

SENATE BILL 207

J5, S2

2lr0014

(PRE-FILED)

By: **Chair, Finance Committee (By Request – Departmental – Maryland Insurance Administration)**

Requested: October 4, 2021

Introduced and read first time: January 12, 2022

Assigned to: Finance

A BILL ENTITLED

1 AN ACT concerning

2 **Insurance Carriers – Cybersecurity Standards**

3 FOR the purpose of establishing certain cybersecurity standards applicable to insurance
4 carriers, including health maintenance organizations and third-party
5 administrators; requiring a carrier to take certain actions related to cybersecurity,
6 including developing, implementing, and maintaining a certain information security
7 program, identifying certain threats, and establishing a certain incident response
8 plan; requiring a carrier, under certain circumstances, to notify the Maryland
9 Insurance Commissioner that a cybersecurity event has occurred; establishing that
10 certain documents, materials, and information are confidential and privileged, not
11 subject to the Maryland Public Information Act, subpoena, and discovery, and not
12 admissible as evidence in certain actions; prohibiting certain persons from being
13 allowed or required to testify in certain proceedings; requiring the Commissioner to
14 maintain as confidential or privileged certain documents, materials, and
15 information; and generally relating to insurance carriers and the security of
16 information.

17 BY adding to
18 Article – Health – General
19 Section 19–706(p) and 19–729(a)(13)
20 Annotated Code of Maryland
21 (2019 Replacement Volume and 2021 Supplement)

22 BY repealing and reenacting, with amendments,
23 Article – Health – General
24 Section 19–729(a)(11) and (12)
25 Annotated Code of Maryland
26 (2019 Replacement Volume and 2021 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



BY repealing and reenacting, without amendments,
Article – Health – General
Section 19–729(b)
Annotated Code of Maryland
(2019 Replacement Volume and 2021 Supplement)

BY repealing
Article – Insurance
Section 4–406
Annotated Code of Maryland
(2017 Replacement Volume and 2021 Supplement)

BY adding to
Article – Insurance
Section 8–321.2; and 33–101 through 33–108 to be under the new title “Title 33.
Insurance Data Security”
Annotated Code of Maryland
(2017 Replacement Volume and 2021 Supplement)

BY repealing and reenacting, with amendments,
Article – Insurance
Section 14–102(g)
Annotated Code of Maryland
(2017 Replacement Volume and 2021 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,
That the Laws of Maryland read as follows:

Article – Health – General

19–706.

**(P) THE PROVISIONS OF TITLE 33 OF THE INSURANCE ARTICLE APPLY TO
HEALTH MAINTENANCE ORGANIZATIONS.**

19–729.

(a) A health maintenance organization may not:

(11) Fail to comply with the provisions of Title 15, Subtitle 10A, 10B, 10C,
or 10D or § 2–112.2 of the Insurance Article; [or]

(12) Violate any provision of § 19–712.5 of this subtitle; **OR**

**(13) VIOLATE ANY PROVISION OF TITLE 33 OF THE INSURANCE
ARTICLE.**

(b) If any health maintenance organization violates this section, the Commissioner may pursue any one or more of the courses of action described in § 19–730 of this subtitle.

Article – Insurance

[4–406.

(a) (1) In this section the following words have the meanings indicated.

(2) “Breach of the security of a system” has the meaning stated in § 14–3504 of the Commercial Law Article.

(3) “Carrier” means:

- (i) an insurer;
- (ii) a nonprofit health service plan;
- (iii) a health maintenance organization;
- (iv) a dental organization;
- (v) a managed care organization;
- (vi) a managed general agent; and
- (vii) a third party administrator.

(4) “Personal information” has the meaning stated in § 14–3501 of the Commercial Law Article.

(b) (1) A carrier shall notify the Commissioner on a form and in a manner approved by the Commissioner that a breach of the security of a system has occurred if the carrier:

- (i) conducts an investigation required under § 14–3504(b) or (c) of the Commercial Law Article; and
- (ii) determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused.

(2) The carrier shall provide the notice required under paragraph (1) of this subsection at the same time the carrier provides notice to the Office of the Attorney General under § 14–3504(h) of the Commercial Law Article.

(c) Compliance with this section does not relieve a carrier from a duty to comply with any other requirements of federal law or Title 14 of the Commercial Law Article relating to the protection and privacy of personal information.]

8–321.2.

A THIRD-PARTY ADMINISTRATOR SHALL COMPLY WITH TITLE 33 OF THIS ARTICLE.

14–102.

(g) A corporation without capital stock organized for the purpose of establishing, maintaining, and operating a nonprofit health service plan through which health care providers provide health care services to subscribers to the plan under contracts that entitle each subscriber to certain health care services shall be governed and regulated by:

(1) this subtitle;

(2) Title 2, Subtitle 2 of this article and §§ 1–206, 3–127, and 12–210 of this article;

(3) Title 2, Subtitle 5 of this article;

(4) §§ 4–113, 4–114, [4–406,] and 4–503 of this article;

(5) Title 5, Subtitles 1, 2, 3, 4, and 5 of this article;

(6) Title 7 of this article, except for § 7–706 and Subtitle 2 of Title 7;

(7) Title 9, Subtitles 1, 2, and 4 of this article;

(8) Title 10, Subtitle 1 of this article;

(9) Title 27 of this article; [and]

(10) TITLE 33 OF THIS ARTICLE; AND

[(10)] (11) any other provision of this article that:

(i) is expressly referred to in this subtitle;

(ii) expressly refers to this subtitle; or

(iii) expressly refers to nonprofit health service plans or persons subject to this subtitle.

