SPONSOR: Rep. Bush & Rep. Griffith & Sen. Paradee & Sen. Poore
Reps. Baumbach, Dorsey Walker, Dukes, Matthews, Seigfried, Michael Smith; Sens. Pettyjohn, Sokola

HOUSE OF REPRESENTATIVES
150th GENERAL ASSEMBLY

HOUSE BILL NO. 174

AN ACT TO AMEND TITLE 18 OF THE DELAWARE CODE RELATING TO THE INSURANCE DATA SECURITY ACT.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Title 18 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underlining as follows:

Chapter 86. Insurance Data Security Act.

§ 8601. Short title.

This Act is known and may be cited as the "Insurance Data Security Act."

§ 8602. Purpose and intent.

(a) Notwithstanding any other provision of law, this chapter establishes the exclusive state standards for data security and the investigation of, and notification to, the Commissioner and consumers when a cybersecurity event involving a licensee under Title 18 occurs.

(b) This chapter may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this chapter.

§ 8603. Definitions.

As used in this chapter:

(1) "Authorized individual" means an individual to whom a licensee gave authorization to access and use nonpublic information that the licensee and the licensee's information system holds.

(2) "Commissioner" means the Insurance Commissioner of the State of Delaware.

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

(4) "Cybersecurity event" means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on an information system. "Cybersecurity event" does not include either of the following:

LC : HVW : CM
5081500099
Released: 06/03/2019 12:24 PM

23 a. The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is
24 not also acquired, released, or used without authorization.
25 b. An event for which the licensee has determined that the nonpublic information accessed by an
26 unauthorized person has not been used or released and has been returned or destroyed.
27 (5) "Department" means the Department of Insurance.
28 (6) "Encrypted" means the transformation of data into a form which results in a low probability of assigning
29 meaning without the use of a protective process or key.
30 (7) "Information security program" means the administrative, technical, and physical safeguards that a
31 licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle
32 nonpublic information.
33 (8) "Information system" means a discrete set of electronic information resources organized for the collection,
34 processing, maintenance, use, sharing, dissemination, or disposition of electronic information, and a specialized system
35 such as an industrial or process controls system, telephone switching and private branch exchange system, or
36 environmental control system.
37 (9) "Insurer" includes an insurer, health service corporation, managed care organization, or health
38 maintenance organization licensed under Title 18.
39 (10) "Licensee" means a person who is licensed, authorized to operate, or registered, or required to be
40 licensed, authorized, or registered, under the insurance laws of this State. "Licensee" does not mean either of the
41 following:
42 a. A purchasing group or risk retention group that is chartered and licensed in a state other than this State.
43 b. A licensee that is acting as an assuming insurer that is domiciled in a state other than this State or
44 another jurisdiction.
45 (11) "Multi-factor authentication" means authentication through verification of at least 2 of the following
46 types of authentication factors:
47 a. Knowledge factors, such as a password.
48 b. Possession factors, such as a token or text message on a mobile phone.
49 c. Inherence factors, such as a biometric characteristic.
50 (12) "Nonpublic Information" means electronic information that is not publicly-available information and is at
51 least 1 of the following:

52 a. Information concerning a consumer which because of name, number, personal mark, or other identifier
53 can be used to identify the consumer, in combination with any 1 or more of the following data elements:
54 1. Social Security number.
55 2. Driver's license number or non-driver identification card number.
56 3. Financial account number or credit or debit card number.
57 4. A security code, access code, or password that would permit access to a consumer's financial
58 account.
59 5. A biometric record.
60 b, Information or data, except age or gender, in any form or medium created by or derived from a health
61 care provider or consumer that can be used to identify a consumer and relates to any of the following:
62 1. The past, present, or future physical, mental, or behavioral health or condition of a consumer or a
63 member of a consumer's family.
64 2. The provision of health care to a consumer.
65 3. Payment for the provision of health care to a consumer.
66 (13) "Notice", for purposes of the consumer notice required under § 8606(c) of this title, means any of the
67 following:
68 a. Written notice.
69 b. Telephonic notice.
70 c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic
71 signatures and records under 15 U.S.C. § 7001 or if the licensee's primary means of communication with the
72 consumer is by electronic means.
73 1. Substitute notice, if any of the following apply:
74 A. The licensee who is required to provide notice under this chapter demonstrates that the cost of
75 providing notice will exceed $75,000.
76 B. The affected number of consumers to be notified exceeds 100,000.
77 C. The licensee does not have sufficient contact information to provide notice.
78 2. "Substitute notice" means all of the following:
79 A. Electronic notice, if the licensee has an email address for the affected consumer.
80 B. Conspicuous posting of the notice on the licensee's website page, if the licensee maintains 1
81 or more website pages.

