Chapter 5

(House Bill 333 of the 2025 Regular Session)

AN ACT concerning

~~Cybersecurity –~~ Healthcare Ecosystem Stakeholder Cybersecurity Workgroup

FOR the purpose of ~~requiring the Maryland Health Care Commission and the Maryland Insurance Administration to include a cybersecurity expert as staff to perform certain functions and submit to the State Chief Information Security Officer a report on the cybersecurity practices and policies of certain healthcare ecosystem entities on a certain basis; requiring healthcare ecosystem entities to take certain actions related to cybersecurity, including adopting and implementing certain cybersecurity standards, undergoing a third–party cybersecurity audit on a certain basis, and reporting cybersecurity incidents to the State Security Operations Center in the Department of Information Technology; requiring the Center to notify certain agencies of a cybersecurity incident reported under this Act; authorizing the Maryland Department of Emergency Management to convene a workgroup to review cybersecurity practices, threats, and emerging issues in the healthcare ecosystem; requiring the Maryland Department of Emergency Management to convene a workgroup to study and make recommendations to improve the cybersecurity of the healthcare ecosystem~~ establishing the Healthcare Ecosystem Stakeholder Cybersecurity Workgroup to develop strategies to prevent cybersecurity disruptions to the healthcare ecosystem, ensure the continuous delivery of essential healthcare ecosystem services, and enhance recovery efforts of the healthcare ecosystem following a cybersecurity incident; ~~and generally relating to the Healthcare Ecosystem Stakeholder Cybersecurity Workgroup;~~ and generally relating to ~~cybersecurity and the healthcare ecosystem~~ the Healthcare Ecosystem Stakeholder Cybersecurity Workgroup.

~~BY repealing and reenacting, without amendments,~~
~~Article – Health – General~~
~~Section 19–101~~
~~Annotated Code of Maryland~~
~~(2023 Replacement Volume and 2024 Supplement)~~

~~BY adding to~~
~~Article – Health – General~~
~~Section 19–113~~
~~Annotated Code of Maryland~~
~~(2023 Replacement Volume and 2024 Supplement)~~

~~BY repealing and reenacting, without amendments,~~
~~Article – Insurance~~
~~Section 1–101(a), (b), and (k)~~
~~Annotated Code of Maryland~~

~~(2017 Replacement Volume and 2024 Supplement)~~

~~BY adding to~~
~~Article – Insurance~~
~~Section 2–117~~
~~Annotated Code of Maryland~~
~~(2017 Replacement Volume and 2024 Supplement)~~

~~BY repealing and reenacting, without amendments,~~
~~Article – State Finance and Procurement~~
~~Section 3.5–101(a) and (e), 3.5–2A–01, and 3.5–301(a) and (e)~~
~~Annotated Code of Maryland~~
~~(2021 Replacement Volume and 2024 Supplement)~~

~~BY adding to~~
~~Article – State Finance and Procurement~~
~~Section 3.5–2A–07~~
~~Annotated Code of Maryland~~
~~(2021 Replacement Volume and 2024 Supplement)~~

~~BY adding to~~
~~Article – Health – General~~
~~Section 19–113(f)~~
~~Annotated Code of Maryland~~
~~(2023 Replacement Volume and 2024 Supplement)~~
~~(As enacted by Section 1 of this Act)~~

~~BY adding to~~
~~Article – Insurance~~
~~Section 2–117(f)~~
~~Annotated Code of Maryland~~
~~(2017 Replacement Volume and 2024 Supplement)~~
~~(As enacted by Section 1 of this Act)~~

~~BY repealing and reenacting, without amendments,~~
~~Article – Public Safety~~
~~Section 14–101(a) and (b)~~
~~Annotated Code of Maryland~~
~~(2022 Replacement Volume and 2024 Supplement)~~

~~BY adding to~~
~~Article – Public Safety~~
~~Section 14–104.3~~
~~Annotated Code of Maryland~~
~~(2022 Replacement Volume and 2024 Supplement)~~

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

~~Article – Health – General~~

~~19–101.~~

~~In this subtitle, "Commission" means the Maryland Health Care Commission.~~

~~19–113.~~

~~(A)~~ **~~(1)~~** **~~IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.~~**

~~(2)~~ **~~"CYBERSECURITY" HAS THE MEANING STATED IN § 3.5–301 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.~~**

~~(3)~~ **~~"ESSENTIAL CAPABILITIES" MEANS THE SERVICES THAT MUST BE AVAILABLE IN THE HEALTHCARE ECOSYSTEM TO ENSURE THE CONTINUITY OF CRITICAL CARE AND PATIENT SAFETY, INCLUDING DURING AN INCIDENT DIMINISHING THE CAPACITY OF THE HEALTHCARE ECOSYSTEM.~~**

