



## 102ND GENERAL ASSEMBLY

### State of Illinois

2021 and 2022

HB5248

Introduced 1/31/2022, by Rep. Keith R. Wheeler

#### SYNOPSIS AS INTRODUCED:

New Act  
5 ILCS 140/7.5

Creates the Insurance Data Security Act. Requires any person licensed, authorized to operate, or registered as an insurer in accordance with the insurance laws of this State to conduct a risk assessment of cybersecurity threats, implement appropriate security measures, and no less than annually assess the effectiveness of the safeguards' key controls, systems, and procedures. Requires a licensee to develop, implement, and maintain a written information security program based on the licensee's risk assessment. Requires each licensee to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations. Requires licensees domiciled in this State to annually submit a written certification of compliance to the Director of Insurance. Provides that a licensee shall notify the Director as promptly as possible, but not later than 72 hours from a determination that a cybersecurity event has occurred in specified circumstances. Provides standards and procedures for risk management, data security, and notification and investigation of cybersecurity events resulting in unauthorized access to, disruption of, or misuse of nonpublic data. Provides that the Director has the power to examine and investigate to determine whether a licensee has been or is engaged in any conduct in violation of the Act. Grants the Department of Insurance rulemaking authority to implement the Act. Provides that any documents, materials, or other information obtained pursuant to the Act is confidential by law and privileged, is not subject to the Freedom of Information Act, is not subject to subpoena, and is not subject to discovery or admissible in evidence in any private civil action. Makes a conforming change in the Freedom of Information Act. Defines terms. Effective January 1, 2023.

LRB102 22798 BMS 31948 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 Act.

6 Section 5. Purpose.

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

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

15 Section 10. 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, a policyholder, an insured, a beneficiary, a  
22 claimant, and a 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 of, 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 that results in a low probability of assigning meaning without  
18 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 an industrial or process control  
3 system, a telephone switching and private branch exchange  
4 system, or an environmental control system.

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

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

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

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

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

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

6           (a) Social Security number;

7           (b) driver's license number or non-driver  
8 identification card number;

9           (c) account number and credit or debit card  
10 number;

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

14           (e) biometric records; or

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

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

21           (b) the provision of health care to any consumer;  
22 or

23           (c) payment for the provision of health care to  
24 any consumer.

25           "Person" means any individual or any non-governmental  
26 entity, including, but not limited to, any non-governmental

1 partnership, corporation, branch, agency, or association.

2 "Publicly available information" means any information  
3 that a licensee has a reasonable basis to believe is lawfully  
4 made available to the general public from: federal, State, or  
5 local government records; widely distributed media; or  
6 disclosures to the general public that are required to be made  
7 by federal, State, or local law. For the purposes of this  
8 definition, a licensee has a reasonable basis to believe that  
9 information is lawfully made available to the general public  
10 if the licensee has taken steps to determine:

11 (1) that the information is of the type that is  
12 available to the general public; and

13 (2) whether a consumer can direct that the information  
14 not be made available to the general public and, if so,  
15 that such consumer has not done so.

16 "Risk assessment" means the risk assessment that each  
17 licensee is required to conduct under subsection (c) of  
18 Section 15 of this Act.

19 "State" means the State of Illinois.

20 "Third-party service provider" means a person, not  
21 otherwise defined as a licensee, that contracts with a  
22 licensee to maintain, process, store, or is otherwise  
23 permitted access to nonpublic information through its  
24 provision of services to the licensee.

25 Section 15. Information security program.

1           (a) No later than one year after the effective date of this  
2 Act, each licensee shall develop, implement, and maintain a  
3 comprehensive written information security program based on  
4 the licensee's risk assessment. The information security  
5 program shall contain administrative, technical, and physical  
6 safeguards for the protection of nonpublic information and the  
7 licensee's information system. The information security  
8 program shall be commensurate with the size and complexity of  
9 the licensee, the nature and scope of the licensee's  
10 activities, including its use of third-party service  
11 providers, and the sensitivity of the nonpublic information  
12 used by the licensee or in the licensee's possession, custody,  
13 or control.

