b) or confirm and document that  
12          the third-party service provider has completed those steps.

13          (d) The licensee shall maintain records concerning all  
14          cybersecurity events for a period of at least 5 years from the  
15          date of the cybersecurity event and shall produce those  
16          records upon demand of the Director.

17          Section 20. Notification of a cybersecurity event.

18          (a) A licensee shall notify the Director as promptly as  
19          possible but no later than 72 hours after a determination that  
20          a cybersecurity event has occurred when either of the  
21          following criteria has been met:

22                 (1) this State is the licensee's state of domicile, in  
23                 the case of an insurer, or this State is the licensee's  
24                 home state, in the case of an insurance producer, as those  
25                 terms are defined in Article XXXI of the Illinois

1 Insurance Code; or

2 (2) the licensee reasonably believes that the  
3 nonpublic information involved is of 250 or more consumers  
4 residing in this State and that is either of the  
5 following:

6 (A) a cybersecurity event impacting the licensee  
7 of which notice is required to be provided to any  
8 government body, self-regulatory agency, or any other  
9 supervisory body pursuant to any State or federal law;  
10 or

11 (B) a cybersecurity event that has a reasonable  
12 likelihood of materially harming:

13 (i) any consumer residing in this State; or

14 (ii) any material part of the normal  
15 operations of the licensee.

16 (b) A licensee shall provide as much of the following  
17 information as possible:

18 (1) the date of the cybersecurity event;

19 (2) a description of how the information was exposed,  
20 lost, stolen, or breached, including the specific roles  
21 and responsibilities of third-party service providers, if  
22 any;

23 (3) how the cybersecurity event was discovered;

24 (4) whether any lost, stolen, or breached information  
25 has been recovered and if so, how it was recovered;

26 (5) the identity of the source of the cybersecurity



1 event;

2 (6) whether the licensee has filed a police report or  
3 has notified any regulatory, government, or law  
4 enforcement agencies and, if so, when such notification  
5 was provided;

6 (7) a description of the specific types of information  
7 acquired without authorization, including types of medical  
8 information, types of financial information, or types of  
9 information allowing identification of the consumer;

10 (8) the period during which the information system was  
11 compromised by the cybersecurity event;

12 (9) the number of total consumers in this State  
13 affected by the cybersecurity event; the licensee shall  
14 provide the best estimate in the initial report to the  
15 Director and update this estimate with each subsequent  
16 report to the Director pursuant to this Section;

17 (10) the results of any internal review identifying a  
18 lapse in either automated controls or internal procedures,  
19 or confirming that all automated controls or internal  
20 procedures were followed;

21 (11) a description of efforts being undertaken to  
22 remediate the situation which permitted the cybersecurity  
23 event to occur;

24 (12) a copy of the licensee's privacy policy and a  
25 statement outlining the steps the licensee will take to  
26 investigate and notify consumers affected by the

1           cybersecurity event; and

2           (13) the name of a contact person who is both familiar  
3           with the cybersecurity event and authorized to act for the  
4           licensee.

5           The licensee shall provide the information in electronic  
6           form as directed by the Director. The licensee shall have a  
7           continuing obligation to update and supplement initial and  
8           subsequent notifications to the Director concerning the  
9           cybersecurity event.

10          (c) Licensees shall comply with the Personal Information  
11          Protection Act, as applicable, and provide a copy of the  
12          notice sent to consumers under that statute to the Director  
13          when a licensee is required to notify the Director under  
14          subsection (a).

15          (d) If a licensee becomes aware of a cybersecurity event  
16          in a system maintained by a third-party service provider, the  
17          licensee shall treat the event as it would under subsection  
18          (a). The computation of licensee's deadlines shall begin on  
19          the day after the third-party service provider notifies the  
20          licensee of the cybersecurity event or the licensee otherwise  
21          has actual knowledge of the cybersecurity event, whichever is  
22          sooner.

23          (e) Nothing in this Act shall prevent or abrogate an  
24          agreement between a licensee and another licensee, a  
25          third-party service provider, or any other party to fulfill  
26          any of the investigation requirements imposed under Section 15

1 or notice requirements imposed under this Section.

2 (f) In the case of a cybersecurity event involving  
3 nonpublic information that is used by the licensee that is  
4 acting as an assuming insurer or in the possession, custody,  
5 or control of a licensee that is acting as an assuming insurer  
6 and that does not have a direct contractual relationship with  
7 the affected consumers, the assuming insurer shall notify its  
8 affected ceding insurers and the Director of its state of  
9 domicile within 72 hours after making the determination that a  
10 cybersecurity event has occurred.

