40 Pa.C.S. § 4502

Pa.C.S. documents are current through 2024 Regular Session Act 13; P.S. documents are current through 2024 Regular Session Act 13

§ 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.

History

Act 2023-2 (H.B. 739), § 1, approved June 14, 2023, effective December 11, 2023.