14           (b) A licensee's information security program shall be  
15 designed to:

16                 (1) protect the security and confidentiality of  
17 nonpublic information and the security of the information  
18 system;

19                 (2) protect against any threats or hazards to the  
20 security or integrity of nonpublic information and the  
21 information system;

22                 (3) protect against unauthorized access to or use of  
23 nonpublic information and minimize the likelihood of harm  
24 to any consumer; and

25                 (4) define and periodically reevaluate a schedule for  
26 retention of nonpublic information and a mechanism for its

1 destruction when no longer needed.

2 (c) The licensee shall:

3 (1) designate one or more employees, an affiliate, or  
4 an outside vendor designated to act on behalf of the  
5 licensee who is responsible for the information security  
6 program;

7 (2) identify reasonably foreseeable internal or  
8 external threats that could result in unauthorized access,  
9 transmission, disclosure, misuse, alteration, or  
10 destruction of nonpublic information, including the  
11 security of information systems and nonpublic information  
12 that is accessible to, or held by, third-party service  
13 providers;

14 (3) assess the likelihood and potential damage of  
15 these threats, taking into consideration the sensitivity  
16 of the nonpublic information;

17 (4) assess the sufficiency of policies, procedures,  
18 information systems, and other safeguards in place to  
19 manage these threats, including consideration of threats  
20 in each relevant area of the licensee's operations,  
21 including:

22 (A) employee training and management;

23 (B) information systems, including network and  
24 software design, as well as information  
25 classification, governance, processing, storage,  
26 transmission, and disposal; and



1 (C) detecting, preventing, and responding to  
2 attacks, intrusions, or other system failures; and

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

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

8 (1) design its information security program to  
9 mitigate the identified risks, commensurate with the size  
10 and complexity of the licensee's activities, including its  
11 use of third-party service providers, and the sensitivity  
12 of the nonpublic information used by the licensee or in  
13 the licensee's possession, custody, or control;

14 (2) determine which security measures listed below are  
15 appropriate and implement such security measures:

16 (A) place access controls on information systems,  
17 including controls to authenticate and permit access  
18 only to authorized individuals to protect against the  
19 unauthorized acquisition of nonpublic information;

20 (B) identify and manage the data, personnel,  
21 devices, systems, and facilities that enable the  
22 organization to achieve business purposes in  
23 accordance with their relative importance to business  
24 objectives and the organization's risk strategy;

25 (C) restrict access at physical locations  
26 containing nonpublic information only to authorized

1 individuals;

2 (D) protect by encryption or other appropriate  
3 means all nonpublic information while it is  
4 transmitted over an external network and all nonpublic  
5 information stored on a laptop computer or other  
6 portable computing or storage device or media;

7 (E) adopt secure development practices for  
8 in-house developed applications utilized by the  
9 licensee and procedures for evaluating, assessing, or  
10 testing the security of externally developed  
11 applications utilized by the licensee;

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

14 (G) utilize effective controls, which may include  
15 multi-factor authentication procedures for any  
16 individual accessing nonpublic information;

17 (H) regularly test and monitor systems and  
18 procedures to detect actual and attempted attacks on,  
19 or intrusions into, information systems;

20 (I) include audit trails within the information  
21 security program designed to detect and respond to  
22 cybersecurity events and designed to reconstruct  
23 material financial transactions sufficient to support  
24 normal operations and obligations of the licensee;

25 (J) implement measures to protect against  
26 destruction, loss, or damage of nonpublic information

1 due to environmental hazards, such as fire and water  
2 damage or other catastrophes or technological  
3 failures; and

4 (K) develop, implement, and maintain procedures  
5 for the secure disposal of nonpublic information in  
6 any format.

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

9 (4) stay informed regarding emerging threats or  
10 vulnerabilities and utilize reasonable security measures  
11 when sharing information relative to the character of the  
12 sharing and the type of information shared; and

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

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

18 (1) require the licensee's executive management or its  
19 delegates to develop, implement, and maintain the  
20 licensee's information security program; and

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

24 (A) the overall status of the information security  
25 program and the licensee's compliance with this Act;  
26 and

1 (B) material matters related to the information  
2 security program, addressing issues such as risk  
3 assessment, risk management and control decisions,  
4 third-party service provider arrangements, results of  
5 testing, cybersecurity events or violations and  
6 management's responses thereto, and recommendations  
7 for changes in the information security program.