11 In the case of a cybersecurity event involving nonpublic  
12 information that is in the possession, custody, or control of  
13 a third-party service provider of a licensee that is an  
14 assuming insurer, the assuming insurer shall notify its  
15 affected ceding insurers and the Director of its state of  
16 domicile within 72 hours after receiving notice from its  
17 third-party service provider that a cybersecurity event has  
18 occurred.

19 The ceding insurers that have a direct contractual  
20 relationship with affected consumers shall fulfill the  
21 consumer notification requirements imposed under the Personal  
22 Information Protection Act and any other notification  
23 requirements relating to a cybersecurity event imposed under  
24 this Section.

25 (g) In the case of a cybersecurity event involving  
26 nonpublic information that is in the possession, custody, or

1 control of a licensee that is an insurer or its third-party  
2 service provider and for which a consumer accessed the  
3 insurer's services through an independent insurance producer,  
4 the insurer shall notify the producers of record of all  
5 affected consumers as soon as practicable as directed by the  
6 Director. The insurer is excused from this obligation for  
7 those instances in which it does not have the current producer  
8 of record information for any individual consumer.

9 Section 25. Power of Director.

10 (a) The Director shall have power to examine and  
11 investigate into the affairs of any licensee to determine  
12 whether the licensee has been or is engaged in any conduct in  
13 violation of this Act. This power is in addition to the powers  
14 which the Director has under the Illinois Insurance Code,  
15 including Sections 132, 132.3, 132.4, 133, 401, 402, 403, and  
16 425 of the Illinois Insurance Code. Any investigation or  
17 examination shall be conducted pursuant to the Illinois  
18 Insurance Code, including Sections 132, 132.3, 132.4, 133,  
19 401, 402, 403, and 425 of the Illinois Insurance Code.

20 (b) Whenever the Director has reason to believe that a  
21 licensee has been or is engaged in conduct in this State which  
22 violates this Act, the Director may take action that is  
23 necessary or appropriate to enforce the provisions of this  
24 Act.

1 Section 30. Confidentiality.

2 (a) Any documents, materials, or other information in the  
3 control or possession of the Department that are furnished by  
4 a licensee or an employee or agent thereof acting on behalf of  
5 licensee pursuant to subsection (i) of Section 10, subsection  
6 (b) of Section 20, or that are obtained by the Director in an  
7 investigation or examination pursuant to Section 25 shall be  
8 confidential by law and privileged, shall not be subject to  
9 the Freedom of Information Act, shall not be subject to  
10 subpoena, and shall not be subject to discovery or admissible  
11 in evidence in any private civil action. However, the Director  
12 is authorized to use the documents, materials, or other  
13 information in the furtherance of any regulatory or legal  
14 action brought as a part of the Director's duties.

15 (b) Neither the Director nor any person who received  
16 documents, materials, or other information while acting under  
17 the authority of the Director shall be permitted or required  
18 to testify in any private civil action concerning any  
19 confidential documents, materials, or information subject to  
20 subsection (a).

21 (c) In order to assist in the performance of the  
22 Director's duties under this Act, the Director:

23 (1) may share documents, materials, or other  
24 information, including the confidential and privileged  
25 documents, materials, or information subject to subsection  
26 (a), with other State, federal, and international

1 regulatory agencies, with the National Association of  
2 Insurance Directors and its affiliates or subsidiaries,  
3 and with State, federal, and international law enforcement  
4 authorities, if the recipient agrees in writing to  
5 maintain the confidentiality and privileged status of the  
6 document, material, or other information;

7 (2) may receive documents, materials, or information,  
8 including otherwise confidential and privileged documents,  
9 materials, or information, from the National Association  
10 of Insurance Directors and its affiliates or subsidiaries  
11 and from regulatory and law enforcement officials of other  
12 foreign or domestic jurisdictions, and shall maintain as  
13 confidential or privileged any document, material, or  
14 information received with notice or the understanding that  
15 it is confidential or privileged under the laws of the  
16 jurisdiction that is the source of the document, material,  
17 or information;

18 (3) may share documents, materials, or other  
19 information subject to subsection (a), with a third-party  
20 consultant or vendor if the consultant agrees in writing  
21 to maintain the confidentiality and privileged status of  
22 the document, material, or other information; and

23 (4) may enter into agreements governing sharing and  
24 use of information consistent with this subsection.

25 (d) No waiver of any applicable privilege or claim of  
26 confidentiality in the documents, materials, or information

1 shall occur as a result of disclosure to the Director under  
2 this Section or as a result of sharing as authorized in  
3 subsection (c).