82 C. Notice to major statewide media, including newspapers, radio, and television.

83 D. Publication on the major social media platforms of the licensee who is providing notice.

84 (14) "Person" means as defined in § 102 of this title.

85 (15)a. "Publicly-available information" means information that a licensee has a reasonable basis to believe is

86 lawfully made available to the general public, including any of the following:

87 1. A federal, state, or local government record.

88 2. A widely-distributed information source or media.

89 3. A disclosure to the general public that is required under federal, state, or local law.

90 b. For purposes of this definition, "reasonable basis to believe that information is lawfully made available

91 to the general public" means a licensee has taken steps and determined all of the following:

92 1. That the information is of the type that is available to the general public.

93 2. If a consumer can direct that the information may not be made available to the general public, the

94 consumer has not done so.

95 (16) "Risk assessment" means the action that a licensee is required to take under § 8604(c) of this title.

96 (17) "State", if capitalized, means the State of Delaware.

97 (18) "Third-party service provider" means a person who is not a licensee and who contracts with a licensee to

98 maintain, process, store, or otherwise is permitted access to nonpublic information through the person's provision of

99 services to the licensee.

100 § 8604. Information security program.

101 (a) Implementation of an information security program.

102 (1) A licensee shall develop, implement, and maintain a comprehensive, written information security program

103 that is based on the licensee's risk assessment and contains administrative, technical, and physical safeguards for the

104 protection of nonpublic information and the licensee's information system.

105 (2) An information security program under this section must be commensurate with the size and complexity of

106 a licensee; the nature and scope of a licensee's activities, including the licensee's use of a third-party service provider;

107 and the sensitivity of the nonpublic information that the licensee uses or has in the licensee's possession, custody, or

108 control.

109 (b) Objectives of information security program. A licensee's information security program must be designed to do

110 all of the following:

111 (1) Protect the security and confidentiality of nonpublic information and the security of the information
112 system.
113 (2) Protect against threats or hazards to the security or integrity of nonpublic information and the information
114 system.
115 (3) Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of
116 harm to a consumer.
117 (4) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for
118 its destruction when retention of the nonpublic information is no longer needed.
119 (c) Risk assessment. A licensee shall do all of the following:
120 (1) Designate 1 or more employees, an affiliate, or an outside vendor designated to act on the licensee's behalf
121 and be responsible for managing and overseeing the information security program.
122 (2) Identify reasonably-foreseeable internal or external threats that could result in unauthorized access,
123 transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of an
124 information system or nonpublic information that a third-party service provider has access to or holds.
125 (3) Assess the likelihood and potential damage of a threat identified under paragraph (c)(2) of this section,
126 taking into consideration the sensitivity of the nonpublic information.
127 (4) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to
128 manage a threat identified under paragraph (c)(2) of this section, including consideration of threats in each relevant
129 area of the licensee's operations, including all of the following:
130 a. Employee training and management.
131 b. An information system, including network and software design and information classification,
132 governance, processing, storage, transmission, and disposal.
133 c. Detecting, preventing, and responding to an attack, intrusion, or other system failure.
134 (5) Implement information safeguards to manage the threats identified in the licensee's ongoing assessment
135 under paragraph (c)(2) of this section and, at least annually, assess the effectiveness of the safeguards' key controls,
136 systems, and procedures.
137 (d) Risk management. Based on a licensee's risk assessment, the licensee shall do all of the following:
138 (1) Design an information security program to mitigate the identified risks, commensurate with all of the
139 following:
140 a. The licensee's size and complexity.

