

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2499 Session of
2022

INTRODUCED BY PICKETT, DeLUCA, CIRESI, GUZMAN, HENNESSEY,
MENTZER, MILLARD, B. MILLER, OTTEN, RYAN AND THOMAS,
APRIL 8, 2022

REFERRED TO COMMITTEE ON INSURANCE, APRIL 8, 2022

AN ACT

1 Amending Title 40 (Insurance) of the Pennsylvania Consolidated
2 Statutes, in regulation of insurers and related persons
3 generally, providing for insurance data security and
4 establishing penalties.

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

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

9 CHAPTER 45

10 INSURANCE DATA SECURITY

11 Subchapter

12 A. Preliminary Provisions

13 B. Procedures

14 C. Enforcement

15 D. Miscellaneous Provisions

16 SUBCHAPTER A

17 PRELIMINARY PROVISIONS

18 Sec.

1 4501. Scope of chapter.

2 4502. Definitions.

3 § 4501. Scope of chapter.

4 This chapter relates to insurance data security.

5 § 4502. Definitions.

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

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

13 "Commissioner." The Insurance Commissioner of the
14 Commonwealth.

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

20 "Cybersecurity event." As follows:

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

24 (2) The term does not include:

25 (i) The unauthorized acquisition of encrypted
26 nonpublic information if the encryption, process or key
27 is not also acquired, released or used without
28 authorization.

29 (ii) An event in which the licensee has determined
30 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

1 of this Commonwealth.

2 (2) The term does not include:

3 (i) A purchasing group or risk retention group as
4 defined in section 1502 of the act of May 17, 1921
5 (P.L.682, No.284), known as The Insurance Company Law of
6 1921, that is chartered and licensed in a state other
7 than this Commonwealth.

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

10 "Multifactor authentication." Authentication through
11 verification of at least two of the following types of
12 authentication factors:

13 (1) Knowledge factors, such as a password.

14 (2) Possession factors, such as a token or text message
15 on a mobile telephone.

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

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

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

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

30 (i) Social Security number.

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

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

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

7 (v) Biometric records.

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

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

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

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

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

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

24 (1) Federal, State or local government records.

25 (2) Widely distributed media.

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

28 "Risk assessment." The assessment that each licensee is
29 required to conduct under section 4512 (relating to risk
30 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.

4512. Risk assessment.

4513. Information security program.

4514. Corporate oversight.

4515. Oversight of third-party service provider arrangements.

4516. Certification.

4517. Investigation of cybersecurity event.

4518. Notification of cybersecurity event.

§ 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

1 threats that could result in unauthorized access,
2 transmission, disclosure, misuse, alteration or destruction
3 of nonpublic information, including the security of
4 information systems and nonpublic information that are
5 accessible to, or held by, third-party service providers.

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

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

13 (i) Employee training and management.

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

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

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

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

24 § 4513. Information security program.

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

29 (1) Contains administrative, technical and physical
30 safeguards for the protection of nonpublic information and

1 the licensee's information systems.

2 (2) Is commensurate with the following:

3 (i) The size and complexity of the licensee.

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

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

10 (3) Is designed to protect:

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

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

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

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

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

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

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

1 (i) The size and complexity of the licensee.

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

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

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

10 (i) Placing access controls on information systems,
11 including controls to authenticate and permit access only
12 to authorized individuals to protect against the
13 unauthorized acquisition of nonpublic information.

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

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

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

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

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

30 (vii) Utilizing effective controls, which may

1 include multifactor authentication procedures, for any
2 employees accessing nonpublic information.

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

6 (ix) Including audit trails within the information
7 security program designed to detect and respond to
8 cybersecurity events and designed to reconstruct material
9 financial transactions sufficient to support normal
10 operations and obligations of the licensee.

11 (x) Implementing measures to protect against
12 destruction, loss or damage of nonpublic information due
13 to environmental hazards, such as fire and water damage
14 or other catastrophes or technological failures.

15 (xi) Developing, implementing and maintaining
16 procedures for the secure disposal of nonpublic
17 information in any format.

18 (3) Include cybersecurity risks in the licensee's
19 enterprise risk management process.

20 (4) Stay informed regarding emerging threats or
21 vulnerabilities and utilize security measures when sharing
22 information relative to the character of the sharing and the
23 type of information shared.

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

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

30 (1) Any relevant changes in technology.

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

3 (3) Internal or external threats to information.

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

8 (e) Incident response plan.--As part of its information
9 security program, each licensee shall establish and maintain a
10 written incident response plan designed to promptly respond to,
11 and recover from, any cybersecurity event that compromises the
12 confidentiality, integrity or availability of nonpublic
13 information in its possession, the licensee's information
14 systems or the continuing functionality of any aspect of the
15 licensee's business or operations. The incident response plan
16 shall address the following areas:

17 (1) The internal process for responding to a
18 cybersecurity event.

19 (2) The goals of the incident response plan.

20 (3) The definition of clear roles, responsibilities and
21 levels of decision-making authority.