4 (e) Nothing in this Act shall prohibit the Director from  
5 releasing final, adjudicated actions that are open to public  
6 inspection pursuant to the Illinois Insurance Code to a  
7 database or other clearinghouse service maintained by the  
8 National Association of Insurance Directors and its affiliates  
9 or subsidiaries.

10 Section 35. Exceptions.

11 (a) The following exceptions shall apply to this Act:

12 (1) A licensee with fewer than 10 employees, including  
13 any independent contractors, is exempt from Section 10.

14 (2) A licensee subject to the Health Insurance  
15 Portability and Accountability Act that has established  
16 and maintains an information security program pursuant to  
17 such statutes, rules, regulations, procedures, or  
18 guidelines established thereunder, shall be considered to  
19 meet the requirements of Section 10 if the licensee is  
20 compliant with the Health Insurance Portability and  
21 Accountability Act and submits a written statement  
22 certifying its compliance with the same.

23 (3) An employee, agent, representative, or designee of  
24 a licensee that is also a licensee is exempt from Section  
25 10 and need not develop its own information security

1 program to the extent that the employee, agent,  
2 representative, or designee is covered by the information  
3 security program of the other licensee.

4 (b) If a licensee ceases to qualify for an exception, the  
5 licensee shall comply with this Act within 180 days.

6 Section 40. Penalties. In the case of a violation of this  
7 Act, a licensee may be penalized in accordance with the  
8 provisions of the Illinois Insurance Code, including Section  
9 403A of the Illinois Insurance Code.

10 Section 45. Rules. The Department may, in accordance with  
11 the Illinois Administrative Procedure Act and Section 401 of  
12 the Illinois Insurance Code, adopt such rules as shall be  
13 necessary to carry out the provisions of this Act.

14 Section 50. Severability. If any provision of this Act or  
15 its application to any person or circumstance is held invalid,  
16 the invalidity of that provision or application does not  
17 affect other provisions or applications of this Act that can  
18 be given effect without the invalid provision or application.

19 Section 105. The Freedom of Information Act is amended by  
20 changing Section 7.5 as follows:

21 (5 ILCS 140/7.5)



1           Sec. 7.5. Statutory exemptions. To the extent provided for  
2 by the statutes referenced below, the following shall be  
3 exempt from inspection and copying:

4           (a) All information determined to be confidential  
5 under Section 4002 of the Technology Advancement and  
6 Development Act.

7           (b) Library circulation and order records identifying  
8 library users with specific materials under the Library  
9 Records Confidentiality Act.

10          (c) Applications, related documents, and medical  
11 records received by the Experimental Organ Transplantation  
12 Procedures Board and any and all documents or other  
13 records prepared by the Experimental Organ Transplantation  
14 Procedures Board or its staff relating to applications it  
15 has received.

16          (d) Information and records held by the Department of  
17 Public Health and its authorized representatives relating  
18 to known or suspected cases of sexually transmissible  
19 disease or any information the disclosure of which is  
20 restricted under the Illinois Sexually Transmissible  
21 Disease Control Act.

22          (e) Information the disclosure of which is exempted  
23 under Section 30 of the Radon Industry Licensing Act.

24          (f) Firm performance evaluations under Section 55 of  
25 the Architectural, Engineering, and Land Surveying  
26 Qualifications Based Selection Act.

1 (g) Information the disclosure of which is restricted  
2 and exempted under Section 50 of the Illinois Prepaid  
3 Tuition Act.

4 (h) Information the disclosure of which is exempted  
5 under the State Officials and Employees Ethics Act, and  
6 records of any lawfully created State or local inspector  
7 general's office that would be exempt if created or  
8 obtained by an Executive Inspector General's office under  
9 that Act.

10 (i) Information contained in a local emergency energy  
11 plan submitted to a municipality in accordance with a  
12 local emergency energy plan ordinance that is adopted  
13 under Section 11-21.5-5 of the Illinois Municipal Code.

14 (j) Information and data concerning the distribution  
15 of surcharge moneys collected and remitted by carriers  
16 under the Emergency Telephone System Act.

17 (k) Law enforcement officer identification information  
18 or driver identification information compiled by a law  
19 enforcement agency or the Department of Transportation  
20 under Section 11-212 of the Illinois Vehicle Code.

21 (l) Records and information provided to a residential  
22 health care facility resident sexual assault and death  
23 review team or the Executive Council under the Abuse  
24 Prevention Review Team Act.