141 b. The nature and scope of the licensee's activities, including the licensee's use of a third-party service
142 provider.
143 c. The sensitivity of the nonpublic information that the licensee uses or has in the licensee's possession,
144 custody, or control.
145 (2) Determine if a security measure listed in paragraphs (d)(2)a. through k. of this section is appropriate and
146 implement each appropriate security measure.
147 a. Place an access control on an information system, including a control to authenticate and permit access
148 only to an authorized individual to protect against the unauthorized acquisition of nonpublic information.
149 b. Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to
150 achieve business purposes in accordance with their relative importance to business objectives and the
151 organization's risk strategy.
152 c. Restrict physical access to nonpublic information to authorized individuals only.
153 d. Protect by encryption or other appropriate means all nonpublic information while the nonpublic
154 information is transmitted over an external network and all nonpublic information stored on a laptop computer or
155 other portable computing or storage device or media.
156 e. Adopt both of the following:
157 1. Secure development practices for an application that a licensee uses and was developed in-house.
158 2. Procedures for evaluating, assessing, or testing the security of an application that a licensee uses
159 and was developed externally.
160 f. Modify the information system in accordance with the licensee's information security program.
161 g. Utilize effective controls, which may include multi-factor authentication procedures for employees or
162 authorized individuals accessing nonpublic information.
163 h. Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or
164 intrusions, into an information system.
165 i. Include audit controls within the information security program designed to do both of the following:
166 1. Detect and respond to a cybersecurity event.
167 2. Reconstruct material financial transactions sufficient to support the licensee's normal operations
168 and obligations.
169 j. Implement measures to protect against the destruction, loss, or damage of nonpublic information due to
170 environmental hazards, such as fire and water damage, other catastrophes, or technological failures.

171 k. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any
172 format.
173 (3) Include cybersecurity risks in the licensee's enterprise risk management process.
174 (4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when
175 sharing information relative to the character of the sharing and the type of information shared.
176 (5) Provide the licensee's personnel with cybersecurity awareness training that is updated as necessary to
177 reflect risks that the licensee identified in the licensee's risk assessment under this section.
178 (e) Oversight by board of directors. If a licensee has a board of directors, the board or an appropriate committee of
179 the board shall, at a minimum, do all of the following:
180 (1) Require the licensee's executive management or its delegates to develop, implement, and maintain the
181 licensee's information security program.
182 (2) Require the licensee's executive management or its delegates to report in writing at least annually all of
183 the following information:
184 a. The overall status of the information security program and the licensee's compliance with this chapter.
185 b. Material matters related to the information security program, including addressing issues such as the
186 following:
187 1. Risk assessment, risk management, and control decisions.
188 2. Third-party service provider arrangements.
189 3. Results of testing.
190 4. Cybersecurity events or violations and management's responses to the events.
191 5. Recommendations for changes in the information security program.
192 (3) If executive management delegates any of its responsibilities under § 8604 of this title, all of the following
193 must occur:
194 a. Executive management shall oversee the development, implementation, and maintenance of the
195 licensee's information security program that the delegate prepares.
196 b. The delegate shall submit to executive management a report that complies with the requirements of the
197 report to the board of directors under paragraph (e)(2) of this section.
198 (f) Oversight of third-party service provider arrangements.
199 (1) A licensee shall exercise due diligence in selecting a third-party service provider.

