

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) financial account number, credit card number,  
9 or debit 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, except if the  
20 information is otherwise required to be retained by law or  
21 rule or if targeted disposal is not reasonably feasible  
22 due to the manner in which the information is maintained.

23 (c) A licensee shall:

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

1 program;

2 (2) identify reasonably foreseeable internal or  
3 external threats that could result in unauthorized access,  
4 transmission, disclosure, misuse, alteration, or  
5 destruction of nonpublic information, including the  
6 security of information systems and nonpublic information  
7 that are accessible to or held by third-party service  
8 providers;

9 (3) assess the likelihood and potential damage of  
10 these threats, taking into consideration the sensitivity  
11 of the nonpublic information;

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

17 (A) employee training and management;

18 (B) information systems, including network and  
19 software design, as well as information  
20 classification, governance, processing, storage,  
21 transmission, and disposal; and

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

24 (5) implement information safeguards to manage the  
25 threats identified in its ongoing assessment, and, no less  
26 than annually, assess the effectiveness of the safeguards'

1 key controls, systems, and procedures.

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

3 (1) design its information security program to  
4 mitigate the identified risks, commensurate with the size  
5 and complexity of the licensee, the nature and scope of  
6 the licensee's activities, including its use of  
7 third-party service providers, and the sensitivity of the  
8 nonpublic information used by the licensee or in the  
9 licensee's possession, custody, or control;

10 (2) select and implement appropriate security measures  
11 from the following:

12 (A) place access controls on information systems,  
13 including controls to authenticate and permit access  
14 only to authorized individuals to protect against the  
15 unauthorized acquisition of nonpublic information;

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

21 (C) restrict access at physical locations  
22 containing nonpublic information only to authorized  
23 individuals;

24 (D) protect, by encryption or other appropriate  
25 means, all nonpublic information while being  
26 transmitted over an external network and all nonpublic



1 information stored on a laptop computer or other  
2 portable computing or storage device or media;

3 (E) adopt secure development practices for  
4 in-house-developed applications utilized by the  
5 licensee and procedures for evaluating, assessing, or  
6 testing the security of externally developed  
7 applications utilized by the licensee;

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

10 (G) utilize effective controls, including  
11 multifactor authentication procedures for any  
12 individual accessing nonpublic information;

13 (H) regularly test and monitor systems and  
14 procedures to detect actual and attempted attacks on  
15 or intrusions into information systems;

16 (I) include audit trails within the information  
17 security program designed to detect and respond to  
18 cybersecurity events and designed to reconstruct  
19 material financial transactions sufficient to support  
20 normal operations and obligations of the licensee;

21 (J) implement measures to protect against  
22 destruction, loss, or damage of nonpublic information  
23 due to environmental hazards, including fire and water  
24 damage, other catastrophes, or technological failures;  
25 and

26 (K) develop, implement, and maintain procedures

1 for the secure disposal of nonpublic information in  
2 any format;

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

5 (4) stay informed regarding emerging threats or  
6 vulnerabilities and utilize reasonable security measures  
7 when sharing information relative to the character of the  
8 sharing and the type of information shared; and

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

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

14 (1) require the licensee's executive management or its  
15 delegates to develop, implement, and maintain the  
16 licensee's information security program;

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

20 (A) the overall status of the information security  
21 program and the licensee's compliance with this Act;  
22 and

23 (B) material matters related to the information  
24 security program, addressing issues such as risk  
25 assessment, risk management and control decisions,  
26 third-party service provider arrangements, results of

1 testing, cybersecurity events or violations and  
2 management's responses thereto, and recommendations  
3 for changes in the information security program; and

4 (3) if executive management delegates any of its  
5 responsibilities under this Section, it shall oversee the  
6 development, implementation, and maintenance of the  
7 licensee's information security program prepared by the  
8 delegate and shall receive a report from the delegate  
9 complying with the requirements of the report to the board  
10 of directors.

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

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

26 (h) As part of its information security program, a

1 licensee shall establish a written incident response plan  
2 designed to promptly respond to and recover from any  
3 cybersecurity event that compromises the confidentiality,  
4 integrity, or availability of nonpublic information in its  
5 possession, the licensee's information systems, or the  
6 continuing functionality of any aspect of the licensee's  
7 business or operations. The incident response plan shall  
8 address the following areas:

9 (1) the internal process for responding to a  
10 cybersecurity event;

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

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

14 (4) external and internal communications and  
15 information sharing;

16 (5) identification of requirements for the remediation  
17 of any identified weaknesses in information systems and  
18 associated controls;

19 (6) documentation and reporting regarding  
20 cybersecurity events and related incident response  
21 activities; and

22 (7) the evaluation and revision of the incident  
23 response plan following a cybersecurity event, as  
24 necessary.