22 (4) External and internal communications and information
23 sharing.

24 (5) Identification of requirements for the remediation
25 of any identified weaknesses in information systems and
26 associated controls.

27 (6) Documentation and reporting regarding cybersecurity
28 events and related incident response activities.

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

1 § 4514. Corporate oversight.

2 (a) Duties.--If a licensee has a board of directors, the
3 board or an appropriate committee of the board shall, at a
4 minimum:

5 (1) Require the licensee's executive management or
6 delegates to develop, implement and maintain the licensee's
7 information security program.

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

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

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

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

17 (B) Third-party service provider arrangements.

18 (C) The results of testing.

19 (D) Cybersecurity events.

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

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

24 (b) Delegation.--If the executive management of a licensee
25 delegates any of its responsibilities under this section or
26 section 4512 (relating to risk assessment), 4513 (relating to
27 information security program) or 4515 (relating to oversight of
28 third-party service provider arrangements), the executive
29 management shall oversee the development, implementation and
30 maintenance of the licensee's information security program

1 prepared by the delegated entity, which shall provide a written
2 report to the executive management in accordance with the
3 reporting requirements of this chapter.

4 § 4515. Oversight of third-party service provider arrangements.

5 A licensee shall:

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

8 (2) Require a third-party service provider to implement
9 appropriate administrative, technical and physical measures
10 to protect and secure the information systems and nonpublic
11 information that are accessible to, or held by, the third-
12 party service provider.

13 § 4516. Certification.

14 (a) Requirement.--No later than the April 15 that is at
15 least one year after the effective date of this section, and
16 each April 15 thereafter, each insurer domiciled in this
17 Commonwealth shall submit to the commissioner, in the form and
18 manner prescribed by the department, a written statement
19 certifying that the insurer is in compliance with the
20 requirements of sections 4512 (relating to risk assessment),
21 4513 (relating to information security program), 4514 (relating
22 to corporate oversight) and 4515 (relating to oversight of
23 third-party service provider arrangements).

24 (b) Documentation.--

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

29 (2) To the extent that an insurer has identified areas,
30 systems or processes that require material improvement,

1 updating or redesign, the insurer shall document the
2 identification and the remedial efforts planned and underway
3 to address the areas, systems or processes. The documentation
4 shall be available for inspection by the department.

5 § 4517. Investigation of cybersecurity event.

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

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

15 (1) Determine whether a cybersecurity event has
16 occurred.

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

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

21 (4) Perform or oversee reasonable measures to restore
22 the security of the information systems compromised in the
23 cybersecurity event in order to prevent further unauthorized
24 acquisition, release or use of nonpublic information in the
25 licensee's possession, custody or control.

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

1 those steps.

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

6 § 4518. Notification of cybersecurity event.

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

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

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

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

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

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

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

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

7 (1) The date of the cybersecurity event.

8 (2) A description of how the information was exposed,
9 lost, stolen or breached, including the specific roles and
10 responsibilities of third-party service providers, if any.

11 (3) How the cybersecurity event was discovered.

12 (4) Whether any lost, stolen or breached information has
13 been recovered and, if so, how this was done.

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

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

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

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

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

1 (10) The results of any internal review identifying a
2 lapse in either automated controls or internal procedures or
3 confirming that all automated controls or internal procedures
4 were followed.

5 (11) A description of efforts being undertaken to
6 remediate the situation that permitted the cybersecurity
7 event to occur.

8 (12) A copy of the licensee's privacy policy and a
9 statement outlining the steps that the licensee will take to
10 investigate and notify consumers affected by the
11 cybersecurity event.

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

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

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

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

28 (1) In the case of a cybersecurity event in a system
29 maintained by a third-party service provider of which the
30 licensee has become aware, the licensee shall treat the event

1 as it would under subsection (a) unless the third-party
2 service provider provides the notice required under
3 subsection (a) directly to the commissioner.

4 (2) The computation of a licensee's deadlines under this
5 section shall begin on the day after the third-party service
6 provider notifies the licensee of the cybersecurity event or
7 the licensee otherwise has actual knowledge of the
8 cybersecurity event, whichever is sooner.

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

11 (1) In the case of a cybersecurity event involving
12 nonpublic information that is used by a licensee, which is
13 acting as an assuming insurer, or that is in the possession,
14 custody or control of a licensee, which is acting as an
15 assuming insurer and which does not have a direct contractual
16 relationship with the affected consumers, the assuming
17 insurer shall notify its affected ceding insurers and the
18 commissioner of its state of domicile within three business
19 days of making the determination that a cybersecurity event
20 has occurred. The ceding insurers that have a direct
21 contractual relationship with the affected consumers shall
22 fulfill the consumer notification requirements imposed under
23 section 3 of the Breach of Personal Information Notification
24 Act and any other notification requirements relating to a
25 cybersecurity event imposed under this section.

