INSURANCE (40 PA.C.S.) - INSURANCE DATA SECURITY, REPEALING PROVISIONS RELATING TO SMALL COMPANY EXEMPTION, ADOPTION OF EXEMPTION STANDARDS OF NAIC VALUATION MANUAL AND IMPOSING PENALTIES

Act of Jun. 14, 2023, P.L. 4, No. 2 Cl. 40
Session of 2023
No. 2023-2

HB 739

AN ACT

Amending Title 40 (Insurance) of the Pennsylvania Consolidated Statutes, in regulation of insurers and related persons generally, providing for insurance data security; in reserve liabilities, repealing provisions relating to small company exemption and providing for adoption of exemption standards of NAIC Valuation Manual; and imposing penalties.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Title 40 of the Pennsylvania Consolidated Statutes is amended by adding a chapter to read:

CHAPTER 45
INSURANCE DATA SECURITY

Subchapter
A. Preliminary Provisions
B. Procedures
C. Enforcement
D. Miscellaneous Provisions

SUBCHAPTER A
PRELIMINARY PROVISIONS

Sec.
4501. Scope of chapter.
4502. Definitions.

§ 4501. Scope of chapter.

This chapter relates to insurance data security.

§ 4502. Definitions.

The following words and phrases when used in this chapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

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

"Commissioner." The Insurance Commissioner of the Commonwealth.

"Consumer." An individual, including an applicant, policyholder, insured, beneficiary, claimant or certificate holder, who is a resident of this Commonwealth and whose nonpublic information is in a licensee's possession, custody or control.

"Cybersecurity event." As follows:

(1) An event resulting in unauthorized access to, disruption of or misuse of an information system or nonpublic information stored on the information system.

(2) The term does not include:

(i) The unauthorized acquisition of encrypted nonpublic information if the encryption, process or key

is not also acquired, released or used without authorization.

(ii) An event in 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." The Insurance Department of the Commonwealth.

"Encrypted." The transformation of data into a form that has a low probability of assignment of meaning without the use of a protective process or key.

"Information security program." 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." Any of the following:

(1) A discrete set of information resources that is stored in an electronic system and is organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic nonpublic information.

(2) Any specialized system such as an industrial or process control system, telephone switching and private branch exchange system or an environmental control system.

"Insurer." An insurance company, association, exchange, interinsurance exchange, health maintenance organization, preferred provider organization, professional health services plan corporation subject to Chapter 63 (relating to professional health services plan corporations), a hospital plan corporation subject to Chapter 61 (relating to hospital plan corporations), fraternal benefit society, beneficial association, Lloyd's insurer or health plan corporation.

"Licensee." As follows:

(1) A person that is or is required to be licensed, authorized to operate or registered under the insurance laws of this Commonwealth.

(2) The term does not include:

(i) A purchasing group or risk retention group as defined in section 1502 of the act of May 17, 1921 (P.L.682, No.284), known as The Insurance Company Law of 1921, that is chartered and licensed in a state other than this Commonwealth.

(ii) A person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

"Multifactor authentication." Authentication through verification of at least two 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 telephone.

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

"Nonpublic information." Information that is stored or maintained in an electronic system, is not publicly available information and is any of the following:

(1) Business-related information of a licensee that would cause a materially adverse impact to the business, operations or security of the licensee if the information is tampered with, accessed, used or subject to unauthorized disclosure.

(2) Information concerning a consumer that because of a name, number, personal mark or other identifier, can be

used to identify the consumer, in combination with any one or more of the following data elements:

(i) Social Security number.

(ii) Driver's license number or nondriver identification card number.

(iii) Financial account number, credit card number or debit card number.

(iv) A security code, access code or password that would permit access to a consumer's financial account.

(v) Biometric records.

(3) Information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that can be used to identify a particular consumer and that relates to any of the following:

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

(ii) The provision of health care to any consumer.

(iii) Payment for the provision of health care to any consumer.

"Person." An individual or nongovernmental entity, including a nongovernmental partnership, corporation, branch, agency or association.

"Publicly available information." Information that a licensee has a reasonable basis to believe is lawfully made available to the general public from any of the following:

(1) Federal, State or local government records.

(2) Widely distributed media.

(3) Disclosures to the general public that are required to be made in accordance with Federal, State or local law.