200 (2) A licensee shall require a third-party service provider to implement appropriate administrative, technical,
201 and physical measures to protect and secure the information system and nonpublic information that the third-party
202 service provider has access to or holds. The third-party service provider is not considered to have access to or hold
203 encrypted nonpublic information for purposes of this section if the associated protective process or key necessary to
204 assign meaning to the nonpublic information is not within the third-party service provider's possession.
205 (g) Program adjustments. A licensee shall monitor, evaluate, and adjust as appropriate the information security
206 program consistent with all of the following:
207 (1) Relevant changes in technology.
208 (2) The sensitivity of the licensee's nonpublic information.
209 (3) Internal or external threats to information.
210 (4) The licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint
211 ventures, outsourcing arrangements, and changes to information systems.
212 (h) Incident response plan.
213 (1) As part of a licensee's information security program, the licensee shall establish a written incident
214 response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises the
215 confidentiality, integrity, or availability of any of the following:
216 a. Nonpublic information in the licensee's possession.
217 b. The licensee's information system.
218 c. The continuing functionality of any aspect of the licensee's business or operations.
219 (2) An incident response plan under this section must address all of the following areas:
220 a. The internal process for responding to a cybersecurity event.
221 b. The goals of the incident response plan.
222 c. The definition of clear roles, responsibilities, and levels of decision-making authority.
223 d. External and internal communications and information sharing.
224 e. Identification of requirements for the remediation of any identified weaknesses in an information
225 system and associated controls.
226 f. Documentation and reporting regarding cybersecurity events and related incident response activities.
227 g. As necessary, the evaluation and revision of the incident response plan following a cybersecurity event.
228 (i) Annual certification to the Commissioner of Domiciliary State. An insurer domiciled in this State shall do all of
229 the following:

230 (1) Submit annually to the Commissioner a written statement by February 15, certifying that the insurer is in
231 compliance with the requirements under in this section.
232 (2) Maintain for the Department's examination all records, schedules, and data supporting a certificate under
233 this paragraph (i) of this section for a period of 5 years.
234 (3) To the extent an insurer has identified an area, system, or process that requires material improvement,
235 updating, or redesign, document the identification and the remedial effort planned and underway to address the
236 identified area, system, or process. Documentation under this paragraph (i)(3) of this section must be available for the
237 Commissioner's inspection.
238 § 8605. Investigation of a cybersecurity event.
239 (a) If a licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or
240 service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.
241 (b) During an investigation under this section, the licensee, or an outside vendor or service provider designated to
242 act on behalf of the licensee, shall, at a minimum, do as much of the following as possible:
243 (1) Determine whether a cybersecurity event has occurred.
244 (2) Assess the nature and scope of the cybersecurity event.
245 (3) Identify the nonpublic information that may have been involved in the cybersecurity event.
246 (4) Perform or oversee reasonable measures to restore the security of the information system compromised in
247 the cybersecurity event to prevent further unauthorized acquisition, release, or use of nonpublic information that is in
248 the licensee's possession, custody, or control.
249 (c) If a licensee provides nonpublic information to a third-party service provider and learns that a cybersecurity
250 event has or may have occurred in a system that the third-party service provider maintains, the licensee shall complete the
251 steps listed in § 8605(b) of this title or make reasonable efforts to confirm and document that the third-party service
252 provider has completed the steps.
253 (d) A licensee shall maintain records concerning a cybersecurity event for a period of at least 5 years from the date
254 of the cybersecurity event and shall produce those records upon the Commissioner's demand.
255 § 8606. Notification of a cybersecurity event.
256 (a) Notification to the commissioner. A licensee shall notify the Commissioner as promptly as possible but in no
257 event later than 3 business days from the licensee's determination that a cybersecurity event has occurred if either of the
258 following criteria has been met:

259 (1) The licensee is an insurer who is domiciled in this State or a producer whose home state is this State, as
260 "home state" is defined under Chapter 17 of this title, and the cybersecurity event results in any of the following:
261 a. A reasonable likelihood of materially harming a consumer.
262 b. A reasonable likelihood of materially harming any material part of the licensee's normal operation.
263 c. The licensee is required to provide notice of the cybersecurity event to a government body, self-
264 regulatory agency, or other supervisory body under state or federal law.
265 (2) The licensee reasonably believes that the nonpublic information involved is regarding 250 or more
266 consumers and either of the following apply:
267 a. The cybersecurity event impacts a licensee that is required to provide notice to a government body,
268 self-regulatory agency, or other supervisory body under state or federal law.
269 b. The cybersecurity event has a reasonable likelihood of materially harming either of the following:
270 1. A consumer.
271 2. A material part of the licensee's normal operations.
272 (b) Notice requirements.
273 (1)a. If notice to the Commissioner is required under subsection (a) of this section, a licensee shall provide the
274 information in a form as directed by the Commissioner.
275 b. A licensee has a continuing obligation to update and supplement initial and subsequent notifications to
276 the Commissioner regarding material changes to previously-provided information relating to a cybersecurity event.
277 (2) A licensee shall provide as much of the following information as possible:
278 a. Date of the cybersecurity event.
279 b. Description of how the information was exposed, lost, stolen, or breached, including the specific role
280 and responsibility of a third-party service provider, if any.
281 c. How the cybersecurity event was discovered.
282 d. Whether any lost, stolen, or breached information has been recovered and, if so, how it was lost, stolen,
283 or breached.
284 e. The identity of the source of the cybersecurity event.
285 f. Whether the licensee has filed a police report or notified a regulatory, government, or law enforcement
286 agency and, if so, when the notification was provided.