8 If executive management delegates any of its  
9 responsibilities under this Section, it shall oversee the  
10 development, implementation, and maintenance of the licensee's  
11 information security program prepared by the delegates and  
12 shall receive a report from the delegates complying with the  
13 requirements of the report to the board of directors as  
14 provided in paragraph (2) of this subsection (e).

15 (f) A licensee shall exercise due diligence in selecting  
16 its third-party service provider and, no later than 2 years  
17 after the effective date of this Act, shall require a  
18 third-party service provider to implement appropriate  
19 administrative, technical, and physical measures to protect  
20 and secure the information systems and nonpublic information  
21 that are accessible to, or held by, the third-party service  
22 provider.

23 (g) The licensee shall monitor, evaluate, and adjust, as  
24 appropriate, the information security program consistent with  
25 any relevant changes in technology, the sensitivity of its  
26 nonpublic information, internal or external threats to

1 information, and the licensee's own changing business  
2 arrangements, such as mergers and acquisitions, alliances and  
3 joint ventures, outsourcing arrangements, and changes to  
4 information systems.

5 (h) As part of its information security program, each  
6 licensee shall establish a written incident response plan  
7 designed to promptly respond to and recover from any  
8 cybersecurity event that compromises the confidentiality,  
9 integrity, or availability of nonpublic information in its  
10 possession, the licensee's information systems, or the  
11 continuing functionality of any aspect of the licensee's  
12 business or operations.

13 Such incident response plan shall address the following  
14 areas:

15 (1) the internal process for responding to a  
16 cybersecurity event;

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

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

20 (4) external and internal communications and  
21 information sharing;

22 (5) identification of requirements for the remediation  
23 of any identified weaknesses in information systems and  
24 associated controls;

25 (6) documentation and reporting regarding  
26 cybersecurity events and related incident response

1 activities; and

2 (7) the evaluation and revision as necessary of the  
3 incident response plan following a cybersecurity event.

4 (i) Annually by February 15, each insurer domiciled in  
5 this State shall submit to the Director a written statement  
6 certifying that the insurer is in compliance with the  
7 requirements set forth in this Section. Each insurer shall  
8 maintain for examination by the Department all records,  
9 schedules, and data supporting this certificate for a period  
10 of 5 years. To the extent an insurer has identified areas,  
11 systems, or processes that require material improvement,  
12 updating, or redesign, the insurer shall document the  
13 identification and the remedial efforts planned and underway  
14 to address such areas, systems, or processes. Such  
15 documentation must be available for inspection by the  
16 Director.

17 Section 20. Investigation of a cybersecurity event.

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

22 (b) During the investigation, the licensee, or an outside  
23 vendor or service provider designated to act on behalf of the  
24 licensee, shall perform or oversee reasonable measures to  
25 restore the security of the information systems compromised in

1 the cybersecurity event in order to prevent further  
2 unauthorized acquisition, release, or use of nonpublic  
3 information in the licensee's possession, custody, or control,  
4 and shall, at a minimum, determine as much of the following  
5 information as possible:

- 6 (1) whether a cybersecurity event has occurred;  
7 (2) the nature and scope of the cybersecurity event;  
8 and  
9 (3) any nonpublic information that may have been  
10 involved in the cybersecurity event.

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

16 (d) The licensee shall maintain records concerning all  
17 cybersecurity events for a period of at least 5 years after the  
18 date of the cybersecurity event and shall produce those  
19 records upon demand of the Director.

20 Section 25. Notification of a cybersecurity event.

21 (a) Each licensee shall notify the Director as promptly as  
22 possible, but in no event later than 72 hours from a  
23 determination that a cybersecurity event has occurred, when  
24 either of the following criteria has been met:

- 25 (1) this State is the licensee's state of domicile or

1 home state; 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 the cybersecurity event is  
5 either of the 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: (i) any consumer  
13 residing in this State; or (ii) any material part of  
14 the normal operations of the licensee.