~~(4)~~ **~~"HEALTHCARE ECOSYSTEM" MEANS THE ENTITIES AND RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS.~~**

~~(5)~~ **~~(I)~~** **~~"HEALTHCARE ECOSYSTEM ENTITY" INCLUDES:~~**

~~1. AN ELECTRONIC DATA INTERCHANGE CLEARINGHOUSE;~~

~~2. A FREESTANDING MEDICAL FACILITY, AS DEFINED IN § 19–3A–01 OF THIS TITLE;~~

~~3. A HEALTH INFORMATION EXCHANGE, AS DEFINED IN § 4–301 OF THIS ARTICLE;~~

~~4. A HOSPITAL, AS DEFINED IN § 19–301 OF THIS TITLE; AND~~

~~5. AN ENTITY IDENTIFIED BY THE COMMISSION IN REGULATIONS TO BE INCLUDED IN THE HEALTHCARE ECOSYSTEM.~~

~~(II)~~ **~~"HEALTHCARE ECOSYSTEM ENTITY" DOES NOT INCLUDE:~~**

~~1. A CARRIER, AS DEFINED IN § 2–117 OF THE INSURANCE ARTICLE; OR~~

~~2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN § 15–1601 OF THE INSURANCE ARTICLE.~~

~~(6) "ZERO–TRUST" MEANS A CYBERSECURITY APPROACH:~~

~~(I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND~~

~~(II) BASED ON THE PREMISE THAT TRUST IS NOT GRANTED IMPLICITLY BUT MUST BE EVALUATED CONTINUALLY.~~

~~(B) THE COMMISSION SHALL INCLUDE ON ITS STAFF AT LEAST ONE EMPLOYEE WHO IS AN EXPERT IN CYBERSECURITY TO:~~

~~(1) ADVISE THE CHAIRMAN AND MEMBERS OF THE COMMISSION ON MEASURES TO IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF HEALTHCARE ECOSYSTEM ENTITIES;~~

~~(2) CONSULT WITH THE OFFICE OF SECURITY MANAGEMENT ON CYBERSECURITY ISSUES RELATED TO HEALTH CARE REGULATION; AND~~

~~(3) REPRESENT THE COMMISSION ON ANY WORKGROUP, TASK FORCE, OR SIMILAR ENTITY THAT IS FOCUSED ON CYBERSECURITY AND ON WHICH REPRESENTATION FROM THE COMMISSION IS REQUESTED OR REQUIRED.~~

~~(C) A HEALTHCARE ECOSYSTEM ENTITY SHALL:~~

~~(1) ADOPT AND IMPLEMENT CYBERSECURITY STANDARDS THAT ARE EQUAL TO OR EXCEED ANY STANDARDS ADOPTED BY THE COMMISSION;~~

~~(2) ADOPT A ZERO–TRUST CYBERSECURITY APPROACH FOR ON–PREMISES SERVICES AND CLOUD–BASED SERVICES;~~

~~(3) ESTABLISH MINIMUM SECURITY STANDARDS FOR EACH OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICE BASED ON THE LEVEL OF SECURITY RISK FOR EACH DEVICE, INCLUDING SECURITY RISKS ASSOCIATED WITH SUPPLY CHAINS; AND~~

~~(4) ON OR BEFORE JANUARY 1, 2026, AND EVERY 2 YEARS THEREAFTER:~~

~~(I) UNDERGO A THIRD–PARTY AUDIT TO EVALUATE THE ENTITY'S CYBERSECURITY PRACTICES AND RESOURCES BASED ON THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS–SECTOR CYBERSECURITY PERFORMANCE GOALS OR A MORE STRINGENT STANDARD BASED ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FRAMEWORK; AND~~

~~(II) SUBMIT TO THE COMMISSION A REPORT THAT INCLUDES:~~

~~1. THE RESULTS AND RECOMMENDATIONS OF THE AUDIT;~~

~~2. THE DATE OF THE CYBERSECURITY AUDIT;~~

~~3. THE STANDARD USED TO EVALUATE THE ENTITY; AND~~

~~4. THE NAME OF THE THIRD–PARTY THAT CONDUCTED THE AUDIT.~~

~~(D) ON OR BEFORE JULY 1, 2026, AND EVERY 2 YEARS THEREAFTER, THE COMMISSION SHALL COLLECT CERTIFICATION OF A HEALTHCARE ECOSYSTEM ENTITY'S COMPLIANCE WITH THE STANDARD USED IN THE AUDIT CONDUCTED UNDER SUBSECTION (C)(4) OF THIS SECTION FOR CYBERSECURITY–RELATED POLICIES AND PROCEDURES.~~

~~(E) ON OR BEFORE JANUARY 1, 2027, AND EVERY 2 YEARS THEREAFTER, THE COMMISSION SHALL SUBMIT A REPORT TO THE STATE CHIEF INFORMATION SECURITY OFFICER OR THE OFFICER'S DESIGNEE THAT INCLUDES:~~

~~(1) A GENERAL OVERVIEW OF CYBERSECURITY TECHNOLOGY AND POLICIES USED BY HEALTHCARE ECOSYSTEM ENTITIES IN THE STATE, GROUPED IN THE FOLLOWING MANNER:~~

