# HB3040

LRB10209898BMS15216b

## 102ND GENERAL ASSEMBLY

## State of Illinois

## 2021 and 2022

### HB3040

Introduced 2/19/2021, 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, 2022.

LRB102 09898 BMS 15216 b

A BILL FOR

AN ACT concerning regulation.

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

Section 1. Short title. This Act may be cited as the Insurance Data Security Act.

Section 5. Purpose.

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

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

Section 10. Definitions. As used in this Act:

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

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

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

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

"Department" means the Department of Insurance.

"Director" means the Director of Insurance.

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

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

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

disposition of electronic information, as well as any specialized system, such as an industrial or process control system, a telephone switching and private branch exchange system, or an environmental control system.

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

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

(1) knowledge factors, such as a password;

(2) possession factors, such as a token or text message on a mobile phone; or

(3) inherence factors, such as a biometric characteristic.

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

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

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

(a) Social Security number;

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

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

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

(e) biometric records; or

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

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

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

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

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

partnership, corporation, branch, agency, or association.

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

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

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

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

"State" means the State of Illinois.

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

Section 15. Information security program.

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

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

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

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

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

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

destruction when no longer needed.

(c) The licensee shall:

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

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

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

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

(A) employee training and management;

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

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

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

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

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

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

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

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

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

individuals;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(h) As part of its information security program, each licensee shall 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.

Such incident response plan shall address the following areas:

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

(2) the goals of the incident response plan;

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

(4) external and internal communications and information sharing;

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

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

activities; and

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

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

Section 20. Investigation of a cybersecurity event.

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

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

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

(1) whether a cybersecurity event has occurred;

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

(3) any nonpublic information that may have been involved in the cybersecurity event.

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

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

Section 25. Notification of a cybersecurity event.

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

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

home state; or

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

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

(B) a cybersecurity event that has a reasonable likelihood of materially harming: (i) any consumer residing in this State; or (ii) any material part of the normal operations of the licensee.

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

(1) the date of the cybersecurity event;

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

(3) how the cybersecurity event was discovered;

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

(5) the identity of the source of the cybersecurity

event;

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

(7) a description of the specific types of information acquired without authorization; in this paragraph, "specific types of information" means particular data elements, including types of medical information, types of financial information, or types of information allowing identification of the consumer;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The ceding insurers that have a direct contractual

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

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

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

Section 30. Power of the Director.

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

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

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

Section 35. Confidentiality.

(a) Any documents, materials, or other information in the control or possession of the Department that is furnished by the licensee or an employee or agent thereof acting on behalf of the licensee in accordance with subsection (i) of Section 15 or paragraph (2), (3), (4), (5), (8), (10), or (11) of subsection (b) of Section 25 or that are obtained by, created by, or disclosed to the Director in an investigation or examination under Section 30 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. However, the Director may use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the Director's duties. The Director shall not otherwise make the documents, materials, or other information public without the prior written consent of the licensee.

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

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

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

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

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

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

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

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

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

Section 40. Exceptions.

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

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

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

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

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

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

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

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

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

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

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

(5 ILCS 140/7.5)

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

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

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

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

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

restricted under the Illinois Sexually Transmissible Disease Control Act.

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

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

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

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

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

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

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

under Section 11-212 of the Illinois Vehicle Code.

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

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

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

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

(p) Security portions of system safety program plans, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority under Section 2.11 of the Regional Transportation Authority Act or the St. Clair County Transit District under the Bi-State Transit Safety Act.

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

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

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

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

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

(v) Names and information of people who have applied for or received Firearm Owner's Identification Cards under the Firearm Owners Identification Card Act or applied for

or received a concealed carry license under the Firearm Concealed Carry Act, unless otherwise authorized by the Firearm Concealed Carry Act; and databases under the Firearm Concealed Carry Act, records of the Concealed Carry Licensing Review Board under the Firearm Concealed Carry Act, and law enforcement agency objections under the Firearm Concealed Carry Act.

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

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

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

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

(aa) Information which is exempted from disclosure

under Section 2.37 of the Wildlife Code.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(tt) Recordings made under the Children's Advocacy

Center Act, except to the extent authorized under that Act.

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

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

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

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

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

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

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

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

(Source: P.A. 100-20, eff. 7-1-17; 100-22, eff. 1-1-18; 100-201, eff. 8-18-17; 100-373, eff. 1-1-18; 100-464, eff. 8-28-17; 100-465, eff. 8-31-17; 100-512, eff. 7-1-18; 100-517, eff. 6-1-18; 100-646, eff. 7-27-18; 100-690, eff. 1-1-19; 100-863, eff. 8-14-18; 100-887, eff. 8-14-18; 101-13, eff. 6-12-19; 101-27, eff. 6-25-19; 101-81, eff. 7-12-19; 101-221,

eff. 1-1-20; 101-236, eff. 1-1-20; 101-375, eff. 8-16-19; 101-377, eff. 8-16-19; 101-452, eff. 1-1-20; 101-466, eff. 1-1-20; 101-600, eff. 12-6-19; 101-620, eff 12-20-19; 101-649, eff. 7-7-20.)

Section 999. Effective date. This Act takes effect on January 1, 2022.