25 (i) Annually, an insurer domiciled in this State shall  
26 submit to the Director a written statement by April 15

1 certifying that the insurer is in compliance with the  
2 requirements set forth in this Section. Each insurer shall  
3 maintain for examination by the Department all records,  
4 schedules, and data supporting this certificate for a period  
5 of 5 years. To the extent an insurer has identified areas,  
6 systems, or processes that require material improvement,  
7 updating, or redesign, the insurer shall document the  
8 identification and the remedial efforts planned and underway  
9 to address such areas, systems, or processes. The  
10 documentation of identified areas, systems, or processes must  
11 be available for inspection by the Director.

12 (j) Licensees shall comply with subsection (f) 2 years  
13 after the effective date of this Act, and shall comply with all  
14 other subsections of this Section one year after the effective  
15 date of this Act.

16 Section 15. Investigation of a cybersecurity event.

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

21 (b) During the investigation the licensee, or an outside  
22 vendor or service provider designated to act on behalf of the  
23 licensee, shall, at a minimum, comply with as many of the  
24 following as possible:

25 (1) determine whether a cybersecurity event has

1 occurred;

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

4 (3) identify any nonpublic information that may have  
5 been involved in the cybersecurity event; and

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

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

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

21 Section 20. Notification of a cybersecurity event.

22 (a) A licensee shall notify the Director as promptly as  
23 possible but no later than 3 business days after a  
24 determination that a cybersecurity event has occurred when  
25 either of the following criteria has been met:

1           (1) this State is the licensee's state of domicile, in  
2           the case of an insurer, or this State is the licensee's  
3           home state, in the case of an insurance producer, as those  
4           terms are defined in Article XXXI of the Illinois  
5           Insurance Code, and the cybersecurity event has a  
6           reasonable likelihood of materially harming any consumer  
7           residing in this State or any material part of the normal  
8           operations of the licensee; or

9           (2) the licensee reasonably believes that the  
10          nonpublic information involved is of 250 or more consumers  
11          residing in this State and that is either of the  
12          following:

13                (A) a cybersecurity event impacting the licensee  
14                of which notice is required to be provided to any  
15                government body, self-regulatory agency, or any other  
16                supervisory body pursuant to any State or federal law;  
17                or

18                (B) a cybersecurity event that has a reasonable  
19                likelihood of materially harming:

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

21                       (ii) any material part of the normal  
22                       operations of the licensee.

23          (b) A licensee shall provide as much of the following  
24          information as possible:

25                (1) the date of the cybersecurity event;

26                (2) a description of how the information was exposed,

1 lost, stolen, or breached, including the specific roles  
2 and responsibilities of third-party service providers, if  
3 any;

4 (3) how the cybersecurity event was discovered;

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

7 (5) the identity of the source of the cybersecurity  
8 event;

9 (6) whether the licensee has filed a police report or  
10 has notified any regulatory, government, or law  
11 enforcement agencies and, if so, when such notification  
12 was provided;

13 (7) a description of the specific types of information  
14 acquired without authorization, including types of medical  
15 information, types of financial information, or types of  
16 information allowing identification of the consumer;

17 (8) the period during which the information system was  
18 compromised by the cybersecurity event;

19 (9) the number of total consumers in this State  
20 affected by the cybersecurity event; the licensee shall  
21 provide the best estimate in the initial report to the  
22 Director and update this estimate with each subsequent  
23 report to the Director pursuant to this Section;

24 (10) the results of any internal review identifying a  
25 lapse in either automated controls or internal procedures,  
26 or confirming that all automated controls or internal



1 procedures were followed;

2 (11) a description of efforts being undertaken to  
3 remediate the situation which permitted the cybersecurity  
4 event to occur;

5 (12) a copy of the licensee's privacy policy and a  
6 statement outlining the steps the licensee will take to  
7 investigate and notify consumers affected by the  
8 cybersecurity event; and

9 (13) the name of a contact person who is both familiar  
10 with the cybersecurity event and authorized to act for the  
11 licensee.

12 The licensee shall provide the information in electronic  
13 form as directed by the Director. The licensee shall have a  
14 continuing obligation to update and supplement initial and  
15 subsequent notifications to the Director regarding material  
16 changes to previously provided information relating to the  
17 cybersecurity event.