"Risk assessment." The assessment that each licensee is required to conduct under section 4512 (relating to risk assessment).

"Third-party service provider." As follows:

(1) A person that contracts with a licensee to maintain, process or store, or is otherwise permitted to access, nonpublic information through its provision of services to the licensee.

(2) The term does not include a licensee.

SUBCHAPTER B
PROCEDURES

Sec.

§ 4511. Differentiation between types of information.

For purposes of determining what constitutes publicly available information, a licensee is deemed to have 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 is able to direct that the information not be made available to the general public and, if so, that the consumer has not done so.

§ 4512. Risk assessment.

A licensee shall conduct a risk assessment, which must:

(1) 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 are accessible to, or held by, third-party service providers.

(2) Assess the likelihood and potential damage of threats, taking into consideration the sensitivity of the nonpublic information.

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

(i) Employee training and management.

(ii) Information systems, including network and software design and information classification, governance, processing, storage, transmission and disposal.

(iii) Detection, prevention and response to attacks, intrusions or other system failures.

(4) Implement information safeguards to manage the threats identified in its ongoing assessment.

(5) At least annually, assess the effectiveness of the safeguards' key controls, systems and procedures.

§ 4513. Information security program.

(a) Requirement for implementation and objectives.--Each licensee shall develop, implement and maintain a comprehensive written information security program based on the licensee's risk assessment that:

(1) Contains administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information systems.

(2) Is commensurate with the following:

(i) The size and complexity of the licensee.

(ii) The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

(iii) The sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

(3) Is designed to protect:

(i) The security and confidentiality of nonpublic information and the security of the information systems.

(ii) Against any threats or hazards to the security or integrity of nonpublic information and the information systems.

(iii) Against unauthorized access to or use of nonpublic information and that minimizes the likelihood of harm to a consumer.

(4) Defines and periodically reevaluates a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(b) Designation of responsibility.--A licensee shall designate one or more employees, an affiliate or an outside vendor to act on behalf of the licensee who shall be responsible for the information security program of the licensee.

(c) Standards.--A licensee shall develop an information security program based on its risk assessment and shall:

(1) Design its information security program to mitigate the identified risks, in a manner that is commensurate with the following:

(i) The size and complexity of the licensee.

(ii) The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

(iii) The sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

(2) Determine which security measures are appropriate and implement the security measures by:

(i) Placing 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.

(ii) Identifying and managing the data, personnel, devices, systems and facilities that enable the licensee to achieve business purposes in accordance with their relative importance to business objectives and the licensee's risk strategy.

(iii) Restricting physical access to nonpublic information only to authorized individuals.

(iv) Protecting, by encryption or other appropriate means, all nonpublic information transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media.

(v) Adopting secure development practices for in-house developed applications utilized by the licensee.

(vi) Modifying the information systems in accordance with the licensee's information security program.

(vii) Utilizing effective controls, which may include multifactor authentication procedures, for any employees accessing nonpublic information.

(viii) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(ix) Including 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.

(x) Implementing 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.

(xi) Developing, implementing and maintaining 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 security measures when sharing information relative to the character of the sharing and the type of information shared.

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

(d) Monitoring, evaluation and adjustment.--A licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with:

(1) Any relevant changes in technology.

(2) The sensitivity of the licensee's nonpublic information.

(3) Internal or external threats to information.

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

(e) Incident response plan.--As part of its information security program, each licensee shall establish and maintain 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. The 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.

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

§ 4514. Corporate oversight.

(a) Duties.--If a 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 delegates to develop, implement and maintain the licensee's information security program.

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

(i) The overall status of the information security program and the licensee's compliance with this chapter.

(ii) Material matters related to the information security program, addressing issues such as:

(A) Risk assessment, risk management and control decisions.

(B) Third-party service provider arrangements.

(C) The results of testing.

(D) Cybersecurity events.

(E) Any violation of this chapter and management's responses to the violation.

(F) Recommendations for changes in the information security program.

(b) Delegation.--If the executive management of a licensee delegates any of its responsibilities under this section or section 4512 (relating to risk assessment), 4513 (relating to information security program) or 4515 (relating to oversight of third-party service provider arrangements), the executive management shall oversee the development, implementation and maintenance of the licensee's information security program prepared by the delegated entity, which shall provide a written report to the executive management in accordance with the reporting requirements of this chapter.