26 (2) In the case of a cybersecurity event involving
27 nonpublic information that is in the possession, custody or
28 control of a third-party service provider of a licensee that
29 is an assuming insurer, the assuming insurer shall notify its
30 affected ceding insurers and the commissioner of its state of

1 domicile within three business days of receiving notice from
2 its third-party service provider that a cybersecurity event
3 has occurred. The ceding insurers that have a direct
4 contractual relationship with the affected consumers shall
5 fulfill the consumer notification requirements imposed under
6 section 3 of the Breach of Personal Information Notification
7 Act and any other notification requirements relating to a
8 cybersecurity event imposed under this section.

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

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

27 SUBCHAPTER C

28 ENFORCEMENT

29 Sec.

30 4521. Power to examine licensees.

1 4522. Penalties.

2 § 4521. Power to examine licensees.

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

12 (b) Licensees other than insurers.--

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

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

25 (3) Each licensee subject to examination in accordance
26 with paragraph (1) from whom information is sought and the
27 officers, directors, employees and agents of the licensee
28 shall provide to the examiners timely, convenient and free
29 access at all reasonable hours at the licensee's offices to
30 all books, records, accounts, papers, documents and any

1 computer or other recordings relating to the property,
2 assets, business and affairs of the licensee being examined.

3 The following apply:

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

7 (ii) The refusal of a licensee by its officers,
8 directors, employees or agents to submit to examination
9 or to comply with any reasonable written request of the
10 examiners shall be grounds for suspension, revocation,
11 refusal or nonrenewal of any license or authority held by
12 the licensee to engage in an insurance or other business
13 subject to the department's jurisdiction.

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

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

24 § 4522. Penalties.

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

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

30 (2) Refusal to issue or renew a license, authorization

1 to operate or registration.

2 (3) A cease and desist order.

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

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

11 SUBCHAPTER D

12 MISCELLANEOUS PROVISIONS

13 Sec.

14 4531. Confidentiality.

15 4532. Exemptions.

16 4533. Rules and regulations.

17 4534. Construction with other laws.

18 4535. Prevention or abrogation of agreements.

19 4536. Initial compliance.

20 § 4531. Confidentiality.

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

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

29 (2) Shall not be subject to subpoena.

30 (3) Shall be exempt from access under the act of

1 February 14, 2008 (P.L.6, No.3), known as the Right-to-Know
2 Law.

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

8 (b) Civil actions.--The commissioner, department or any
9 person that receives documents, materials or other information
10 while acting under the authority of the commissioner or
11 department or with whom the documents, materials or other
12 information are shared under this chapter may not be permitted
13 or required to testify in a private civil action concerning
14 confidential documents, materials or information covered under
15 subsection (a).

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

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

22 (i) Federal, state and international regulatory
23 agencies.

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

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

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

1 information.

2 (2) May receive documents, materials or other
3 information, including otherwise confidential and privileged
4 documents, materials or other information, from the National
5 Association of Insurance Commissioners, its affiliates or
6 subsidiaries and from regulatory and law enforcement
7 officials of other foreign or domestic jurisdictions, and
8 shall maintain as confidential or privileged any document,
9 material or other information received with notice or the
10 understanding that it is confidential or privileged under the
11 laws of the jurisdiction that is the source of the document,
12 material or other information.

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

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

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

26 (1) Be confidential and privileged.

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

28 (3) Not be subject to subpoena.

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

1 § 4532. Exemptions.

2 (a) Licensee criteria.--A licensee meeting any of the
3 following criteria shall be exempt from sections 4512 (relating
4 to risk assessment), 4513 (relating to information security
5 program), 4514 (relating to corporate oversight), 4515 (relating
6 to oversight of third-party service provider arrangements) and
7 4516 (relating to certification):

8 (1) The licensee has fewer than 10 employees.

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

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

13 (b) Federal law.--A licensee that is subject to and governed
14 by the privacy, security and breach notification rules issued by
15 the United States Department of Health and Human Services under
16 45 CFR Pts. 160 (relating to general administrative
17 requirements) and 164 (relating to security and privacy),
18 established in accordance with the Health Insurance Portability
19 and Accountability Act of 1996 (Public Law 104-191, 110 Stat.
20 1936) and the Health Information Technology for Economic and
21 Clinical Health Act (Public Law 111-5, 123 Stat. 226-279 and
22 467-496), and which maintains nonpublic information in the same
23 manner as protected health information shall be deemed to comply
24 with the requirements of this chapter except for the
25 notification requirements of section 4518(a), (b) and (c)
26 (relating to notification of cybersecurity event).

27 (c) Employees, agents, representatives and designees.--An
28 employee, agent, representative or designee of a licensee, who
29 is also a licensee, shall be exempt from sections 4512, 4513,
30 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.

1 Licensees shall have one year from the effective date of this
2 section to implement sections 4512 (relating to risk
3 assessment), 4513 (relating to information security program),
4 4514 (relating to corporate oversight) and 4516 (relating to
5 certification) and two years from the effective date of this
6 section to implement section 4515 (relating to oversight of
7 third-party service provider arrangements).

8 Section 2. This act shall take effect in 180 days.