18 (c) Licensees shall comply with the Personal Information  
19 Protection Act, as applicable, and provide a copy of the  
20 notice sent to consumers under that statute to the Director  
21 when a licensee is required to notify the Director under  
22 subsection (a).

23 (d) If a licensee becomes aware of a cybersecurity event  
24 in a system maintained by a third-party service provider, the  
25 licensee shall treat the event as it would under subsection  
26 (a) unless the third-party service provider provides the

1 notice required under subsection (a) to the Director. The  
2 computation of licensee's deadlines shall begin on the day  
3 after the third-party service provider notifies the licensee  
4 of the cybersecurity event or the licensee otherwise has  
5 actual knowledge of the cybersecurity event, whichever is  
6 sooner.

7 (e) Nothing in this Act shall prevent or abrogate an  
8 agreement between a licensee and another licensee, a  
9 third-party service provider, or any other party to fulfill  
10 any of the investigation requirements imposed under Section 15  
11 or notice requirements imposed under this Section.

12 (f) In the case of a cybersecurity event involving  
13 nonpublic information that is used by the licensee that is  
14 acting as an assuming insurer or in the possession, custody,  
15 or control of a licensee that is acting as an assuming insurer  
16 and that does not have a direct contractual relationship with  
17 the affected consumers, the assuming insurer shall notify its  
18 affected ceding insurers and the Director of its state of  
19 domicile within 3 business days after making the determination  
20 that a cybersecurity event has occurred.

21 In the case of a cybersecurity event involving nonpublic  
22 information that is in the possession, custody, or control of  
23 a third-party service provider of a licensee that is an  
24 assuming insurer, the assuming insurer shall notify its  
25 affected ceding insurers and the Director of its state of  
26 domicile within 3 business days after receiving notice from

1 its third-party service provider that a cybersecurity event  
2 has occurred.

3 The ceding insurers that have a direct contractual  
4 relationship with affected consumers shall fulfill the  
5 consumer notification requirements imposed under the Personal  
6 Information Protection Act and any other notification  
7 requirements relating to a cybersecurity event imposed under  
8 this Section.

9 (g) In the case of a cybersecurity event involving  
10 nonpublic information that is in the possession, custody, or  
11 control of a licensee that is an insurer or its third-party  
12 service provider and for which a consumer accessed the  
13 insurer's services through an independent insurance producer,  
14 the insurer shall notify the producers of record of all  
15 affected consumers as soon as practicable as directed by the  
16 Director. The insurer is excused from this obligation for  
17 those instances in which it does not have the current producer  
18 of record information for any individual consumer.

19 Section 25. Power of Director.

20 (a) The Director shall have power to examine and  
21 investigate the affairs of any licensee to determine whether  
22 the licensee has been or is engaged in any conduct in violation  
23 of this Act. This power is in addition to the powers which the  
24 Director has under the Illinois Insurance Code, including  
25 Sections 132, 132.3, 132.4, 133, 401, 402, 403, and 425 of the

1 Illinois Insurance Code. Any investigation or examination  
2 shall be conducted pursuant to the Illinois Insurance Code,  
3 including Sections 132, 132.3, 132.4, 133, 401, 402, 403, and  
4 425 of the Illinois Insurance Code.

5 (b) Whenever the Director has reason to believe that a  
6 licensee has been or is engaged in conduct in this State which  
7 violates this Act, the Director may take action that is  
8 necessary or appropriate to enforce the provisions of this  
9 Act.

10 Section 30. Confidentiality.

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

24 (b) Neither the Director nor any person who received  
25 documents, materials, or other information while acting under

1 the authority of the Director shall be permitted or required  
2 to testify in any private civil action concerning any  
3 confidential documents, materials, or information subject to  
4 subsection (a).

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

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

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

1 document, material, or information;

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

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

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

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

20 Section 35. Exceptions.

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

22 (1) A licensee with fewer than 50 employees, including  
23 any independent contractors, is exempt from Section 10.

24 (2) A licensee that is subject to, governed by, and  
25 compliant with the privacy, security, and breach

1 notification rules issued by the United States Department  
2 of Health and Human Services, Parts 160 and 164 of Title 45  
3 of the Code of Federal Regulations, established pursuant  
4 to the Health Insurance Portability and Accountability Act  
5 of 1996, Public Law 104-191, and the Health Information  
6 Technology for Economic and Clinical Health Act, Public  
7 Law 111-5, HITECH, and that maintains nonpublic  
8 information in the same manner as protected health  
9 information pursuant to an information security program  
10 shall be considered to meet the requirements of Section 10  
11 and Section 15 of this Act. To claim this exemption, the  
12 licensee must submit an annual statement by April 15  
13 certifying its compliance with the applicable provisions  
14 of federal law referenced in this paragraph.