15 (b) The licensee shall provide as much of the following  
16 information as possible in electronic form as directed by the  
17 Director:

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; in this paragraph,  
8 "specific types of information" means particular data  
9 elements, including types of medical information, types of  
10 financial information, or types of information allowing  
11 identification of the consumer;

12 (8) the period during which the information system was  
13 compromised by the cybersecurity event;

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

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

23 (11) a description of events being undertaken to  
24 remediate the situation that permitted the cybersecurity  
25 event to occur;

26 (12) a copy of the licensee's privacy policy and a

1 statement outlining the steps the licensee will take to  
2 investigate and notify consumers affected by the  
3 cybersecurity event; and

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

7 The licensee has a continuing obligation to update and  
8 supplement initial and subsequent notifications to the  
9 Director concerning the cybersecurity event.

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

15 (d) If the licensee has become aware of a cybersecurity  
16 event in a system maintained by a third-party service  
17 provider, the licensee shall treat the event as it would under  
18 subsection (a).

19 The computation of licensee's deadlines shall begin on the  
20 day after the third-party service provider notifies the  
21 licensee of the cybersecurity event or the licensee otherwise  
22 has actual knowledge of the cybersecurity event, whichever is  
23 sooner.

24 Nothing in this Act shall prevent or abrogate an agreement  
25 between a licensee and another licensee, a third-party service  
26 provider, or any other party to fulfill any of the

1 investigation requirements imposed under Section 20 or notice  
2 requirements imposed under this Section.

3 (e)(1) In the case of a cybersecurity event involving  
4 nonpublic information that is used by the licensee that is  
5 acting as an assuming insurer or in the possession, custody,  
6 or control of a licensee that is acting as an assumed insurer  
7 and that does not have a direct contractual relationship with  
8 the affected consumers, the assuming insurer shall notify its  
9 affected ceding insurers and the Director of its state of  
10 domicile within 72 hours of making the determination that a  
11 cybersecurity event has occurred.

12 The ceding insurers that have a direct contractual  
13 relationship with the affected consumers shall fulfill the  
14 consumer notification requirements imposed under the Personal  
15 Information Protection Act and any other notification  
16 requirements relating to a cybersecurity event under this  
17 Section.

18 (2) In the case of a cybersecurity event involving  
19 nonpublic information that is in the possession, custody, or  
20 control of a third-party service provider of a licensee that  
21 is an assuming insurer, the assuming insurer shall notify its  
22 affected ceding insurers and the Director of its state of  
23 domicile within 72 hours of receiving notice from its  
24 third-party service provider that a cybersecurity event has  
25 occurred.

26 The ceding insurers that have a direct contractual

1 relationship with affected consumers shall fulfill the  
2 consumer notification requirements imposed under the Personal  
3 Information Protection Act and any other notification  
4 requirements relating to a cybersecurity event imposed under  
5 this Section.

6 (f) In the case of a cybersecurity event involving  
7 nonpublic information that is in the possession, custody, or  
8 control of a licensee that is an insurer or its third-party  
9 service provider and for which a consumer accessed the  
10 insurer's services through an independent insurance producer,  
11 the insurer shall notify the producers of record of all  
12 affected consumers as soon as practicable as directed by the  
13 Director.

14 The insurer is excused from this obligation for those  
15 instances in which it does not have the current producer of  
16 record information for any individual consumer.

17 Section 30. Power of the Director.

18 (a) The Director has power to examine and investigation  
19 into the affairs of any licensee to determine whether the  
20 licensee has been or is engaged in any conduct in violation of  
21 this Act. This power is in addition to the powers the Director  
22 has under the Illinois Insurance Code. Any such investigation  
23 or examination shall be conducted pursuant to the requirements  
24 of the Illinois Insurance Code.

25 (b) Whenever the Director has reason to believe that a

1 licensee has been or is engaged in conduct in this State that  
2 violates this Act, the Director may take action that is  
3 necessary or appropriate to enforce the provisions of this  
4 Act.