TITLE 33. INSURANCE DATA SECURITY.**33-101.**

(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) “CARRIER” MEANS:

(1) AN INSURER;

(2) A NONPROFIT HEALTH SERVICE PLAN;

(3) A HEALTH MAINTENANCE ORGANIZATION;

(4) A DENTAL ORGANIZATION;

(5) A MANAGED CARE ORGANIZATION;

(6) A MANAGED GENERAL AGENT; AND

(7) A THIRD-PARTY ADMINISTRATOR.

(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 INFORMATION STORED ON AN INFORMATION SYSTEM.

(2) “CYBERSECURITY EVENT” DOES NOT INCLUDE:

(I) THE UNAUTHORIZED ACQUISITION OF ENCRYPTED

1 NONPUBLIC INFORMATION IF THE ENCRYPTION, PROCESS, OR KEY IS NOT ALSO
2 ACQUIRED, RELEASED, OR USED WITHOUT AUTHORIZATION; OR

3 (II) AN EVENT WITH REGARD TO WHICH THE CARRIER HAS
4 DETERMINED THAT THE NONPUBLIC INFORMATION ACCESSED BY AN
5 UNAUTHORIZED PERSON HAS NOT BEEN USED OR RELEASED AND HAS BEEN
6 RETURNED OR DESTROYED.

7 (F) "ENCRYPTED" MEANS THE TRANSFORMATION OF DATA INTO A FORM
8 WHICH RESULTS IN A LOW PROBABILITY OF ASSIGNING MEANING WITHOUT THE USE
9 OF A PROTECTIVE PROCESS OR KEY.

10 (G) "INFORMATION SECURITY PROGRAM" MEANS THE ADMINISTRATIVE,
11 TECHNICAL, AND PHYSICAL SAFEGUARDS THAT A CARRIER USES TO ACCESS,
12 COLLECT, DISTRIBUTE, PROCESS, PROTECT, STORE, USE, TRANSMIT, DISPOSE OF,
13 OR OTHERWISE HANDLE NONPUBLIC INFORMATION.

14 (H) (1) "INFORMATION SYSTEM" MEANS A DISCRETE SET OF ELECTRONIC
15 INFORMATION RESOURCES ORGANIZED FOR THE COLLECTION, PROCESSING,
16 MAINTENANCE, USE, SHARING, DISSEMINATION, OR DISPOSITION OF ELECTRONIC
17 INFORMATION.

18 (2) "INFORMATION SYSTEM" INCLUDES INDUSTRIAL OR PROCESS
19 CONTROL SYSTEMS, TELEPHONE SWITCHING AND PRIVATE BRANCH EXCHANGE
20 SYSTEMS, ENVIRONMENTAL CONTROL SYSTEMS, AND OTHER SPECIALIZED
21 SYSTEMS.

22 (I) "MULTIFACTOR AUTHENTICATION" MEANS AUTHENTICATION
23 THROUGH VERIFICATION OF AT LEAST TWO OF THE FOLLOWING TYPES OF
24 AUTHENTICATION FACTORS:

25 (1) KNOWLEDGE FACTORS, SUCH AS A PASSWORD;

26 (2) POSSESSION FACTORS, SUCH AS A TOKEN OR TEXT MESSAGE ON A
27 MOBILE PHONE; OR

28 (3) INHERENCE FACTORS, SUCH AS A BIOMETRIC CHARACTERISTIC.

29 (J) "NONPUBLIC INFORMATION" MEANS INFORMATION THAT IS NOT
30 PUBLICLY AVAILABLE INFORMATION AND IS:

31 (1) BUSINESS-RELATED INFORMATION OF A CARRIER THE
32 TAMPERING WITH WHICH, OR UNAUTHORIZED DISCLOSURE, ACCESS, OR USE OF

1 WHICH, WOULD CAUSE A MATERIAL ADVERSE IMPACT TO THE BUSINESS,
2 OPERATIONS, OR SECURITY OF THE CARRIER;

3 (2) INFORMATION CONCERNING A CONSUMER THAT, BECAUSE OF
4 NAME, NUMBER, PERSONAL MARK, OR OTHER IDENTIFIER, CAN BE USED TO
5 IDENTIFY THE CONSUMER, IN COMBINATION WITH ONE OR MORE OF THE
6 FOLLOWING DATA ELEMENTS:

7 (I) SOCIAL SECURITY NUMBER;

8 (II) DRIVER'S LICENSE NUMBER OR NONDRIVER
9 IDENTIFICATION CARD NUMBER;

10 (III) ACCOUNT, CREDIT, OR DEBIT CARD NUMBER;

11 (IV) A SECURITY CODE, AN ACCESS CODE, OR A PASSWORD THAT
12 WOULD ALLOW ACCESS TO A CONSUMER'S FINANCIAL ACCOUNT; OR

13 (V) BIOMETRIC RECORDS; OR

14 (3) INFORMATION OR DATA, EXCEPT AGE OR GENDER, IN ANY FORM
15 OR MEDIUM CREATED BY OR DERIVED FROM A HEALTH CARE PROVIDER OR A
16 CONSUMER THAT RELATES TO:

17 (I) THE PAST, PRESENT, OR FUTURE PHYSICAL, MENTAL, OR
18 BEHAVIORAL HEALTH OR CONDITION OF A CONSUMER OR A MEMBER OF THE
19 CONSUMER'S FAMILY;

20 (II) THE PROVISION OF HEALTH CARE TO A CONSUMER; OR

21 (III) PAYMENT FOR THE PROVISION OF HEALTH CARE TO A
22 CONSUMER.