287 g. Description of the specific types of information acquired without authorization. For the purposes of this
288 paragraph (b)(2)g. of this section, "specific types of information" means particular data elements, including
289 medical information, financial information, or information allowing identification of a consumer.
290 h. The period during which the cybersecurity event compromised the information system.
291 i. The number of total consumers in this State who are affected by the cybersecurity event. The licensee
292 shall provide the best estimate in the initial report to the Commissioner and update the estimate with each
293 subsequent report to the Commissioner under this section.
294 j. The results of an internal review identifying a lapse in either automated controls or internal procedures,
295 or confirming that the automated controls or internal procedures were followed.
296 k. Description of efforts being undertaken to remediate the situation which permitted the cybersecurity
297 event to occur.
298 *l.* A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to
299 investigate and notify a consumer affected by a cybersecurity event.
300 m. The name of a contact person who is both familiar with the cybersecurity event and authorized to act
301 for the licensee.
302 (c) Notification to consumers. If a licensee determines that a cybersecurity event that has a reasonable likelihood
303 of materially harming a consumer has occurred and the event is 1 for which the licensee is required under subsection (a) of
304 this section to notify the Commissioner, the licensee shall provide notice of the event to each affected consumer and
305 provide a copy of the notice to the Commissioner.
306 (1) A licensee must provide notice under this subsection (c) of this section without unreasonable delay but no
307 later than 60 days after determining that a cybersecurity event occurred, unless any of the following apply:
308 a. Federal law requires a shorter time period.
309 b. A law-enforcement agency determines that the notice will impede a criminal investigation and the law-
310 enforcement agency has requested that the licensee delay notice. Delayed notice must be made after the law-
311 enforcement agency determines, and notifies the licensee, that notice will not compromise the criminal
312 investigation.
313 c. If a licensee that is otherwise required by this section to provide notice could not, through reasonable
314 diligence, identify within 60 days of a cybersecurity event that a customer's nonpublic information was included in
315 the event, the licensee must provide the notice required under this section to the consumer as soon as practicable

316 after the identification, unless the licensee provides or has provided substitute notice under § 8603(m)(4) of this
317 title.
318 (2) If a cybersecurity event includes a Social Security number, a licensee shall offer to each consumer whose
319 nonpublic information, including Social Security number, was breached or is reasonably believed to have been
320 breached, credit monitoring services at no cost to the consumer for a period of 1 year.
321 a. The licensee shall provide all information necessary for the consumer to enroll in credit monitoring
322 services and include information on how the consumer can place a credit freeze on the consumer's credit file.
323 b. Credit monitoring services are not required if, after an appropriate investigation, the licensee
324 reasonably determines that the cybersecurity event is unlikely to result in harm to the consumer whose nonpublic
325 information has been breached.
326 (3) If a cybersecurity event consists of a breach of email account login credentials that the licensee furnished
327 to the consumer, including a username or email address and in combination with a password or security question and
328 answer that permit access to an online account, the licensee may not provide notice under this section via the involved
329 email address. The licensee must instead provide notice under this section through another method under § 8603(m) of
330 this title or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the
331 online account from an internet protocol address or online location from which the licensee knows the consumer
332 customarily accesses the account.
333 (d) Notice regarding cybersecurity events of third-party service providers.
334 (1) If a cybersecurity event occurs in a system that a third-party service provider maintains and of which a
335 licensee has become aware, the licensee shall treat the event as it would under subsection (a) of this section unless the
336 third-party service provider provides the notice to the Commissioner under § 8606 of this title.
337 (2) The computation of a licensee's deadline under this section begins on the first business day after the third-
338 party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of
339 the cybersecurity event, whichever is sooner.
340 (3) Nothing in this chapter prevents or abrogates an agreement between a licensee and another licensee, a
341 third-party service provider, or another party to fulfill the investigation requirements under § 8605 of this title or notice
342 requirements under this section.
343 (e) Notice regarding cybersecurity events of reinsurers to insurers.
344 (1) If a cybersecurity event involves nonpublic information that is used by a licensee who is acting as an
345 assuming insurer, or the nonpublic information is in the possession, custody, or control of a licensee who is acting as