5 Section 35. Confidentiality.

6 (a) Any documents, materials, or other information in the  
7 control or possession of the Department that is furnished by  
8 the licensee or an employee or agent thereof acting on behalf  
9 of the licensee in accordance with subsection (i) of Section  
10 15 or paragraph (2), (3), (4), (5), (8), (10), or (11) of  
11 subsection (b) of Section 25 or that are obtained by, created  
12 by, or disclosed to the Director in an investigation or  
13 examination under Section 30 is confidential by law and  
14 privileged, is not subject to the Freedom of Information Act,  
15 is not subject to subpoena, and is not subject to discovery or  
16 admissible in evidence in any private civil action. However,  
17 the Director may use the documents, materials, or other  
18 information in the furtherance of any regulatory or legal  
19 action brought as a part of the Director's duties. The  
20 Director shall not otherwise make the documents, materials, or  
21 other information public without the prior written consent of  
22 the licensee.

23 (b) Neither the Director nor any person who received  
24 documents, materials, or other information while acting under  
25 the authority of the Director shall be permitted or required

1 to testify in any private civil action concerning any  
2 confidential documents, materials, or information subject to  
3 subsection (a).

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

6 (1) may share documents, materials, or other  
7 information, including the confidential and privileged  
8 documents, materials, or information subject to subsection  
9 (a), with other State, federal, and international  
10 regulatory agencies, with the National Association of  
11 Insurance Commissioners, its affiliates or subsidiaries,  
12 and with State, federal, and international law enforcement  
13 authorities, provided that the recipient agrees in writing  
14 to maintain the confidentiality and privileged status of  
15 the document, material, or other information;

16 (2) may receive documents, materials, or information,  
17 including otherwise confidential and privileged documents,  
18 materials, or information, from the National Association  
19 of Insurance Commissioners, its affiliates or  
20 subsidiaries, and from regulatory and law enforcement  
21 officials of other foreign or domestic jurisdictions, and  
22 shall maintain as confidential and privileged any  
23 document, material, or information received with notice or  
24 the understanding that it is confidential or privileged  
25 under the laws of the jurisdiction that is the source of  
26 the document, material, or information;

1           (3) may share documents, materials, or other  
2 information subject to subsection (a) with a third-party  
3 consultant or vendor, if the consultant agrees in writing  
4 to maintain the confidentiality and privileged status of  
5 the document, material, or other information; and

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

8           (d) No waiver of any applicable privilege or claim of  
9 confidentiality in the documents, materials, or information  
10 shall occur as a result of disclosure to the Director under  
11 this Section or as a result of sharing as authorized in  
12 subsection (c).

13           (e) Nothing in this Act shall prohibit the Director from  
14 releasing final, adjudicated actions that are open to public  
15 inspection pursuant to the Illinois Insurance Code to a  
16 database or other clearinghouse service maintained by the  
17 National Association of Insurance Commissioners, its  
18 affiliates, or its subsidiaries.

19           Section 40. Exceptions.

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

21           (1) A licensee with fewer than 10 employees, including  
22 any independent contractors, is exempt from Section 15 of  
23 this Act.

24           (2) A licensee subject to the federal Health Insurance  
25 Portability and Accountability Act that has established

1 and maintains an information security program pursuant to  
2 such statutes, rules, regulations, procedures, or  
3 guidelines established thereunder will be considered to  
4 meet the requirements of Section 15, provided that  
5 licensee is compliant with, and submits a written  
6 statement certifying its compliance with, the same.

7 (3) An employee, agent, representative, or designee of  
8 a licensee, who is also a licensee, is exempt from Section  
9 15 and need not develop its own information security  
10 program to the extent that the employee, agent,  
11 representative, or designee is covered by the information  
12 security program of the other licensee.

13 (b) If a licensee ceases to qualify for an exception, such  
14 licensee has 180 days to comply with this Act.

15 Section 45. Penalties. In the case of a violation of this  
16 Act, a licensee may be penalized in accordance with the  
17 provisions of the Illinois Insurance Code.

18 Section 50. Rules. The Department may, in accordance with  
19 the Illinois Administrative Procedure Act, adopt rules to  
20 implement the provisions of this Act.

21 Section 55. Severability. If any provision of this Act or  
22 its application to any person or circumstance is for any  
23 reason held to be invalid, the remainder of this Act and the



1 application of such provision to other persons or  
2 circumstances shall not be affected.

3 Section 900. The Freedom of Information Act is amended by  
4 changing Section 7.5 as follows:

5 (5 ILCS 140/7.5)

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

9 (a) All information determined to be confidential  
10 under Section 4002 of the Technology Advancement and  
11 Development Act.

