Chapter 231

(Senate Bill 207)

AN ACT concerning

Insurance Carriers and Managed Care Organizations – Cybersecurity Standards

FOR the purpose of establishing certain cybersecurity standards applicable to insurance carriers, including health maintenance organizations and third–party administrators; requiring a carrier to take certain actions related to cybersecurity, including developing, implementing, and maintaining a certain information security program, identifying certain threats, and establishing a certain incident response plan; requiring a carrier, under certain circumstances, to notify the Maryland Insurance Commissioner that a cybersecurity event has occurred; establishing that certain documents, materials, and information are confidential and privileged, not subject to the Maryland Public Information Act, subpoena, and discovery, and not admissible as evidence in certain actions; prohibiting certain persons from being allowed or required to testify in certain proceedings; requiring the Commissioner to maintain as confidential or privileged certain documents, materials, and information; applying certain requirements relating to cybersecurity to managed care organizations; and generally relating to insurance carriers and managed care organizations and the security of information.

BY adding to
Article – Health – General
Section ~~19–706(p)~~ 15–102.3(j), 19–706(p), and 19–729(a)(13)
Annotated Code of Maryland
(2019 Replacement Volume and 2021 Supplement)

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

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~~ 33–109 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

15–102.3.

(J) THE PROVISIONS OF § 33–105(F) OF THE INSURANCE ARTICLE APPLY TO MANAGED CARE ORGANIZATIONS.

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) (1) "CARRIER" MEANS:

~~(1)~~ (I) AN AUTHORIZED INSURER;

~~(2)~~ (II) A NONPROFIT HEALTH SERVICE PLAN;

~~(3)~~ (III) A HEALTH MAINTENANCE ORGANIZATION;

~~(4)~~ (IV) A DENTAL ORGANIZATION;

~~(5) A MANAGED CARE ORGANIZATION;~~

~~(6)~~ (V) A MANAGED GENERAL AGENT; ~~AND~~ OR

~~(7)~~ (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 <u>CAN BE USED TO IDENTIFY A PARTICULAR CONSUMER AND THAT</u> 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 <u>IS</u> OTHERWISE <u>AUTHORIZED</u> ACCESS <u>TO</u> 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.

<u>(C) COMPLIANCE WITH THIS TITLE DOES NOT RELIEVE A CARRIER FROM A DUTY TO COMPLY WITH ANY OTHER REQUIREMENTS OF FEDERAL LAW OR TITLE 14</u>

OF THE COMMERCIAL LAW ARTICLE RELATING TO THE PROTECTION AND PRIVACY OF PERSONAL INFORMATION.

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 OF NONPUBLIC INFORMATION AND THE CARRIER'S INFORMATION SYSTEM.

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

(I) THE SIZE AND COMPLEXITY OF THE CARRIER;

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

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

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

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

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

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

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

(C) EACH CARRIER SHALL:

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

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

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

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

(I) EMPLOYEE TRAINING AND MANAGEMENT;

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

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

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

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

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

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

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

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

(II) IDENTIFICATION AND MANAGEMENT OF THE DATA, PERSONNEL, DEVICES, SYSTEMS, AND FACILITIES THAT ENABLE THE ORGANIZATION TO ACHIEVE BUSINESS PURPOSES IN ACCORDANCE WITH THEIR RELATIVE IMPORTANCE TO BUSINESS OBJECTIVES AND THE ORGANIZATION'S RISK STRATEGY;

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

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

1. DURING TRANSMISSION OVER AN EXTERNAL NETWORK; AND

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

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

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

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

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

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

1. DETECT AND RESPOND TO CYBERSECURITY EVENTS; AND

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

(X) IMPLEMENTATION OF MEASURES TO PROTECT AGAINST 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 THE RESPONSIBILITIES UNDER THIS SECTION, THE EXECUTIVE MANAGEMENT SHALL:

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

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

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

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

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

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

(II) THE GOALS OF THE INCIDENT RESPONSE PLAN;

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

(IV) EXTERNAL AND INTERNAL COMMUNICATIONS AND INFORMATION SHARING;