25 (m) Information provided to the predatory lending  
26 database created pursuant to Article 3 of the Residential

1 Real Property Disclosure Act, except to the extent  
2 authorized under that Article.

3 (n) Defense budgets and petitions for certification of  
4 compensation and expenses for court appointed trial  
5 counsel as provided under Sections 10 and 15 of the  
6 Capital Crimes Litigation Act. This subsection (n) shall  
7 apply until the conclusion of the trial of the case, even  
8 if the prosecution chooses not to pursue the death penalty  
9 prior to trial or sentencing.

10 (o) Information that is prohibited from being  
11 disclosed under Section 4 of the Illinois Health and  
12 Hazardous Substances Registry Act.

13 (p) Security portions of system safety program plans,  
14 investigation reports, surveys, schedules, lists, data, or  
15 information compiled, collected, or prepared by or for the  
16 Department of Transportation under Sections 2705-300 and  
17 2705-616 of the Department of Transportation Law of the  
18 Civil Administrative Code of Illinois, the Regional  
19 Transportation Authority under Section 2.11 of the  
20 Regional Transportation Authority Act, or the St. Clair  
21 County Transit District under the Bi-State Transit Safety  
22 Act.

23 (q) Information prohibited from being disclosed by the  
24 Personnel Record Review Act.

25 (r) Information prohibited from being disclosed by the  
26 Illinois School Student Records Act.

1           (s) Information the disclosure of which is restricted  
2 under Section 5-108 of the Public Utilities Act.

3           (t) All identified or deidentified health information  
4 in the form of health data or medical records contained  
5 in, stored in, submitted to, transferred by, or released  
6 from the Illinois Health Information Exchange, and  
7 identified or deidentified health information in the form  
8 of health data and medical records of the Illinois Health  
9 Information Exchange in the possession of the Illinois  
10 Health Information Exchange Office due to its  
11 administration of the Illinois Health Information  
12 Exchange. The terms "identified" and "deidentified" shall  
13 be given the same meaning as in the Health Insurance  
14 Portability and Accountability Act of 1996, Public Law  
15 104-191, or any subsequent amendments thereto, and any  
16 regulations promulgated thereunder.

17           (u) Records and information provided to an independent  
18 team of experts under the Developmental Disability and  
19 Mental Health Safety Act (also known as Brian's Law).

20           (v) Names and information of people who have applied  
21 for or received Firearm Owner's Identification Cards under  
22 the Firearm Owners Identification Card Act or applied for  
23 or received a concealed carry license under the Firearm  
24 Concealed Carry Act, unless otherwise authorized by the  
25 Firearm Concealed Carry Act; and databases under the  
26 Firearm Concealed Carry Act, records of the Concealed

1 Carry Licensing Review Board under the Firearm Concealed  
2 Carry Act, and law enforcement agency objections under the  
3 Firearm Concealed Carry Act.

4 (v-5) Records of the Firearm Owner's Identification  
5 Card Review Board that are exempted from disclosure under  
6 Section 10 of the Firearm Owners Identification Card Act.

7 (w) Personally identifiable information which is  
8 exempted from disclosure under subsection (g) of Section  
9 19.1 of the Toll Highway Act.

10 (x) Information which is exempted from disclosure  
11 under Section 5-1014.3 of the Counties Code or Section  
12 8-11-21 of the Illinois Municipal Code.

13 (y) Confidential information under the Adult  
14 Protective Services Act and its predecessor enabling  
15 statute, the Elder Abuse and Neglect Act, including  
16 information about the identity and administrative finding  
17 against any caregiver of a verified and substantiated  
18 decision of abuse, neglect, or financial exploitation of  
19 an eligible adult maintained in the Registry established  
20 under Section 7.5 of the Adult Protective Services Act.

21 (z) Records and information provided to a fatality  
22 review team or the Illinois Fatality Review Team Advisory  
23 Council under Section 15 of the Adult Protective Services  
24 Act.

25 (aa) Information which is exempted from disclosure  
26 under Section 2.37 of the Wildlife Code.

1           (bb) Information which is or was prohibited from  
2 disclosure by the Juvenile Court Act of 1987.

3           (cc) Recordings made under the Law Enforcement  
4 Officer-Worn Body Camera Act, except to the extent  
5 authorized under that Act.

6           (dd) Information that is prohibited from being  
7 disclosed under Section 45 of the Condominium and Common  
8 Interest Community Ombudsperson Act.

9           (ee) Information that is exempted from disclosure  
10 under Section 30.1 of the Pharmacy Practice Act.

11           (ff) Information that is exempted from disclosure  
12 under the Revised Uniform Unclaimed Property Act.