12 (b) Library circulation and order records identifying  
13 library users with specific materials under the Library  
14 Records Confidentiality Act.

15 (c) Applications, related documents, and medical  
16 records received by the Experimental Organ Transplantation  
17 Procedures Board and any and all documents or other  
18 records prepared by the Experimental Organ Transplantation  
19 Procedures Board or its staff relating to applications it  
20 has received.

21 (d) Information and records held by the Department of  
22 Public Health and its authorized representatives relating  
23 to known or suspected cases of sexually transmissible  
24 disease or any information the disclosure of which is

1 restricted under the Illinois Sexually Transmissible  
2 Disease Control Act.

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

5 (f) Firm performance evaluations under Section 55 of  
6 the Architectural, Engineering, and Land Surveying  
7 Qualifications Based Selection Act.

8 (g) Information the disclosure of which is restricted  
9 and exempted under Section 50 of the Illinois Prepaid  
10 Tuition Act.

11 (h) Information the disclosure of which is exempted  
12 under the State Officials and Employees Ethics Act, and  
13 records of any lawfully created State or local inspector  
14 general's office that would be exempt if created or  
15 obtained by an Executive Inspector General's office under  
16 that Act.

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

21 (j) Information and data concerning the distribution  
22 of surcharge moneys collected and remitted by carriers  
23 under the Emergency Telephone System Act.

24 (k) Law enforcement officer identification information  
25 or driver identification information compiled by a law  
26 enforcement agency or the Department of Transportation

1 under Section 11-212 of the Illinois Vehicle Code.

2 (l) Records and information provided to a residential  
3 health care facility resident sexual assault and death  
4 review team or the Executive Council under the Abuse  
5 Prevention Review Team Act.

6 (m) Information provided to the predatory lending  
7 database created pursuant to Article 3 of the Residential  
8 Real Property Disclosure Act, except to the extent  
9 authorized under that Article.

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

17 (o) Information that is prohibited from being  
18 disclosed under Section 4 of the Illinois Health and  
19 Hazardous Substances Registry Act.

20 (p) Security portions of system safety program plans,  
21 investigation reports, surveys, schedules, lists, data, or  
22 information compiled, collected, or prepared by or for the  
23 Department of Transportation under Sections 2705-300 and  
24 2705-616 of the Department of Transportation Law of the  
25 Civil Administrative Code of Illinois, the Regional  
26 Transportation Authority under Section 2.11 of the

1 Regional Transportation Authority Act, or the St. Clair  
2 County Transit District under the Bi-State Transit Safety  
3 Act.

4 (q) Information prohibited from being disclosed by the  
5 Personnel Record Review Act.

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

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

10 (t) All identified or deidentified health information  
11 in the form of health data or medical records contained  
12 in, stored in, submitted to, transferred by, or released  
13 from the Illinois Health Information Exchange, and  
14 identified or deidentified health information in the form  
15 of health data and medical records of the Illinois Health  
16 Information Exchange in the possession of the Illinois  
17 Health Information Exchange Office due to its  
18 administration of the Illinois Health Information  
19 Exchange. The terms "identified" and "deidentified" shall  
20 be given the same meaning as in the Health Insurance  
21 Portability and Accountability Act of 1996, Public Law  
22 104-191, or any subsequent amendments thereto, and any  
23 regulations promulgated thereunder.

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

1           (v) Names and information of people who have applied  
2           for or received Firearm Owner's Identification Cards under  
3           the Firearm Owners Identification Card Act or applied for  
4           or received a concealed carry license under the Firearm  
5           Concealed Carry Act, unless otherwise authorized by the  
6           Firearm Concealed Carry Act; and databases under the  
7           Firearm Concealed Carry Act, records of the Concealed  
8           Carry Licensing Review Board under the Firearm Concealed  
9           Carry Act, and law enforcement agency objections under the  
10          Firearm Concealed Carry Act.

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

14          (w) Personally identifiable information which is  
15          exempted from disclosure under subsection (g) of Section  
16          19.1 of the Toll Highway Act.

17          (x) Information which is exempted from disclosure  
18          under Section 5-1014.3 of the Counties Code or Section  
19          8-11-21 of the Illinois Municipal Code.