23 (K) "PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT A
24 CARRIER HAS A REASONABLE BASIS TO BELIEVE IS LAWFULLY MADE AVAILABLE TO
25 THE GENERAL PUBLIC FROM:

26 (1) (I) FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS;

27 (II) WIDELY DISTRIBUTED MEDIA; OR

28 (III) DISCLOSURES TO THE GENERAL PUBLIC THAT ARE
29 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 OTHERWISE ACCESS NONPUBLIC INFORMATION THROUGH ITS PROVISION OF SERVICES TO THE CARRIER.

33–102.

(A) THE PURPOSE OF THIS TITLE IS TO ESTABLISH STANDARDS FOR:

(1) DATA SECURITY; AND

(2) THE INVESTIGATION OF AND NOTIFICATION TO THE COMMISSIONER OF A CYBERSECURITY EVENT APPLICABLE TO CARRIERS.

(B) THIS TITLE MAY NOT BE CONSTRUED TO:

(1) CREATE OR IMPLY A PRIVATE CAUSE OF ACTION FOR VIOLATION OF ITS PROVISIONS; OR

(2) CURTAIL A PRIVATE CAUSE OF ACTION WHICH WOULD OTHERWISE EXIST IN THE ABSENCE OF THIS TITLE.

33–103.

(A) (1) EACH CARRIER SHALL DEVELOP, IMPLEMENT, AND MAINTAIN A COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM BASED ON THE CARRIER’S RISK ASSESSMENT.

(2) THE INFORMATION SECURITY PROGRAM SHALL CONTAIN ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS FOR THE PROTECTION

1 OF NONPUBLIC INFORMATION AND THE CARRIER'S INFORMATION SYSTEM.

2 (3) A CARRIER'S INFORMATION SECURITY PROGRAM SHALL BE
3 COMMENSURATE WITH:

4 (I) THE SIZE AND COMPLEXITY OF THE CARRIER;

5 (II) THE NATURE AND SCOPE OF THE CARRIER'S ACTIVITIES,
6 INCLUDING ITS USE OF THIRD-PARTY SERVICE PROVIDERS; AND

7 (III) THE SENSITIVITY OF THE NONPUBLIC INFORMATION USED
8 BY THE CARRIER OR IN THE CARRIER'S POSSESSION, CUSTODY, OR CONTROL.

9 (B) A CARRIER'S INFORMATION SECURITY PROGRAM SHALL BE DESIGNED
10 TO:

11 (1) PROTECT THE SECURITY AND CONFIDENTIALITY OF NONPUBLIC
12 INFORMATION AND THE SECURITY OF THE INFORMATION SYSTEM;

13 (2) PROTECT AGAINST THREATS OR HAZARDS TO THE SECURITY OR
14 INTEGRITY OF NONPUBLIC INFORMATION AND THE INFORMATION SYSTEM;

15 (3) PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF
16 NONPUBLIC INFORMATION AND MINIMIZE THE LIKELIHOOD OF HARM TO A
17 CONSUMER; AND

18 (4) DEFINE AND PERIODICALLY REEVALUATE A SCHEDULE FOR
19 RETENTION OF NONPUBLIC INFORMATION AND A MECHANISM FOR ITS
20 DESTRUCTION WHEN NO LONGER NEEDED.

21 (C) EACH CARRIER SHALL:

22 (1) DESIGNATE ONE OR MORE EMPLOYEES, AN AFFILIATE, OR AN
23 OUTSIDE VENDOR DESIGNATED TO ACT ON BEHALF OF THE CARRIER WHO IS
24 RESPONSIBLE FOR THE INFORMATION SECURITY PROGRAM;

25 (2) IDENTIFY REASONABLY FORESEEABLE INTERNAL OR EXTERNAL
26 THREATS THAT COULD RESULT IN UNAUTHORIZED ACCESS, TRANSMISSION,
27 DISCLOSURE, MISUSE, ALTERATION, OR DESTRUCTION OF NONPUBLIC
28 INFORMATION, INCLUDING THE SECURITY OF INFORMATION SYSTEMS AND
29 NONPUBLIC INFORMATION THAT ARE ACCESSIBLE TO, OR HELD BY, THIRD-PARTY
30 SERVICE PROVIDERS;

1 **(3) ASSESS THE LIKELIHOOD AND POTENTIAL DAMAGE OF THE**
2 **THREATS DESCRIBED UNDER ITEM (2) OF THIS SUBSECTION, TAKING INTO**
3 **CONSIDERATION THE SENSITIVITY OF THE NONPUBLIC INFORMATION;**

4 **(4) ASSESS THE SUFFICIENCY OF POLICIES, PROCEDURES,**
5 **INFORMATION SYSTEMS, AND OTHER SAFEGUARDS IN PLACE TO MANAGE THE**
6 **THREATS DESCRIBED UNDER ITEM (2) OF THIS SUBSECTION, INCLUDING**
7 **CONSIDERATION OF THREATS IN EACH RELEVANT AREA OF THE CARRIER'S**
8 **OPERATIONS, SUCH AS:**