15 (3) An employee, agent, representative, or designee of  
16 a licensee that is also a licensee is exempt from Section  
17 10 and need not develop its own information security  
18 program to the extent that the employee, agent,  
19 representative, or designee is covered by the information  
20 security program of the other licensee.

21 (b) If a licensee ceases to qualify for an exception, the  
22 licensee shall demonstrate a good faith effort to comply with  
23 this Act within 180 days and shall certify compliance in  
24 accordance with subsection (i) of Section 10 no sooner than  
25 one year after ceasing to qualify for an exception.

1           Section 40. Penalties. In the case of a violation of this  
2 Act, a licensee may be penalized in accordance with the  
3 provisions of the Illinois Insurance Code, including Section  
4 403A of the Illinois Insurance Code.

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

9           Section 50. Severability. If any provision of this Act or  
10 its application to any person or circumstance is held invalid,  
11 the invalidity of that provision or application does not  
12 affect other provisions or applications of this Act that can  
13 be given effect without the invalid provision or application.

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

16           (5 ILCS 140/7.5)

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

20           (a) All information determined to be confidential  
21 under Section 4002 of the Technology Advancement and  
22 Development Act.



1           (b) Library circulation and order records identifying  
2 library users with specific materials under the Library  
3 Records Confidentiality Act.

4           (c) Applications, related documents, and medical  
5 records received by the Experimental Organ Transplantation  
6 Procedures Board and any and all documents or other  
7 records prepared by the Experimental Organ Transplantation  
8 Procedures Board or its staff relating to applications it  
9 has received.

10          (d) Information and records held by the Department of  
11 Public Health and its authorized representatives relating  
12 to known or suspected cases of sexually transmissible  
13 disease or any information the disclosure of which is  
14 restricted under the Illinois Sexually Transmissible  
15 Disease Control Act.

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

18          (f) Firm performance evaluations under Section 55 of  
19 the Architectural, Engineering, and Land Surveying  
20 Qualifications Based Selection Act.

21          (g) Information the disclosure of which is restricted  
22 and exempted under Section 50 of the Illinois Prepaid  
23 Tuition Act.

24          (h) Information the disclosure of which is exempted  
25 under the State Officials and Employees Ethics Act, and  
26 records of any lawfully created State or local inspector

1 general's office that would be exempt if created or  
2 obtained by an Executive Inspector General's office under  
3 that Act.

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

8 (j) Information and data concerning the distribution  
9 of surcharge moneys collected and remitted by carriers  
10 under the Emergency Telephone System Act.

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

15 (l) Records and information provided to a residential  
16 health care facility resident sexual assault and death  
17 review team or the Executive Council under the Abuse  
18 Prevention Review Team Act.

19 (m) Information provided to the predatory lending  
20 database created pursuant to Article 3 of the Residential  
21 Real Property Disclosure Act, except to the extent  
22 authorized under that Article.

23 (n) Defense budgets and petitions for certification of  
24 compensation and expenses for court appointed trial  
25 counsel as provided under Sections 10 and 15 of the  
26 Capital Crimes Litigation Act. This subsection (n) shall

1 apply until the conclusion of the trial of the case, even  
2 if the prosecution chooses not to pursue the death penalty  
3 prior to trial or sentencing.

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

7 (p) Security portions of system safety program plans,  
8 investigation reports, surveys, schedules, lists, data, or  
9 information compiled, collected, or prepared by or for the  
10 Department of Transportation under Sections 2705-300 and  
11 2705-616 of the Department of Transportation Law of the  
12 Civil Administrative Code of Illinois, the Regional  
13 Transportation Authority under Section 2.11 of the  
14 Regional Transportation Authority Act, or the St. Clair  
15 County Transit District under the Bi-State Transit Safety  
16 Act.

17 (q) Information prohibited from being disclosed by the  
18 Personnel Record Review Act.