§ 4515. Oversight of third-party service provider arrangements.

A licensee shall:

(1) Exercise due diligence in selecting its third-party service provider.

(2) 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.

§ 4516. Certification.

(a) Requirement.--No later than the April 15 that is at least one year after the effective date of this section, and each April 15 thereafter, each insurer domiciled in this Commonwealth shall submit to the commissioner, in the form and manner prescribed by the department, a written statement certifying that the insurer is in compliance with the requirements of sections 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight) and 4515 (relating to oversight of third-party service provider arrangements).

(b) Documentation.--

(1) Each insurer shall maintain all records, schedules and data supporting the certification under this section for a period of five years and shall make that information available for examination by the department.

(2) To the extent that 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 the areas, systems or processes. The documentation shall be available for inspection by the department.

§ 4517. Investigation of cybersecurity event.

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

(b) Determination.--During an investigation under this section, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall, at a minimum, do as much of the following as possible:

(1) Determine whether a cybersecurity event has occurred.

(2) Assess the nature and scope of the cybersecurity event.

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

(4) 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.

(c) Third-party service provider.--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 specified in subsection (b) or confirm and document that the third-party service provider has completed those steps.

(d) Records.--A licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and shall produce those records upon demand of the commissioner.

§ 4518. Notification of cybersecurity event.

(a) Notification to commissioner.--A licensee shall notify the commissioner as promptly as possible, but in no event later than five business days from a determination, that a cybersecurity event involving nonpublic information that is in the possession of the licensee has occurred when either of the following criteria have been met:

(1) The cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this Commonwealth or any material part of the normal operations of the licensee and either:

(i) in the case of an insurer, this Commonwealth is the insurer's state of domicile; or

(ii) in the case of an insurance producer, as defined in section 601-A of the act of May 17, 1921 (P.L.789, No.285), known as The Insurance Department Act of 1921, this Commonwealth is the insurance producer's home state.

(2) The licensee reasonably believes that the nonpublic information involves 250 or more consumers residing in this Commonwealth and the cybersecurity event:

(i) impacts the licensee of which notice is required to be provided to a governmental body, self-regulatory agency or another supervisory body under any Federal or State law; or

(ii) has a reasonable likelihood of materially harming a consumer residing in this Commonwealth or any material part of the normal operations of the licensee.

(b) Content of notification.--As part of the notification under this section, a licensee shall provide as much of the following information as possible in electronic form:

(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 this was done.

(5) The identity of the source of the cybersecurity event.

(6) Whether the licensee has filed a police report or has notified any regulatory, governmental or law enforcement agency and, if so, when the notification was provided.

(7) A description of the specific types of information acquired without authorization, including particular data elements such as the types of medical information, financial information or other types of information allowing identification of the consumer.

(8) The period during which the information systems were compromised by the cybersecurity event.

(9) The number of total consumers in this Commonwealth affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner under this section.

(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 efforts 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 that the licensee will take to investigate and notify consumers affected by the cybersecurity event.

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

(c) Continuing obligation.--A licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relating to a cybersecurity event.

(d) Other notices required.--A licensee shall comply with section 3 of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, as applicable, and provide a copy of the notice sent to consumers under the Breach of Personal Information Notification Act to the commissioner, whenever the licensee is required to notify the commissioner under subsection (a).

(e) Notice regarding cybersecurity events of third-party service providers.--

(1) In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware, the licensee shall treat the event as it would under subsection (a) unless the third-party service provider provides the notice required under subsection (a) directly to the commissioner.

(2) The computation of a licensee's deadlines under this section 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.

(f) Notice regarding cybersecurity events of reinsurers to insurers.--

(1) In the case of a cybersecurity event involving nonpublic information that is used by a licensee, which is acting as an assuming insurer, or that is in the possession, custody or control of a licensee, which is acting as an assuming insurer and which does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three business days 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 section 3 of the Breach of Personal Information Notification Act and any other notification requirements relating to a cybersecurity event imposed 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 commissioner of its state of domicile within three business days 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 the affected consumers shall fulfill the consumer notification requirements imposed under section 3 of the Breach of Personal Information Notification Act and any other notification requirements relating to a cybersecurity event imposed under this section.