9 **(I) EMPLOYEE TRAINING AND MANAGEMENT;**

10 **(II) INFORMATION SYSTEMS, INCLUDING NETWORK AND**
11 **SOFTWARE DESIGN, AS WELL AS INFORMATION CLASSIFICATION, GOVERNANCE,**
12 **PROCESSING, STORAGE, TRANSMISSION, AND DISPOSAL; AND**

13 **(III) DETECTING, PREVENTING, AND RESPONDING TO ATTACKS,**
14 **INTRUSIONS, OR OTHER SYSTEM FAILURES;**

15 **(5) IMPLEMENT INFORMATION SAFEGUARDS TO MANAGE THE**
16 **THREATS IDENTIFIED IN ITS ONGOING ASSESSMENT; AND**

17 **(6) AT LEAST ANNUALLY, ASSESS THE EFFECTIVENESS OF THE KEY**
18 **CONTROLS, SYSTEMS, AND PROCEDURES OF THE SAFEGUARDS.**

19 **(D) BASED ON ITS RISK ASSESSMENT, A CARRIER SHALL:**

20 **(1) DESIGN ITS INFORMATION SECURITY PROGRAM TO MITIGATE THE**
21 **IDENTIFIED RISKS, COMMENSURATE WITH THE SIZE AND COMPLEXITY OF THE**
22 **CARRIER'S ACTIVITIES, INCLUDING ITS USE OF THIRD-PARTY SERVICE PROVIDERS,**
23 **AND THE SENSITIVITY OF THE NONPUBLIC INFORMATION USED BY THE CARRIER OR**
24 **IN THE CARRIER'S POSSESSION, CUSTODY, OR CONTROL; AND**

25 **(2) DETERMINE WHICH OF THE FOLLOWING SECURITY MEASURES**
26 **ARE APPROPRIATE AND IMPLEMENT THE APPROPRIATE SECURITY MEASURES:**

27 **(I) PLACEMENT OF ACCESS CONTROLS ON INFORMATION**
28 **SYSTEMS, INCLUDING CONTROLS TO AUTHENTICATE AND ALLOW ACCESS ONLY TO**
29 **AUTHORIZED INDIVIDUALS TO PROTECT AGAINST THE UNAUTHORIZED**
30 **ACQUISITION OF NONPUBLIC INFORMATION;**

31 **(II) IDENTIFICATION AND MANAGEMENT OF THE DATA,**
32 **PERSONNEL, DEVICES, SYSTEMS, AND FACILITIES THAT ENABLE THE ORGANIZATION**

1 TO ACHIEVE BUSINESS PURPOSES IN ACCORDANCE WITH THEIR RELATIVE
2 IMPORTANCE TO BUSINESS OBJECTIVES AND THE ORGANIZATION'S RISK STRATEGY;

3 (III) RESTRICTION OF ACCESS AT PHYSICAL LOCATIONS
4 CONTAINING NONPUBLIC INFORMATION TO AUTHORIZED INDIVIDUALS ONLY;

5 (IV) PROTECTION, BY ENCRYPTION OR OTHER APPROPRIATE
6 MEANS, OF ALL NONPUBLIC INFORMATION:

7 1. DURING TRANSMISSION OVER AN EXTERNAL
8 NETWORK; AND

9 2. STORED ON A LAPTOP COMPUTER OR OTHER
10 PORTABLE COMPUTING OR STORAGE DEVICE OR MEDIA;

11 (V) ADOPTION OF SECURE DEVELOPMENT PRACTICES FOR
12 IN-HOUSE DEVELOPED APPLICATIONS USED BY THE CARRIER AND PROCEDURES
13 FOR EVALUATING, ASSESSING, OR TESTING THE SECURITY OF EXTERNALLY
14 DEVELOPED APPLICATIONS USED BY THE CARRIER;

15 (VI) MODIFICATION OF THE INFORMATION SYSTEM IN
16 ACCORDANCE WITH THE CARRIER'S INFORMATION SECURITY PROGRAM;

17 (VII) USE OF EFFECTIVE CONTROLS, WHICH MAY INCLUDE
18 MULTIFACTOR AUTHENTICATION PROCEDURES FOR AN INDIVIDUAL ACCESSING
19 NONPUBLIC INFORMATION;

20 (VIII) REGULAR TESTING AND MONITORING OF SYSTEMS AND
21 PROCEDURES TO DETECT ACTUAL AND ATTEMPTED ATTACKS ON, OR INTRUSIONS
22 INTO, INFORMATION SYSTEMS;

23 (IX) INCLUSION OF AUDIT TRAILS WITHIN THE INFORMATION
24 SECURITY PROGRAM DESIGNED TO:

25 1. DETECT AND RESPOND TO CYBERSECURITY EVENTS;
26 AND

27 2. RECONSTRUCT MATERIAL FINANCIAL TRANSACTIONS
28 SUFFICIENT TO SUPPORT NORMAL OPERATIONS AND OBLIGATIONS OF THE
29 CARRIER;

30 (X) IMPLEMENTATION OF MEASURES TO PROTECT AGAINST
31 DESTRUCTION, LOSS, OR DAMAGE OF NONPUBLIC INFORMATION DUE TO

ENVIRONMENTAL HAZARDS, SUCH AS FIRE AND WATER DAMAGE OR OTHER
CATASTROPHES OR TECHNOLOGICAL FAILURES; AND

(XI) DEVELOPMENT, IMPLEMENTATION, AND MAINTENANCE OF
PROCEDURES FOR THE SECURE DISPOSAL OF NONPUBLIC INFORMATION IN ANY
FORMAT.

