Md. Insurance Code Ann. § 33-101

Current through all legislation from the 2023 Regular Session of the General Assembly.

Michie's™ Annotated Code of Maryland > Insurance (Titles 1 — 33) > Title 33. Insurance Data Security. (§§ 33-101 — 33-109)

§ 33-101. Definitions.

(a) In this title the following words have the meanings indicated.

(b) "Authorized individual" means an individual:

(1) known to and screened by the carrier; and

(2) for whom the carrier has determined it to be necessary and appropriate that the individual have access to the nonpublic information held by the carrier and its information systems.

(c)

(1) "Carrier" means:

(i) an authorized insurer;

(ii) a nonprofit health service plan;

(iii) a health maintenance organization;

(iv) a dental organization;

(v) a managed general agent; or

(vi) a third-party administrator.

(2) "Carrier" does not include:

(i) a purchasing group or a risk retention group chartered and licensed in a state other than this State; or

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

(d) "Consumer" means an individual, including an applicant, a policyholder, an insured, a beneficiary, a claimant, and a certificate holder, who is a resident of the State and whose nonpublic information is in a carrier's possession, custody, or control.

(e)

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

(2) "Cybersecurity event" 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; or

(ii) an event with regard to which the carrier has reasonably determined that the nonpublic information accessed by an unauthorized person has not been and will not be used or released and has been returned or destroyed.

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

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

(h)

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

(2) "Information system" includes industrial or process control systems, telephone switching and private branch exchange systems, environmental control systems, and other specialized systems.

(i) "Multifactor authentication" means 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 phone; or

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

(j) "Nonpublic information" means information that is not publicly available information and is:

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

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

(i) Social Security number;

(ii) driver's license number or nondriver identification card number;

(iii) account, credit, or debit card number;

(iv) a security code, an access code, or a password that would allow access to a consumer's financial account; or

(v) biometric records; or

(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:

(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 a consumer; or

(iii) payment for the provision of health care to a consumer.

(k) "Publicly available information" means information that a carrier has a reasonable basis to believe is lawfully made available to the general public from:

(1)

(i) federal, State, or local government records;

(ii) widely distributed media; or

(iii) disclosures to the general public that are required to be made by federal, State, or local law; and

(2) steps taken by the carrier to determine:

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

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

(l) "Risk assessment" means the risk assessment that a carrier is required to conduct under § 33-103(c) of this title.

(m) "Third-party service provider" means a person, other than a carrier, that contracts with a carrier to maintain, process, store, or is otherwise authorized access to nonpublic information through its provision of services to the carrier.

History

2022, ch. 231, § 1.

Michie's™ Annotated Code of Maryland
Copyright © 2024 All rights reserved.

End of Document