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

(VI) DOCUMENTATION AND REPORTING REGARDING CYBERSECURITY EVENTS AND RELATED INCIDENT RESPONSE ACTIVITIES; AND

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

(J) (1) ~~ON~~ EXCEPT AS PROVIDED IN SUBSECTION (K) OF THIS SECTION, ON OR BEFORE ~~FEBRUARY~~ APRIL 15 EACH YEAR, EACH CARRIER SHALL SUBMIT TO THE COMMISSIONER A WRITTEN STATEMENT CERTIFYING THAT THE CARRIER ~~HAS ADOPTED AN INFORMATION SECURITY PROGRAM AND~~ IS IN COMPLIANCE WITH THE ~~ADDITIONAL~~ REQUIREMENTS SET FORTH IN THIS SECTION.

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

(K) A CARRIER THAT IS NOT DOMICILED IN THE STATE IS EXEMPT FROM THE PROVISIONS OF SUBSECTION (J)(1) OF THIS SECTION IF THE CARRIER:

(1) (I) IS DOMICILED IN ANOTHER UNITED STATES INSURING JURISDICTION THAT HAS ADOPTED A LAW OR REGULATION THAT IS SUBSTANTIALLY SIMILAR TO THIS SECTION;

(II) IS SUBJECT TO THAT LAW OR REGULATION;

(III) IS REQUIRED TO FILE A CERTIFICATION OF COMPLIANCE WITH ITS DOMESTIC REGULATOR UNDER THAT LAW OR REGULATION; AND

(IV) ACTUALLY FILES THE REQUIRED CERTIFICATION WITH ITS DOMESTIC REGULATOR; OR

(2) (I) IS A MEMBER OF AN INSURANCE HOLDING COMPANY SYSTEM, AS DEFINED IN § 7–101 OF THIS ARTICLE; AND

(II) HAS IMPLEMENTED AND IS SUBJECT TO AN INFORMATION SECURITY PROGRAM THAT HAS BEEN APPROVED AND IS MAINTAINED BY ANOTHER CARRIER WITHIN THE SAME INSURANCE HOLDING COMPANY SYSTEM THAT MEETS ALL OF THE CRITERIA SET FORTH IN ITEM (1) OF THIS SUBSECTION.

33–104.

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

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

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

(I) WHETHER A CYBERSECURITY EVENT HAS OCCURRED;

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

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

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

(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) (I) THE STATE IS THE CARRIER'S STATE OF DOMICILE; AND

(II) THE CYBERSECURITY EVENT HAS A REASONABLE LIKELIHOOD OF HARMING A CONSUMER RESIDING IN THE STATE OR ANY MATERIAL PART OF THE NORMAL OPERATIONS OF THE CARRIER; 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;

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

(3) HOW THE CYBERSECURITY EVENT WAS DISCOVERED;

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

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

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

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

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

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

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

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

(10) THE RESULTS OF ANY INTERNAL REVIEW:

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

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

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

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

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

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

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

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

(F) IF A MANAGED CARE ORGANIZATION CONDUCTS AN INVESTIGATION AS REQUIRED BY THE MARYLAND DEPARTMENT OF HEALTH IN ACCORDANCE WITH THE MANAGED CARE ORGANIZATION'S CONTRACT WITH THE MARYLAND DEPARTMENT OF HEALTH AND DETERMINES THAT A CYBERSECURITY EVENT HAS OCCURRED, THE MANAGED CARE ORGANIZATION SHALL PROVIDE TO THE COMMISSIONER COPIES OF ALL NOTICES AND REPORTS PROVIDED TO THE MARYLAND DEPARTMENT OF HEALTH AT THE SAME TIME AND IN THE SAME MANNER THAT THE MANAGED CARE ORGANIZATION PROVIDES THE NOTICES AND REPORTS TO THE MARYLAND DEPARTMENT OF HEALTH.

33–106.