(E) A CARRIER'S ENTERPRISE RISK MANAGEMENT PROCESS SHALL
INCLUDE CYBERSECURITY RISKS.

(F) EACH CARRIER SHALL:

(1) STAY INFORMED REGARDING EMERGING THREATS OR
VULNERABILITIES AND USE REASONABLE SECURITY MEASURES WHEN SHARING
INFORMATION RELATIVE TO THE CHARACTER OF THE SHARING AND THE TYPE OF
INFORMATION SHARED; AND

(2) PROVIDE ITS PERSONNEL WITH CYBERSECURITY AWARENESS
TRAINING THAT IS UPDATED AS NECESSARY TO REFLECT RISKS IDENTIFIED BY THE
CARRIER IN THE RISK ASSESSMENT.

(G) (1) IF A CARRIER HAS A BOARD OF DIRECTORS, THE BOARD OR AN
APPROPRIATE COMMITTEE OF THE BOARD SHALL, AT A MINIMUM:

(I) REQUIRE THE CARRIER'S EXECUTIVE MANAGEMENT OR ITS
DELEGATES TO DEVELOP, IMPLEMENT, AND MAINTAIN THE CARRIER'S
INFORMATION SECURITY PROGRAM; AND

(II) REQUIRE THE CARRIER'S EXECUTIVE MANAGEMENT OR ITS
DELEGATES TO REPORT IN WRITING, AT LEAST ANNUALLY, THE FOLLOWING
INFORMATION:

1. THE OVERALL STATUS OF THE INFORMATION
SECURITY PROGRAM AND THE CARRIER'S COMPLIANCE WITH THIS TITLE; AND

2. MATERIAL MATTERS RELATED TO THE INFORMATION
SECURITY PROGRAM, ADDRESSING ISSUES SUCH AS RISK ASSESSMENT, RISK
MANAGEMENT AND CONTROL DECISIONS, THIRD-PARTY SERVICE PROVIDER
ARRANGEMENTS, RESULTS OF TESTING, CYBERSECURITY EVENTS OR VIOLATIONS
AND MANAGEMENT'S RESPONSES THERETO, AND RECOMMENDATIONS FOR
CHANGES IN THE INFORMATION SECURITY PROGRAM.

(2) IF EXECUTIVE MANAGEMENT OF A CARRIER DELEGATES ANY OF

1 THE RESPONSIBILITIES UNDER THIS SECTION, THE EXECUTIVE MANAGEMENT
2 SHALL:

3 (I) OVERSEE THE DEVELOPMENT, IMPLEMENTATION, AND
4 MAINTENANCE OF THE CARRIER'S INFORMATION SECURITY PROGRAM PREPARED
5 BY THE DELEGATES; AND

6 (II) RECEIVE A REPORT FROM THE DELEGATES THAT COMPLIES
7 WITH THE REQUIREMENTS FOR THE REPORT TO THE BOARD OF DIRECTORS UNDER
8 PARAGRAPH (1) OF THIS SUBSECTION.

9 (H) A CARRIER SHALL REQUIRE A THIRD-PARTY SERVICE PROVIDER TO
10 IMPLEMENT APPROPRIATE ADMINISTRATIVE, TECHNICAL, AND PHYSICAL
11 MEASURES TO PROTECT AND SECURE THE INFORMATION SYSTEMS AND NONPUBLIC
12 INFORMATION THAT ARE ACCESSIBLE TO OR HELD BY THE THIRD-PARTY SERVICE
13 PROVIDER.

14 (I) (1) EACH CARRIER SHALL ESTABLISH A WRITTEN INCIDENT
15 RESPONSE PLAN DESIGNED TO PROMPTLY RESPOND TO, AND RECOVER FROM, ANY
16 CYBERSECURITY EVENT THAT COMPROMISES THE CONFIDENTIALITY, INTEGRITY,
17 OR AVAILABILITY OF NONPUBLIC INFORMATION IN ITS POSSESSION, THE CARRIER'S
18 INFORMATION SYSTEMS, OR THE CONTINUING FUNCTIONALITY OF ANY ASPECT OF
19 THE CARRIER'S BUSINESS OR OPERATIONS.

20 (2) THE INCIDENT RESPONSE PLAN SHALL ADDRESS THE FOLLOWING
21 AREAS:

22 (I) THE INTERNAL PROCESS FOR RESPONDING TO A
23 CYBERSECURITY EVENT;

24 (II) THE GOALS OF THE INCIDENT RESPONSE PLAN;

25 (III) THE DEFINITION OF CLEAR ROLES, RESPONSIBILITIES, AND
26 LEVELS OF DECISION-MAKING AUTHORITY;

27 (IV) EXTERNAL AND INTERNAL COMMUNICATIONS AND
28 INFORMATION SHARING;

29 (V) IDENTIFICATION OF REQUIREMENTS FOR THE
30 REMEDIATION OF IDENTIFIED WEAKNESSES IN INFORMATION SYSTEMS AND
31 ASSOCIATED CONTROLS;

32 (VI) DOCUMENTATION AND REPORTING REGARDING

1 CYBERSECURITY EVENTS AND RELATED INCIDENT RESPONSE ACTIVITIES; AND

2 (VII) THE EVALUATION AND REVISION, AS NECESSARY, OF THE
3 INCIDENT RESPONSE PLAN FOLLOWING A CYBERSECURITY EVENT.