346 an assuming insurer and does not have a direct contractual relationship with the affected consumer, the licensee who is
347 acting as an assuming insurer shall notify its affected ceding insurers and the Commissioner of the licensee who is
348 acting as an assuming insurer's state of domicile within 3 business days of determining that a cybersecurity event has
349 occurred. A ceding insurer who has a direct contractual relationship with an affected consumer shall fulfill the
350 consumer notification requirements under subsection (c) of this section and any other notification requirement under
351 this section relating to a cybersecurity event.
352 (2) If a cybersecurity event involves nonpublic information that is in the possession, custody, or control of a
353 third-party service provider of a licensee who is acting as an assuming insurer, the licensee who is acting as an
354 assuming insurer shall notify the affected ceding insurer and the Commissioner of the licensee who is acting as an
355 assuming insurer's state of domicile within 3 business days of receiving notice from the licensee who is acting as an
356 assuming insurer's third-party service provider that a cybersecurity event has occurred. A ceding insurer that has a
357 direct contractual relationship with an affected consumer shall fulfill the consumer notification requirements under
358 subsection (c) of this section and any other notification requirement under this section relating to a cybersecurity event.
359 (f) Notice regarding cybersecurity events of insurers to producers of record. If a cybersecurity event for which
360 consumer notice is required under this section involves nonpublic information that is in the possession, custody, or control
361 of a licensee who is an insurer, or a licensee's third-party service provider and for which a consumer accessed the insurer's
362 services through an independent insurance producer, the licensee shall notify the producers of record of the consumer who
363 was affected by the cybersecurity event in a reasonable manner and at a time reasonably concurrent with the time at which
364 notice is provided to the affected consumer. The insurer is excused from this obligation for a producer who is not
365 authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in an instance in which the insurer
366 does not have the current producer of record information for the consumer.
367 § 8607. Power of Commissioner.
368 (a) The Commissioner may examine and investigate the affairs of a licensee to determine whether the licensee has
369 been or is engaged in any conduct in violation of this chapter. The Commissioner's power under this section is in addition
370 to the powers the Commissioner has under § 318 of this title. An examination or investigation must be conducted under
371 § 320 through § 322 of this title.
372 (b) If the Commissioner has reason to believe that a licensee has been or is engaged in conduct in this State that
373 violates this chapter, the Commissioner may take necessary or appropriate action to enforce the provisions of this chapter.

374 § 8608. Confidentiality.

375 (a)(1) Documents, materials, or other information in the Department's control or possession that a licensee or
376 employee or agent acting on behalf of a licensee furnished under § 8604(i) or § 8606(b)(2)b., (b)(2)c., (b)(c)d., (b)(2)e.,
377 (b)(2)h., (b)(2)j., or (b)(2)k. of this title, or that the Commissioner obtained in an examination or investigation under § 8607
378 of this title are confidential and privileged, and are not subject to any of the following:

379 a. The Freedom of Information Act, Chapter 100 of Title 29.

380 b. Subpoena.

381 c. Discovery or admissible in evidence in any private civil action.

382 (2) Notwithstanding paragraph (a)(1) of this section, the Commissioner may use documents, materials, or
383 other information listed in paragraph (a)(1) of this section in the furtherance of a regulatory or legal action brought as a
384 part of the Commissioner's duties.