(3) A licensee acting as an assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this Commonwealth.

(g) Notice regarding cybersecurity events of insurers to producers of record.--In the case of a cybersecurity event involving nonpublic information in the possession, custody or control of a licensee that is an insurer or its third-party service provider for which a consumer accessed the insurer's services through an insurance producer, and for which consumer notice is required under section 3 of the Breach of Personal Information Notification Act, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers. The insurer shall be excused from this obligation in those instances in which the insurer does not have the current producer of record information for an individual consumer.

SUBCHAPTER C
ENFORCEMENT

Sec.

§ 4521. Power to examine licensees.

(a) Insurers.--The commissioner shall have the powers provided under Article IX of the act of May 17, 1921 (P.L.789, No.285), known as The Insurance Department Act of 1921, to examine and investigate an insurer to determine whether the insurer has been or is engaged in conduct in violation of section 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight), 4515 (relating to oversight of third-party service provider arrangements) or 4516 (relating to certification).

(b) Licensees other than insurers.--

(1) The commissioner shall have the power to examine and investigate a licensee not subject to Article IX of The Insurance Department Act of 1921 to determine whether the licensee has engaged in conduct in violation of this chapter.

(2) Each licensee subject to examination in accordance with paragraph (1) shall keep all books, records, accounts, papers, documents and any computer or other recordings relating to compliance with this chapter in the manner and time periods as the department, in its discretion, may require in order that the department's authorized representatives may verify and ascertain whether the company or person has complied with the requirements of this chapter.

(3) Each licensee subject to examination in accordance with paragraph (1) from whom information is sought and the officers, directors, employees and agents of the licensee shall provide to the examiners timely, convenient and free access at all reasonable hours at the licensee's offices to all books, records, accounts, papers, documents and any computer or other recordings relating to the property, assets, business and affairs of the licensee being examined. The following apply:

(i) The officers, directors, employees and agents of the licensee shall facilitate the examination and aid in the examination insofar as it is in their power to do so.

(ii) The refusal of a licensee by its officers, directors, employees or agents to submit to examination or to comply with any reasonable written request of the

examiners shall be grounds for suspension, revocation, refusal or nonrenewal of any license or authority held by the licensee to engage in an insurance or other business subject to the department's jurisdiction.

(iii) A proceeding for suspension, revocation, refusal or nonrenewal of any license or authority shall be conducted in accordance with 2 Pa.C.S. (relating to administrative law and procedure).

(c) Authorized actions by commissioner.--Notwithstanding and in addition to the powers specified under this section, whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this Commonwealth that violates this chapter, the commissioner may take an action that is necessary or appropriate to enforce the provisions of this chapter.

§ 4522. Penalties.

Upon the determination, after notice and hearing, that this chapter has been violated, the commissioner may impose the following penalties:

(1) Suspension or revocation of the licensee's license, authorization to operate or registration.

(2) Refusal to issue or renew a license, authorization to operate or registration.

(3) A cease and desist order.

(4) For each violation of this chapter that a licensee knew or reasonably should have known was a violation, a penalty of not more than $5,000, not to exceed an aggregate penalty of $100,000 in a single calendar year.

(5) For each violation of this chapter that a licensee did not know nor reasonably should have known was a violation, a penalty of not more than $1,000, not to exceed an aggregate penalty of $20,000 in a single calendar year.

SUBCHAPTER D
MISCELLANEOUS PROVISIONS

Sec.

§ 4531. Confidentiality.

(a) Requirement.--All information, documents, materials and copies thereof in the possession or control of the department that are produced by, obtained by or disclosed to the department or any other person in the course of an examination or investigation under this chapter shall be privileged and given confidential treatment and:

(1) Shall not be subject to discovery or admissible in evidence in a private civil action.

(2) Shall not be subject to subpoena.

(3) Shall be exempt from access under the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law.

(4) Shall not be made public by the department or any other person, except to regulatory or law enforcement officials of other jurisdictions, without the prior written consent of the licensee to which it pertains, except as provided in subsection (c).

(b) Civil actions.--The commissioner, department or any person that receives documents, materials or other information while acting under the authority of the commissioner or

department or with whom the documents, materials or other information are shared under this chapter may not be permitted or required to testify in a private civil action concerning confidential documents, materials or information covered under subsection (a).