4 (J) (1) ON OR BEFORE FEBRUARY 15 EACH YEAR, EACH CARRIER SHALL
5 SUBMIT TO THE COMMISSIONER A WRITTEN STATEMENT CERTIFYING THAT THE
6 CARRIER HAS ADOPTED AN INFORMATION SECURITY PROGRAM AND IS IN
7 COMPLIANCE WITH THE ADDITIONAL REQUIREMENTS SET FORTH IN THIS SECTION.

8 (2) EACH CARRIER SHALL MAINTAIN FOR EXAMINATION BY THE
9 COMMISSIONER ALL RECORDS, SCHEDULES, AND DATA SUPPORTING THIS
10 CERTIFICATE FOR A PERIOD OF 5 YEARS.

11 33-104.

12 (A) IF A CARRIER LEARNS THAT A CYBERSECURITY EVENT HAS OR MAY
13 HAVE OCCURRED, THE CARRIER OR AN OUTSIDE VENDOR OR SERVICE PROVIDER
14 DESIGNATED TO ACT ON BEHALF OF THE CARRIER SHALL CONDUCT A PROMPT
15 INVESTIGATION.

16 (B) DURING THE INVESTIGATION, THE CARRIER OR AN OUTSIDE VENDOR
17 OR SERVICE PROVIDER DESIGNATED TO ACT ON BEHALF OF THE CARRIER, SHALL,
18 AT A MINIMUM:

19 (1) DETERMINE AS MUCH OF THE FOLLOWING INFORMATION AS
20 POSSIBLE:

21 (I) WHETHER A CYBERSECURITY EVENT HAS OCCURRED;

22 (II) THE NATURE AND SCOPE OF THE CYBERSECURITY EVENT;

23 AND

24 (III) IDENTIFICATION OF NONPUBLIC INFORMATION THAT MAY
25 HAVE BEEN INVOLVED IN THE CYBERSECURITY EVENT; AND

26 (2) PERFORM OR OVERSEE REASONABLE MEASURES TO RESTORE
27 THE SECURITY OF THE INFORMATION SYSTEMS COMPROMISED IN THE
28 CYBERSECURITY EVENT TO PREVENT FURTHER UNAUTHORIZED ACQUISITION,
29 RELEASE, OR USE OF NONPUBLIC INFORMATION IN THE CARRIER'S POSSESSION,
30 CUSTODY, OR CONTROL.

31 (C) IF A CARRIER LEARNS THAT A CYBERSECURITY EVENT HAS OR MAY

HAVE OCCURRED IN A SYSTEM MAINTAINED BY A THIRD-PARTY SERVICE PROVIDER, THE CARRIER SHALL COMPLETE THE STEPS LISTED IN SUBSECTION (B) OF THIS SECTION OR CONFIRM AND DOCUMENT THAT THE THIRD-PARTY SERVICE PROVIDER HAS COMPLETED THOSE STEPS.

(D) A CARRIER SHALL:

(1) MAINTAIN RECORDS CONCERNING ALL CYBERSECURITY EVENTS FOR A PERIOD OF AT LEAST 5 YEARS FROM THE DATE OF THE CYBERSECURITY EVENT; AND

(2) PRODUCE THE RECORDS ON DEMAND OF THE COMMISSIONER.

33-105.

(A) A CARRIER SHALL NOTIFY THE COMMISSIONER AS PROMPTLY AS POSSIBLE BUT IN NO EVENT LATER THAN 3 BUSINESS DAYS FROM A DETERMINATION THAT A CYBERSECURITY EVENT HAS OCCURRED WHEN EITHER OF THE FOLLOWING CRITERIA HAS BEEN MET:

(1) THE STATE IS THE CARRIER'S STATE OF DOMICILE; OR

(2) THE CARRIER REASONABLY BELIEVES THAT THE NONPUBLIC INFORMATION INVOLVED IS OF 250 OR MORE CONSUMERS RESIDING IN THE STATE AND EITHER OF THE FOLLOWING CIRCUMSTANCES IS PRESENT:

(I) A CYBERSECURITY EVENT IMPACTING THE CARRIER HAS OCCURRED FOR WHICH NOTICE MUST BE PROVIDED TO A GOVERNMENT BODY, SELF-REGULATORY AGENCY, OR ANY OTHER SUPERVISORY BODY UNDER STATE OR FEDERAL LAW; OR

(II) A CYBERSECURITY EVENT HAS OCCURRED THAT HAS A REASONABLE LIKELIHOOD OF MATERIALLY HARMING:

1. A CONSUMER RESIDING IN THE STATE; OR

2. A MATERIAL PART OF THE NORMAL OPERATION OF THE CARRIER.

(B) THE CARRIER SHALL PROVIDE AS MUCH OF THE FOLLOWING INFORMATION AS REASONABLY POSSIBLE:

(1) THE DATE OF THE CYBERSECURITY EVENT;

1 **(2) A DESCRIPTION OF HOW THE INFORMATION WAS EXPOSED, LOST,**
2 **STOLEN, OR BREACHED, INCLUDING THE SPECIFIC ROLES AND RESPONSIBILITIES**
3 **OF THIRD-PARTY SERVICE PROVIDERS, IF ANY;**

4 **(3) HOW THE CYBERSECURITY EVENT WAS DISCOVERED;**

5 **(4) WHETHER ANY LOST, STOLEN, OR BREACHED INFORMATION HAS**
6 **BEEN RECOVERED AND, IF SO, HOW THIS WAS DONE;**

7 **(5) THE IDENTITY OF THE SOURCE OF THE CYBERSECURITY EVENT;**

8 **(6) WHETHER THE CARRIER HAS FILED A POLICE REPORT OR HAS**
9 **NOTIFIED A REGULATORY, GOVERNMENT, OR LAW ENFORCEMENT AGENCY AND, IF**
10 **SO, WHEN THE NOTIFICATION WAS PROVIDED;**