385 (b) Neither the Commissioner nor a person who received a document, materials, or other information listed in
386 paragraph (a)(1) of this section while acting under the Commissioner's authority is permitted or required to testify in a
387 private civil action concerning the confidential document, materials, or information.

388 (c) In order to assist in the performance of the Commissioner's duties under this chapter, the Commissioner may
389 do any of the following:

390 (1) Share documents, materials, or other information, including a confidential and privileged documents,
391 materials, or information subject to subsection (a) of this section, with another state, federal, or international regulatory
392 agency; the National Association of Insurance Commissioners and its affiliates or subsidiaries; and a state, federal, and
393 international law-enforcement authority, if the recipient agrees in writing to maintain the confidentiality and privileged
394 status of the document, material, or other information.

395 (2) May receive documents, materials, or information, including otherwise confidential and privileged
396 documents, materials, or information from the National Association of Insurance Commissioners or its affiliates or
397 subsidiaries and from a regulatory or law-enforcement official of another foreign or domestic jurisdictions. The
398 Commissioner shall maintain as confidential or privileged documents, materials, or information received with notice or
399 the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the
400 documents, materials, or information.

401 (3) Share documents, materials, or other information subject to subsection (a) of this section with a third-party
402 consultant or vendor, if the consultant agrees in writing to maintain the confidentiality and privileged status of the
403 documents, materials, or other information.

404 (4) Enter into an agreement governing the sharing and use of information consistent with this subsection.

405 (d) A waiver of an applicable privilege or claim of confidentiality in documents, materials, or information may not
406 occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in subsection
407 (c) of this section.

408 (e) Nothing in this chapter prohibits the Commissioner from releasing final, adjudicated actions that are open to
409 public inspection under the Delaware Freedom of Information Act, Chapter 100 of Title 29 to a database or other
410 clearinghouse service that the National Association of Insurance Commissioners or its affiliates or subsidiaries maintains.

411 (f) Documents, materials, or other information that the National Association of Insurance Commissioners or a
412 third-party consultant or vendor possess or controls under this chapter is confidential by law and privileged, is not subject to
413 the Delaware Freedom of Information Act, Chapter 100 of Title 29, is not subject to subpoena, and is not subject to
414 discovery or admissible in evidence in a private civil action.

415 § 8609. Exceptions.

416 (a) The following exceptions apply to this chapter:

417 (1) A licensee with fewer than 15 employees is exempt from § 8604 of this chapter.

418 (2) A licensee subject to the Health Insurance Portability and Accountability Act [P.L. 104-191, as amended]
419 that has established and maintains an information security program under the statutes, rules, regulations, procedures, or
420 guidelines established thereunder, is considered to meet the requirements of § 8604 of this title, if the licensee is
421 compliant with, and submits a written statement certifying its compliance, the same.

422 (3) A licensee's employee, agent, representative, or designee, who is also a licensee, is exempt from § 8604
423 of this title and is not required to develop the employee's, agent's, representative's, or designee's own information
424 security program to the extent that the employee, agent, representative or designee is covered by the other licensee's
425 information security program.

426 (b) Nothing in this chapter creates a duty or liability for a provider of communication services for the transmission
427 of voice, data, or other information over its network.

428 (c) If a licensee ceases to qualify for an exception under this section, the licensee has 180 days to comply with this
429 chapter.

430 § 8610. Penalties. If I licensee violates this chapter, the licensee may be subject to penalties under § 329 of this
431 title.

432 § 8611. Regulations.

433 The Commissioner may, in accordance with § 311 of this title, promulgate regulations necessary to carry out the

434 provisions of this chapter.

435 Section 2. Effective Date. This Act takes effect upon enactment. A licensee under this chapter has 1 year from [the

436 effective date of this Act] to implement § 8604 of this title and 2 years from [the effective date of this Act] to implement

437 § 8604(f) of this title.

SYNOPSIS

This Act establishes standards for data security for Title 18 licensees and standards for the investigation of and notification to the Commissioner of a cybersecurity event affecting Title 18 licensees.