(A) A CARRIER THAT IS SUBJECT TO, GOVERNED BY, AND COMPLIANT WITH THE PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES ISSUED BY THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, 45 C.F.R. PARTS 160 AND 164, ESTABLISHED UNDER THE HEALTH INSURANCE PORTABILITY AND

ACCOUNTABILITY ACT OF 1996, AND THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, AND THAT MAINTAINS NONPUBLIC INFORMATION IN THE SAME MANNER AS PROTECTED HEALTH INFORMATION:

(1) SHALL BE DEEMED TO BE IN COMPLIANCE WITH §§ 33–103 AND 33–104 OF THIS TITLE; AND

(2) MUST COMPLY WITH § 33–105(A) THROUGH (D) OF THIS TITLE.

(B) A CARRIER THAT IS SUBJECT TO, GOVERNED BY, AND IN COMPLIANCE WITH § 33–103 OF THIS TITLE SHALL BE DEEMED TO BE IN COMPLIANCE WITH §§ 14–3502 AND 14–3503 OF THE COMMERCIAL LAW ARTICLE.

~~33–106.~~ **33–107.**

(A) (1) DOCUMENTS, MATERIALS, AND OTHER INFORMATION IN THE CONTROL OR POSSESSION OF THE COMMISSIONER THAT ARE FURNISHED BY A CARRIER OR AN EMPLOYEE OR AGENT THEREOF ACTING ON BEHALF OF THE CARRIER UNDER § 33–103(J) OR § 33–105(B)(2) THROUGH (5), (8), (10), AND (11) OF THIS TITLE OR THAT ARE OBTAINED BY THE COMMISSIONER IN AN INVESTIGATION OR EXAMINATION UNDER THIS SECTION OR FROM A MANAGED CARE ORGANIZATION IN ACCORDANCE WITH § 33–105(F) OF THIS TITLE:

(I) ARE CONFIDENTIAL BY LAW AND PRIVILEGED;

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

(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) IF THE RECIPIENT AGREES TO MAINTAIN THE CONFIDENTIALITY AND PRIVILEGED STATUS OF THE DOCUMENTS, MATERIALS, OR OTHER INFORMATION, 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 CONFIDENTIALITY AND PRIVILEGED STATUS OF THE DOCUMENT, MATERIAL, OR OTHER INFORMATION; AND

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

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

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

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

~~**33–107.**~~ **33–108.**

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

~~**33–108.**~~ **33–109.**

THE COMMISSIONER MAY ADOPT REGULATIONS CONSISTENT WITH THIS TITLE.

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

SECTION 3. AND BE IT FURTHER ENACTED, That, except as provided in ~~Section 4~~ Sections 4 and 5 of this Act, a carrier shall have until October 1, 2023, to implement § 33–103 of the Insurance Article, as enacted by Section 1 of this Act.

SECTION 4. AND BE IT FURTHER ENACTED, That, except as provided in Section 5 of this Act, a carrier shall have until October 1, 2024, to implement § 33–103(h) of the Insurance Article, as enacted by Section 1 of this Act.

SECTION 5. AND BE IT FURTHER ENACTED, That the implementation dates set forth in Sections 3 and 4 of this Act may be deferred for 1 year by a carrier that:

(1) has fewer than 25 employees; and

(2) if the insurance group of which the carrier is a member has annual direct written and unaffiliated assumed premium less than $1,000,000,000, including international direct and assumed premium but excluding premiums reinsured with the Federal Crop Insurance Corporation and the Federal Flood Program, has less than:

(i) $5,000,000 in gross annual revenue;

(ii) $10,000,000 in year–end total assets; or

(iii) $100,000,000 in annual direct written premium, including international direct and assumed premium but excluding premiums reinsured with the Federal Crop Insurance Corporation and the Federal Flood Program.

SECTION 6. AND BE IT FURTHER ENACTED, That it is the intent of the General Assembly that the Maryland Insurance Commissioner be added as a member to any Executive Branch council related to cybersecurity.

SECTION ~~5.~~ ~~6.~~ 7. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2022.

Approved by the Governor, April 21, 2022.