11 **(7) A DESCRIPTION OF THE SPECIFIC TYPES OF INFORMATION**
12 **ACQUIRED WITHOUT AUTHORIZATION AND, MORE SPECIFICALLY, PARTICULAR**
13 **DATA ELEMENTS, SUCH AS TYPES OF MEDICAL INFORMATION, TYPES OF FINANCIAL**
14 **INFORMATION, OR TYPES OF INFORMATION ALLOWING IDENTIFICATION OF THE**
15 **CONSUMER;**

16 **(8) THE PERIOD DURING WHICH THE INFORMATION SYSTEM WAS**
17 **COMPROMISED BY THE CYBERSECURITY EVENT;**

18 **(9) THE NUMBER OF TOTAL CONSUMERS IN THE STATE AFFECTED BY**
19 **THE CYBERSECURITY EVENT, WITH THE CARRIER PROVIDING:**

20 **(I) THE BEST ESTIMATE OF THIS NUMBER IN ITS INITIAL**
21 **REPORT TO THE COMMISSIONER; AND**

22 **(II) AN UPDATED ESTIMATE OF THIS NUMBER IN EACH**
23 **SUBSEQUENT REPORT TO THE COMMISSIONER IN ACCORDANCE WITH THIS**
24 **SECTION;**

25 **(10) THE RESULTS OF ANY INTERNAL REVIEW:**

26 **(I) IDENTIFYING A LAPSE IN EITHER AUTOMATED CONTROLS**
27 **OR INTERNAL PROCEDURES; OR**

28 **(II) CONFIRMING THAT ALL AUTOMATED CONTROLS OR**
29 **INTERNAL PROCEDURES WERE FOLLOWED;**

1 (11) A COPY OF THE CARRIER'S PRIVACY POLICY AND A STATEMENT
2 OUTLINING THE STEPS THE CARRIER WILL TAKE TO INVESTIGATE AND NOTIFY
3 CONSUMERS AFFECTED BY THE CYBERSECURITY EVENT; AND

4 (12) THE NAME OF A CONTACT PERSON WHO IS BOTH FAMILIAR WITH
5 THE CYBERSECURITY EVENT AND AUTHORIZED TO ACT FOR THE CARRIER.

6 (C) A CARRIER SHALL PROVIDE THE INFORMATION REQUIRED UNDER THIS
7 SECTION IN ELECTRONIC FORM AS DIRECTED BY THE COMMISSIONER.

8 (D) A CARRIER SHALL HAVE A CONTINUING OBLIGATION TO UPDATE AND
9 SUPPLEMENT INITIAL AND SUBSEQUENT NOTIFICATIONS TO THE COMMISSIONER
10 CONCERNING THE CYBERSECURITY EVENT.

11 (E) A CARRIER SHALL COMPLY WITH § 14-3504 OF THE COMMERCIAL LAW
12 ARTICLE, AS APPLICABLE, AND PROVIDE A COPY OF THE NOTICE SENT TO
13 CONSUMERS UNDER THAT SECTION TO THE COMMISSIONER.

14 (F) IF A CARRIER DOES NOT MEET THE NOTIFICATION CRITERIA IN
15 SUBSECTION (A) OF THIS SECTION BUT CONDUCTS AN INVESTIGATION REQUIRED
16 UNDER § 14-3504(B) OR (C) OF THE COMMERCIAL LAW ARTICLE AND DETERMINES
17 THAT THE BREACH OF THE SECURITY OF THE SYSTEM CREATES A LIKELIHOOD THAT
18 PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED, THE CARRIER SHALL
19 PROVIDE THE NOTICE TO THE COMMISSIONER AT THE SAME TIME THE CARRIER
20 PROVIDES NOTICE TO THE OFFICE OF THE ATTORNEY GENERAL UNDER §
21 14-3504(H) OF THE COMMERCIAL LAW ARTICLE.

22 **33-106.**

23 (A) (1) DOCUMENTS, MATERIALS, AND OTHER INFORMATION IN THE
24 CONTROL OR POSSESSION OF THE COMMISSIONER THAT ARE FURNISHED BY A
25 CARRIER OR AN EMPLOYEE OR AGENT THEREOF ACTING ON BEHALF OF THE
26 CARRIER UNDER § 33-103(J) OR § 33-105(B)(2) THROUGH (5), (8), (10), AND (11) OF
27 THIS TITLE OR THAT ARE OBTAINED BY THE COMMISSIONER IN AN INVESTIGATION
28 OR EXAMINATION UNDER THIS SECTION:

29 (I) ARE CONFIDENTIAL BY LAW AND PRIVILEGED;

30 (II) ARE NOT SUBJECT TO THE MARYLAND PUBLIC
31 INFORMATION ACT;

32 (III) ARE NOT SUBJECT TO SUBPOENA; AND

(IV) ARE NOT SUBJECT TO DISCOVERY OR ADMISSIBLE IN EVIDENCE IN A PRIVATE CIVIL ACTION.

(2) THE COMMISSIONER IS AUTHORIZED TO USE THE DOCUMENTS, MATERIALS, AND OTHER INFORMATION IN THE FURTHERANCE OF A REGULATORY OR LEGAL ACTION BROUGHT AS A PART OF THE COMMISSIONER'S DUTIES.