13           (gg) Information that is prohibited from being  
14 disclosed under Section 7-603.5 of the Illinois Vehicle  
15 Code.

16           (hh) Records that are exempt from disclosure under  
17 Section 1A-16.7 of the Election Code.

18           (ii) Information which is exempted from disclosure  
19 under Section 2505-800 of the Department of Revenue Law of  
20 the Civil Administrative Code of Illinois.

21           (jj) Information and reports that are required to be  
22 submitted to the Department of Labor by registering day  
23 and temporary labor service agencies but are exempt from  
24 disclosure under subsection (a-1) of Section 45 of the Day  
25 and Temporary Labor Services Act.

26           (kk) Information prohibited from disclosure under the

1           Seizure and Forfeiture Reporting Act.

2           (ll) Information the disclosure of which is restricted  
3           and exempted under Section 5-30.8 of the Illinois Public  
4           Aid Code.

5           (mm) Records that are exempt from disclosure under  
6           Section 4.2 of the Crime Victims Compensation Act.

7           (nn) Information that is exempt from disclosure under  
8           Section 70 of the Higher Education Student Assistance Act.

9           (oo) Communications, notes, records, and reports  
10          arising out of a peer support counseling session  
11          prohibited from disclosure under the First Responders  
12          Suicide Prevention Act.

13          (pp) Names and all identifying information relating to  
14          an employee of an emergency services provider or law  
15          enforcement agency under the First Responders Suicide  
16          Prevention Act.

17          (qq) Information and records held by the Department of  
18          Public Health and its authorized representatives collected  
19          under the Reproductive Health Act.

20          (rr) Information that is exempt from disclosure under  
21          the Cannabis Regulation and Tax Act.

22          (ss) Data reported by an employer to the Department of  
23          Human Rights pursuant to Section 2-108 of the Illinois  
24          Human Rights Act.

25          (tt) Recordings made under the Children's Advocacy  
26          Center Act, except to the extent authorized under that

1 Act.

2 (uu) Information that is exempt from disclosure under  
3 Section 50 of the Sexual Assault Evidence Submission Act.

4 (vv) Information that is exempt from disclosure under  
5 subsections (f) and (j) of Section 5-36 of the Illinois  
6 Public Aid Code.

7 (ww) Information that is exempt from disclosure under  
8 Section 16.8 of the State Treasurer Act.

9 (xx) Information that is exempt from disclosure or  
10 information that shall not be made public under the  
11 Illinois Insurance Code.

12 (yy) Information prohibited from being disclosed under  
13 the Illinois Educational Labor Relations Act.

14 (zz) Information prohibited from being disclosed under  
15 the Illinois Public Labor Relations Act.

16 (aaa) Information prohibited from being disclosed  
17 under Section 1-167 of the Illinois Pension Code.

18 (bbb) ~~(ccc)~~ Information that is prohibited from  
19 disclosure by the Illinois Police Training Act and the  
20 Illinois State Police Act.

21 (ccc) ~~(ddd)~~ Records exempt from disclosure under  
22 Section 2605-304 of the Illinois ~~Department of~~ State  
23 Police Law of the Civil Administrative Code of Illinois.

24 (ddd) ~~(eee)~~ Information prohibited from being  
25 disclosed under Section 35 of the Address Confidentiality  
26 for Victims of Domestic Violence, Sexual Assault, Human



1 Trafficking, or Stalking Act.

2 (eee) ~~(ddd)~~ Information prohibited from being  
3 disclosed under subsection (b) of Section 75 of the  
4 Domestic Violence Fatality Review Act.

5 (fff) Information exempt from disclosure under Section  
6 30 of the Insurance Data Security Law.

7 (Source: P.A. 101-13, eff. 6-12-19; 101-27, eff. 6-25-19;  
8 101-81, eff. 7-12-19; 101-221, eff. 1-1-20; 101-236, eff.  
9 1-1-20; 101-375, eff. 8-16-19; 101-377, eff. 8-16-19; 101-452,  
10 eff. 1-1-20; 101-466, eff. 1-1-20; 101-600, eff. 12-6-19;  
11 101-620, eff. 12-20-19; 101-649, eff. 7-7-20; 101-652, eff.  
12 1-1-22; 101-656, eff. 3-23-21; 102-36, eff. 6-25-21; 102-237,  
13 eff. 1-1-22; 102-292, eff. 1-1-22; 102-520, eff. 8-20-21;  
14 102-559, eff. 8-20-21; revised 10-5-21.)

15 Section 999. Effective date. This Act takes effect January  
16 1, 2023.