CHAPTER 146c. STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.

Authority

The provisions of this Chapter 146c issued under sections 205, 506, 1501 and 1502 of The Administrative Code of 1929 (71 P. S. §§ 66, 186, 411 and 412); section 648 of The Insurance Department Act of 1921 (40 P. S. § 288); and the Unfair Insurance Practices Act (40 P. S. §§ 1171.1—1171.15), unless otherwise noted.

Source

The provisions of this Chapter 146c adopted August 6, 2004, effective March 1, 2005, 34 Pa.B. 4146, unless otherwise noted.

Cross References

This chapter cited in 25 Pa. Code § 401.45 (relating to confidentiality of insureds information).

§ 146c.1. Purpose.

This chapter establishes standards:

(1) For developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, under sections 501, 505(b) and 507 of the Gramm-Leach-Bliley Act (15 U.S.C.A. §§ 6801, 6805(b) and 6807).

(2) For ensuring the security and confidentiality of customer records and information.

(3) To protect against any reasonably anticipated threats or hazards to the security or integrity of the records.

(4) To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(5) That apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

§ 146c.2. Definitions.

The following words and terms, when used in this chapter, have the following meanings, unless the context clearly indicates otherwise:

Act—The Insurance Department Act of 1921 (40 P. S. §§ 1—321)

Customer—Either a ''customer'' as defined in § 146a.2 (relating to definitions) or a ''consumer'' as defined in § 146b.2 (relating to definitions).

Customer information—Either ''nonpublic personal financial information'' as defined in § 146a.2 or ''nonpublic personal health information'' as defined in § 146b.2 about a customer, whether in paper, electronic or other form that is maintained by or on behalf of the licensee.

Customer information systems—The electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

Department—The Insurance Department of the Commonwealth.

Licensee—As defined in either § 146a.2 or § 146b.2, except that the term shall not include a purchasing group or a nonadmitted insurer in regard to the surplus lines business conducted pursuant to sections 1601—1625 of The Insurance Company Law of 1921 (40 P. S. §§ 991.1601—991.1625).

Service provider—A person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

§ 146c.3. Information security program.

A licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation); and 31 Pa. Code § 146c.10 (relating to determined violation).

§ 146c.4. Objectives of information security program.

A licensee's information security program shall be designed to do the following:

(1) Safeguard the security and confidentiality of customer information.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of the information.

(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation); and 31 Pa. Code § 146c.10 (relating to determined violation).

§ 146c.5. Examples of methods of development and implementation.

The actions and procedures described in §§ 146c.6—146c.9 are examples of methods of implementation of the requirements of §§ 146c.3 and 146c.4 (relat-

ing to information security program; and objectives of information security program). These examples are nonexclusive illustrations of actions and procedures that licensees may follow to implement §§ 146c.3 and 146c.4.

§ 146c.6. Assess risk.

The licensee:

(1) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.

(2) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

(3) Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation).

§ 146c.7. Manage and control risk.

The licensee:

(1) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities.

(2) Trains staff, as appropriate, to implement the licensee's information security program.

(3) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation).

§ 146c.8. Oversee service provider arrangements.

The licensee:

(1) Exercises appropriate due diligence in selecting its service providers.

(2) Requires its service providers to implement appropriate measures designed to meet the objectives of this chapter, and, when indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation).

§ 146c.9. Adjust the program.

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer 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 customer information systems.

Cross References

This section cited in 31 Pa. Code § 146c.5 (relating to examples of methods of development and implementation).

§ 146c.10. Determined violation.

(a) Violations of §§ 146c.3 and 146c.4 (relating to information security program; and objectives of information security program) are deemed and defined by the Commissioner to be an unfair method of competition and an unfair or deceptive act or practice and shall be subject to any applicable penalties or remedies contained in the Unfair Insurance Practices Act (40 P. S. §§ 1171.1—1171.15).

(b) A licensee has violated this chapter when the licensee knew or reasonably should have known of a pattern of activity or a practice of a service provider that constitutes either a violation of Chapter 146a (relating to privacy of consumer financial information), Chapter 146b (relating to privacy of consumer health information) or this chapter or a material breach of the contract or other arrangement between the licensee and the service provider, unless the licensee took reasonable steps to cure the breach or end the violation, as applicable, and, if the steps were unsuccessful, did the following:

(1) Terminated the contract or arrangement with the service provider, if feasible.

(2) If termination is not feasible, reported the violation or breach to the Department.

§ 146c.11. Effective date.

Each licensee shall establish and implement an information security program, including appropriate policies and systems under this chapter by March 1, 2005.

[Next page is 146d-1.]