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

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

23 (t) All identified or deidentified health information  
24 in the form of health data or medical records contained  
25 in, stored in, submitted to, transferred by, or released  
26 from the Illinois Health Information Exchange, and

1 identified or deidentified health information in the form  
2 of health data and medical records of the Illinois Health  
3 Information Exchange in the possession of the Illinois  
4 Health Information Exchange Office due to its  
5 administration of the Illinois Health Information  
6 Exchange. The terms "identified" and "deidentified" shall  
7 be given the same meaning as in the Health Insurance  
8 Portability and Accountability Act of 1996, Public Law  
9 104-191, or any subsequent amendments thereto, and any  
10 regulations promulgated thereunder.

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

14 (v) Names and information of people who have applied  
15 for or received Firearm Owner's Identification Cards under  
16 the Firearm Owners Identification Card Act or applied for  
17 or received a concealed carry license under the Firearm  
18 Concealed Carry Act, unless otherwise authorized by the  
19 Firearm Concealed Carry Act; and databases under the  
20 Firearm Concealed Carry Act, records of the Concealed  
21 Carry Licensing Review Board under the Firearm Concealed  
22 Carry Act, and law enforcement agency objections under the  
23 Firearm Concealed Carry Act.

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

1           (w) Personally identifiable information which is  
2           exempted from disclosure under subsection (g) of Section  
3           19.1 of the Toll Highway Act.

4           (x) Information which is exempted from disclosure  
5           under Section 5-1014.3 of the Counties Code or Section  
6           8-11-21 of the Illinois Municipal Code.

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

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

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

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

23          (cc) Recordings made under the Law Enforcement  
24          Officer-Worn Body Camera Act, except to the extent  
25          authorized under that Act.

26          (dd) Information that is prohibited from being

1 disclosed under Section 45 of the Condominium and Common  
2 Interest Community Ombudsperson Act.

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

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

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

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

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

15 (jj) Information and reports that are required to be  
16 submitted to the Department of Labor by registering day  
17 and temporary labor service agencies but are exempt from  
18 disclosure under subsection (a-1) of Section 45 of the Day  
19 and Temporary Labor Services Act.

20 (kk) Information prohibited from disclosure under the  
21 Seizure and Forfeiture Reporting Act.

22 (ll) Information the disclosure of which is restricted  
23 and exempted under Section 5-30.8 of the Illinois Public  
24 Aid Code.

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

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

3           (oo) Communications, notes, records, and reports  
4           arising out of a peer support counseling session  
5           prohibited from disclosure under the First Responders  
6           Suicide Prevention Act.

7           (pp) Names and all identifying information relating to  
8           an employee of an emergency services provider or law  
9           enforcement agency under the First Responders Suicide  
10          Prevention Act.

11          (qq) Information and records held by the Department of  
12          Public Health and its authorized representatives collected  
13          under the Reproductive Health Act.

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

16          (ss) Data reported by an employer to the Department of  
17          Human Rights pursuant to Section 2-108 of the Illinois  
18          Human Rights Act.

19          (tt) Recordings made under the Children's Advocacy  
20          Center Act, except to the extent authorized under that  
21          Act.

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

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

1           (wv) Information that is exempt from disclosure under  
2 Section 16.8 of the State Treasurer Act.

3           (xx) Information that is exempt from disclosure or  
4 information that shall not be made public under the  
5 Illinois Insurance Code.

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

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

10          aaa) Information prohibited from being disclosed  
11 under Section 1-167 of the Illinois Pension Code.

12          bbb) Information that is prohibited from disclosure  
13 by the Illinois Police Training Act and the Illinois State  
14 Police Act.

15          ccc) Records exempt from disclosure under Section  
16 2605-304 of the Illinois State Police Law of the Civil  
17 Administrative Code of Illinois.

18          ddd) Information prohibited from being disclosed  
19 under Section 35 of the Address Confidentiality for  
20 Victims of Domestic Violence, Sexual Assault, Human  
21 Trafficking, or Stalking Act.

22          eee) Information prohibited from being disclosed  
23 under subsection (b) of Section 75 of the Domestic  
24 Violence Fatality Review Act.

25          fff) Images from cameras under the Expressway Camera  
26 Act. This subsection (fff) is inoperative on and after



1 July 1, 2023.

2 (ggg) ~~(fff)~~ Information prohibited from disclosure  
3 under paragraph (3) of subsection (a) of Section 14 of the  
4 Nurse Agency Licensing Act.

5 (hhh) 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; 102-813, eff. 5-13-22; 102-946, eff.  
15 7-1-22; 102-1042, eff. 6-3-22; revised 8-1-22.)

16 Section 999. Effective date. This Act takes effect January  
17 1, 2024.