(B) THE COMMISSIONER AND ANY PERSON WHO RECEIVED DOCUMENTS, MATERIALS, OR OTHER INFORMATION WHILE ACTING UNDER THE AUTHORITY OF THE COMMISSIONER MAY NOT BE ALLOWED OR REQUIRED TO TESTIFY IN A PRIVATE CIVIL ACTION CONCERNING CONFIDENTIAL DOCUMENTS, MATERIALS, OR OTHER INFORMATION SUBJECT TO SUBSECTION (A) OF THIS SECTION.

(C) THE COMMISSIONER MAY:

(1) SHARE DOCUMENTS, MATERIALS, OR OTHER INFORMATION, INCLUDING THE CONFIDENTIAL AND PRIVILEGED DOCUMENTS, MATERIALS, OR OTHER INFORMATION SUBJECT TO SUBSECTION (A) OF THIS SECTION, WITH:

(I) OTHER STATE, FEDERAL, AND INTERNATIONAL REGULATORY AGENCIES;

(II) THE NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, ITS AFFILIATES, OR SUBSIDIARIES; AND

(III) STATE, FEDERAL, AND INTERNATIONAL LAW ENFORCEMENT AUTHORITIES, PROVIDED THAT THE RECIPIENT AGREES TO MAINTAIN THE CONFIDENTIALITY AND PRIVILEGED STATUS OF THE DOCUMENT, MATERIAL, OR OTHER INFORMATION;

(2) RECEIVE DOCUMENTS, MATERIALS, OR OTHER INFORMATION, INCLUDING OTHERWISE CONFIDENTIAL AND PRIVILEGED DOCUMENTS, MATERIALS, OR OTHER INFORMATION, FROM:

(I) THE NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, ITS AFFILIATES, OR SUBSIDIARIES; AND

(II) REGULATORY AND LAW ENFORCEMENT OFFICIALS OF OTHER FOREIGN OR DOMESTIC JURISDICTIONS;

(3) SHARE DOCUMENTS, MATERIALS, OR OTHER INFORMATION SUBJECT TO SUBSECTION (A) OF THIS SECTION WITH A THIRD-PARTY CONSULTANT OR VENDOR, IF THE CONSULTANT AGREES IN WRITING TO MAINTAIN THE

1 CONFIDENTIALITY AND PRIVILEGED STATUS OF THE DOCUMENT, MATERIAL, OR
2 OTHER INFORMATION; AND

3 (4) ENTER INTO AGREEMENTS GOVERNING SHARING AND USE OF
4 INFORMATION CONSISTENT WITH THIS SUBSECTION.

5 (D) THE COMMISSIONER SHALL MAINTAIN AS CONFIDENTIAL OR
6 PRIVILEGED ANY DOCUMENT, MATERIAL, OR OTHER INFORMATION RECEIVED
7 UNDER SUBSECTION (C)(2) OF THIS SECTION WITH NOTICE OR THE UNDERSTANDING
8 THAT IT IS CONFIDENTIAL OR PRIVILEGED UNDER THE LAWS OF THE JURISDICTION
9 THAT IS THE SOURCE OF THE DOCUMENT, MATERIAL, OR OTHER INFORMATION.

10 (E) A WAIVER OF AN APPLICABLE PRIVILEGE OR CLAIM OF
11 CONFIDENTIALITY IN THE DOCUMENTS, MATERIALS, OR OTHER INFORMATION MAY
12 NOT OCCUR AS A RESULT OF DISCLOSURE TO THE COMMISSIONER UNDER THIS
13 SECTION OR AS A RESULT OF SHARING AS AUTHORIZED IN SUBSECTION (C) OF THIS
14 SECTION.

15 (F) THIS SECTION DOES NOT PROHIBIT THE COMMISSIONER FROM
16 RELEASING FINAL, ADJUDICATED ACTIONS THAT ARE OPEN TO PUBLIC INSPECTION.

17 **33-107.**

18 IN ADDITION TO ANY OTHER SANCTION TO WHICH A CARRIER MAY BE
19 SUBJECT, A CARRIER THAT VIOLATES A PROVISION OF THIS TITLE IS SUBJECT TO A
20 PENALTY OF NOT LESS THAN \$100 BUT NOT MORE THAN \$125,000 FOR EACH
21 VIOLATION OF THIS TITLE.

22 **33-108.**

23 THE COMMISSIONER MAY ADOPT REGULATIONS CONSISTENT WITH THIS
24 TITLE.

25 SECTION 2. AND BE IT FURTHER ENACTED, That, if any provision of this Act or
26 the application thereof to any person or circumstance is held invalid for any reason in a
27 court of competent jurisdiction, the invalidity does not affect other provisions or any other
28 application of this Act that can be given effect without the invalid provision or application,
29 and for this purpose the provisions of this Act are declared severable.

30 SECTION 3. AND BE IT FURTHER ENACTED, That, except as provided in Section
31 4 of this Act, a carrier shall have until October 1, 2023, to implement § 33-103 of the
32 Insurance Article, as enacted by Section 1 of this Act.

33 SECTION 4. AND BE IT FURTHER ENACTED, That a carrier shall have until
34 October 1, 2024, to implement § 33-103(h) of the Insurance Article, as enacted by Section

1 1 of this Act.

2 SECTION 5. AND BE IT FURTHER ENACTED, That this Act shall take effect
3 October 1, 2022.