(c) Department actions.--To assist in the performance of the regulatory duties under this chapter, the department:

(1) May share documents, materials or other information, including confidential and privileged documents, materials or other information subject to subsection (a), with the following:

(i) Federal, state and international regulatory agencies.

(ii) The National Association of Insurance Commissioners and its affiliates or subsidiaries.

(iii) Federal, state and international law enforcement authorities.

(iv) Third-party consultants, if the recipient agrees in writing to maintain the confidentiality and privileged status of the documents, materials or other information.

(2) May receive documents, materials or other information, including otherwise confidential and privileged documents, materials or other 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 or privileged any document, material or other 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 other information.

(d) No delegation.--The sharing of information by the department under this chapter shall not constitute a delegation of regulatory authority or rulemaking. The department shall be solely responsible for the administration, execution and enforcement of this chapter.

(e) No waiver of privilege or confidentiality.--The sharing of confidential information with, to or by the department as authorized by this chapter shall not constitute a waiver of any applicable privilege or claim of confidentiality.

(f) Information with third parties.--Confidential information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant as provided under this chapter shall:

(1) Be confidential and privileged.

(2) Be exempt from access under the Right-to-Know Law.

(3) Not be subject to subpoena.

(4) Not be subject to discovery or admissible as evidence in a private civil action.

§ 4532. Exemptions.

(a) Licensee criteria.--A licensee meeting any of the following criteria shall be exempt from sections 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight), 4515 (relating to oversight of third-party service provider arrangements) and 4516 (relating to certification):

(1) The licensee has fewer than 10 employees.

(2) The licensee has less than $5,000,000 in gross revenue.

(3) The licensee has less than $10,000,000 in year-end total assets.

(b) Federal law.--A licensee that is subject to and governed by the privacy, security and breach notification rules issued by the United States Department of Health and Human Services under 45 CFR Pts. 160 (relating to general administrative requirements) and 164 (relating to security and privacy), established in accordance with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, 123 Stat. 226-279 and 467-496), and which maintains nonpublic information in the same manner as protected health information shall be deemed to comply with the requirements of this chapter except for the notification requirements of section 4518(a), (b) and (c) (relating to notification of cybersecurity event).

(c) Employees, agents, representatives and designees.--An employee, agent, representative or designee of a licensee, who is also a licensee, shall be exempt from sections 4512, 4513, 4514, 4515 and 4516 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.

(d) Compliance.--If a licensee ceases to qualify for an exemption under this section, the licensee shall have 180 days to comply with this chapter.

§ 4533. Rules and regulations.

The commissioner may issue rules and regulations necessary to carry out the provisions of this chapter.

§ 4534. Construction with other laws.

(a) Private cause of action.--Nothing in this chapter shall be construed to:

(1) Create or imply a private cause of action for a violation of this chapter.

(2) Curtail a private cause of action that otherwise exists in the absence of this chapter.

(b) Exclusive standards.--Notwithstanding any other provision of law, this chapter shall establish the exclusive State standards applicable to licensees for data security, the licensees' investigation of a cybersecurity event and notification to the commissioner.

§ 4535. Prevention or abrogation of agreements.

Nothing in this chapter 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 4517 (relating to investigation of cybersecurity event) or notice requirements imposed under section 4518 (relating to notification of cybersecurity event).

§ 4536. Initial compliance.

Licensees shall have one year from the effective date of this section to implement sections 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight) and 4516 (relating to certification) and two years from the effective date of this section to implement section 4515 (relating to oversight of third-party service provider arrangements).

Section 2. Section 7142 of Title 40 is repealed:

[§ 7142. Small company exemption.

(a) Requirements.--A company seeking an exemption for any of its ordinary life policies issued on or after the operative date of the valuation manual may file a statement of exemption for the current calendar year with its domestic commissioner

prior to July 1 of that year if the following conditions are met:

(1) The company has less than $300,000,000 of ordinary life premiums and, if the company is a member of an NAIC group of life insurers, the group has combined ordinary life premiums of less than $600,000,000.

(2) The company reported total adjusted capital of at least 450% of the authorized control level risk-based capital in the most recent risk-based capital report. This paragraph shall not apply to fraternal benefit societies with less than $50,000,000 of ordinary life premiums.