20          (y) Confidential information under the Adult  
21          Protective Services Act and its predecessor enabling  
22          statute, the Elder Abuse and Neglect Act, including  
23          information about the identity and administrative finding  
24          against any caregiver of a verified and substantiated  
25          decision of abuse, neglect, or financial exploitation of  
26          an eligible adult maintained in the Registry established

1 under Section 7.5 of the Adult Protective Services Act.

2 (z) Records and information provided to a fatality  
3 review team or the Illinois Fatality Review Team Advisory  
4 Council under Section 15 of the Adult Protective Services  
5 Act.

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

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

10 (cc) Recordings made under the Law Enforcement  
11 Officer-Worn Body Camera Act, except to the extent  
12 authorized under that Act.

13 (dd) Information that is prohibited from being  
14 disclosed under Section 45 of the Condominium and Common  
15 Interest Community Ombudsperson Act.

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

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

20 (gg) Information that is prohibited from being  
21 disclosed under Section 7-603.5 of the Illinois Vehicle  
22 Code.

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

25 (ii) Information which is exempted from disclosure  
26 under Section 2505-800 of the Department of Revenue Law of

1 the Civil Administrative Code of Illinois.

2 (jj) Information and reports that are required to be  
3 submitted to the Department of Labor by registering day  
4 and temporary labor service agencies but are exempt from  
5 disclosure under subsection (a-1) of Section 45 of the Day  
6 and Temporary Labor Services Act.

7 (kk) Information prohibited from disclosure under the  
8 Seizure and Forfeiture Reporting Act.

9 (ll) Information the disclosure of which is restricted  
10 and exempted under Section 5-30.8 of the Illinois Public  
11 Aid Code.

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

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

16 (oo) Communications, notes, records, and reports  
17 arising out of a peer support counseling session  
18 prohibited from disclosure under the First Responders  
19 Suicide Prevention Act.

20 (pp) Names and all identifying information relating to  
21 an employee of an emergency services provider or law  
22 enforcement agency under the First Responders Suicide  
23 Prevention Act.

24 (qq) Information and records held by the Department of  
25 Public Health and its authorized representatives collected  
26 under the Reproductive Health Act.

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

3 (ss) Data reported by an employer to the Department of  
4 Human Rights pursuant to Section 2-108 of the Illinois  
5 Human Rights Act.

6 (tt) Recordings made under the Children's Advocacy  
7 Center Act, except to the extent authorized under that  
8 Act.

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

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

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

16 (xx) Information that is exempt from disclosure or  
17 information that shall not be made public under the  
18 Illinois Insurance Code.

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

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

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

25 (bbb) ~~(ccc)~~ Information that is prohibited from  
26 disclosure by the Illinois Police Training Act and the



1 Illinois State Police Act.

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

5 (ddd) ~~(bbb)~~ Information prohibited from being  
6 disclosed under Section 35 of the Address Confidentiality  
7 for Victims of Domestic Violence, Sexual Assault, Human  
8 Trafficking, or Stalking Act.

9 (eee) ~~(ddd)~~ Information prohibited from being  
10 disclosed under subsection (b) of Section 75 of the  
11 Domestic Violence Fatality Review Act.

12 (fff) Information that is exempt from disclosure under  
13 Section 35 of the Insurance Data Security Act.

14 (Source: P.A. 101-13, eff. 6-12-19; 101-27, eff. 6-25-19;  
15 101-81, eff. 7-12-19; 101-221, eff. 1-1-20; 101-236, eff.  
16 1-1-20; 101-375, eff. 8-16-19; 101-377, eff. 8-16-19; 101-452,  
17 eff. 1-1-20; 101-466, eff. 1-1-20; 101-600, eff. 12-6-19;  
18 101-620, eff. 12-20-19; 101-649, eff. 7-7-20; 101-652, eff.  
19 1-1-22; 101-656, eff. 3-23-21; 102-36, eff. 6-25-21; 102-237,  
20 eff. 1-1-22; 102-292, eff. 1-1-22; 102-520, eff. 8-20-21;  
21 102-559, eff. 8-20-21; revised 10-5-21.)

22 Section 999. Effective date. This Act takes effect January  
23 1, 2023.