(3) The appointed actuary has provided an unqualified opinion on the reserves reported in the most recent annual statement.

(4) Any universal life secondary guarantee policies issued or assumed by the company with an issue date on or after January 1, 2020, meet the definition of a nonmaterial secondary guarantee universal life product.

(b) Certification.--The statement of exemption under subsection (a) must certify that:

(1) The conditions under subsection (a) are met based on premiums and other values from the prior calendar year's financial statements.

(2) Any universal life secondary guarantee business issued since January 1, 2020, meets the definition of a nonmaterial secondary guarantee universal life product.

(c) Inclusion with NAIC filing.--The statement of exemption under subsection (a) shall also be included with the NAIC filing for the second quarter of that year.

(d) Rejection.--If the commissioner finds that the conditions in subsection (a) are not met, the commissioner shall reject the statement of exemption prior to September 1. If the commissioner rejects the exemption or the company does not file a statement of exemption, the company shall follow the requirements of the valuation manual minimum standard entitled VM-20 for the ordinary life policies issued on or after the operative date of the valuation manual.

(e) Approval.--If the statement of exemption under subsection (a) is granted, the minimum reserve requirements for the exempt company's ordinary life policies issued on or after the operative date of the valuation manual shall be as set forth in the valuation manual except for VM-20, but using mortality tables authorized by VM-20.

(f) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection unless the context clearly indicates otherwise:

"Nonmaterial secondary guarantee universal life product." A universal life product where the secondary guarantee meets the following parameters at the time of issue:

(1) The policy has only one secondary guarantee, which is in the form of a required premium consisting of either a specified annual or cumulative premium.

(2) The duration of the secondary guarantee for each policy is no longer than 20 years from issue through issue age 60, grading down by two-thirds year for each higher issue age to age 82, and thereafter five years.

(3) The present value of the required premium under the secondary guarantee must be at least as great as the present value of net premiums resulting from the appropriate valuation basic table over the course of the maximum secondary guarantee duration allowable under the contract

in aggregate and subject to the duration limit under paragraph (2). The following shall apply:

(i) The present value shall use minimum allowable valuation basic table rates, where preferred tables are subject to existing qualification requirements, and the maximum valuation interest rate as defined in VM-20 section 3(C)(2).

(ii) The minimum premiums shall be the annual required premiums over the course of the maximum secondary guarantee duration.

"Ordinary life premiums." Direct premiums plus reinsurance assumed premiums from an unaffiliated company from the ordinary life line of business reported in Exhibit 1-Part 1, entitled Premiums and Annuity Considerations for Life and Accident and Health Contracts, of the prior calendar year's life, accident and health annual statement or the fraternal annual statement.]

Section 3. Title 40 is amended by adding a section to read:

§ 7143. Adoption of exemption standards of NAIC Valuation Manual.

(a) Findings and declarations.--The General Assembly finds and declares that the work of NAIC and the participation of the commissioner in NAIC are essential to the general implementation of this chapter.

(b) Standards.--To effectuate the decision as to whether to exempt certain policies, certificates or products of a particular company from certain provisions of the NAIC Valuation Manual, the commissioner shall determine, on an annual basis, whether to adopt the standards for exemption specified in the most recent version of the NAIC Valuation Manual by submitting a statement of policy to the Legislative Reference Bureau for publication in the next available issue of the Pennsylvania Bulletin.

(c) Statement of policy.--A statement of policy issued under subsection (b) shall be exempt from the following:

(1) Section 205 of the act of July 31, 1968 (P.L.769, No.240), referred to as the Commonwealth Documents Law.

(2) Section 204(b) and 301(10) of the act of October 15, 1980 (P.L.950, No.164), known as the Commonwealth Attorneys Act.

(3) The act of June 25, 1982 (P.L.633, No.181), known as the Regulatory Review Act.

(d) Construction.--Nothing in this section shall affect any other provision in this chapter or apply to any action taken by the department prior to the effective date of this section.

Section 4. This act shall take effect as follows:

(1) The addition of 40 Pa.C.S. Ch. 45 shall take effect in 180 days.

(2) The remainder of this act shall take effect immediately.

APPROVED--The 14th day of June, A.D. 2023.

JOSH SHAPIRO