~~(I) HOSPITALS;~~

~~(II) FREESTANDING MEDICAL FACILITIES;~~

~~(III) ELECTRONIC DATA INTERCHANGE CLEARINGHOUSES;~~

~~(IV) HEALTH INFORMATION EXCHANGES; AND~~

~~(V) ANY OTHER ENTITY THE COMMISSION CONSIDERS SIGNIFICANT ENOUGH TO INCLUDE IN THE REPORT;~~

~~**(2) INFORMATION ABOUT EACH CERTIFICATION COLLECTED, INCLUDING:**~~

~~**(I) THE NAME OF THE HEALTHCARE ECOSYSTEM ENTITY;**~~

~~**(II) THE DATE OF THE HEALTHCARE ECOSYSTEM ENTITY'S MOST RECENT CYBERSECURITY AUDIT;**~~

~~**(III) THE CYBERSECURITY STANDARD USED IN THE CYBERSECURITY AUDIT OF THE HEALTHCARE ECOSYSTEM ENTITY; AND**~~

~~**(IV) THE NAME OF THE THIRD PARTY THAT COMPLETED THE CYBERSECURITY AUDIT;**~~

~~**(3) AN OVERVIEW OF ESSENTIAL CAPABILITIES PROVIDED BY HEALTHCARE ECOSYSTEM ENTITIES;**~~

~~**(4) RECOMMENDATIONS FOR ENSURING THE CONTINUOUS DELIVERY OF ESSENTIAL CAPABILITIES DURING AND FOLLOWING A DISRUPTION TO THE HEALTHCARE ECOSYSTEM; AND**~~

~~**(5) RECOMMENDATIONS TO IMPROVE CYBERSECURITY FOR THE GROUPS OF HEALTHCARE ECOSYSTEM ENTITIES IDENTIFIED IN ITEM (1) OF THIS SUBSECTION.**~~

~~**Article – Insurance**~~

~~1–101.~~

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

~~(b) "Administration" means the Maryland Insurance Administration.~~

~~(k) "Commissioner" means the Maryland Insurance Commissioner.~~

~~**2–117.**~~

~~**(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**~~

~~**(2) "CARRIER" MEANS:**~~

~~**(I) AN INSURER AUTHORIZED TO SELL HEALTH INSURANCE;**~~

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

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

~~(IV) A DENTAL PLAN ORGANIZATION; AND~~

~~(V) ANY OTHER ENTITY PROVIDING A PLAN OF HEALTH INSURANCE, HEALTH BENEFITS, OR HEALTH SERVICES AUTHORIZED UNDER THIS ARTICLE OR THE AFFORDABLE CARE ACT.~~

~~(3) "ESSENTIAL CAPABILITIES" MEANS THE SERVICES THAT MUST BE AVAILABLE IN THE HEALTHCARE ECOSYSTEM TO ENSURE THE CONTINUITY OF CRITICAL CARE AND PATIENT SAFETY, INCLUDING DURING AN INCIDENT DIMINISHING THE CAPACITY OF THE HEALTHCARE ECOSYSTEM.~~

~~(4) "HEALTHCARE ECOSYSTEM" MEANS THE ENTITIES AND RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS.~~

~~(5) (I) "HEALTHCARE ECOSYSTEM ENTITY" MEANS:~~

~~1. A CARRIER; OR~~

~~2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN § 15–1601 OF THIS ARTICLE.~~

~~(II) "HEALTHCARE ECOSYSTEM ENTITY" DOES NOT INCLUDE A GOVERNMENTAL PAYOR.~~

~~(6) "ZERO–TRUST" MEANS A CYBERSECURITY APPROACH:~~

~~(I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND~~

~~(II) BASED ON THE PREMISE THAT TRUST IS NOT GRANTED IMPLICITLY BUT MUST BE EVALUATED CONTINUALLY.~~

~~(B) THE ADMINISTRATION SHALL INCLUDE ON ITS STAFF AT LEAST ONE EMPLOYEE WHO IS AN EXPERT IN CYBERSECURITY TO:~~

~~(1) ADVISE THE COMMISSIONER ON MEASURES TO IMPROVE OVERSIGHT OF THE CYBERSECURITY PRACTICES OF HEALTHCARE ECOSYSTEM ENTITIES;~~

~~(2) CONSULT WITH THE OFFICE OF SECURITY MANAGEMENT ON CYBERSECURITY ISSUES RELATED TO HEALTH INSURANCE REGULATION; AND~~

~~(3) REPRESENT THE ADMINISTRATION ON ANY WORKGROUP, TASK FORCE, OR SIMILAR ENTITY THAT IS FOCUSED ON CYBERSECURITY AND ON WHICH REPRESENTATION FROM THE ADMINISTRATION IS REQUIRED OR REQUESTED.~~

~~(C) A HEALTHCARE ECOSYSTEM ENTITY SHALL:~~

~~(1) ADOPT AND IMPLEMENT CYBERSECURITY STANDARDS THAT ARE EQUAL TO OR EXCEED ANY STANDARDS ADOPTED BY THE ADMINISTRATION;~~

~~(2) ADOPT A ZERO–TRUST CYBERSECURITY APPROACH FOR ON–PREMISES SERVICES AND CLOUD–BASED SERVICES;~~

~~(3) ESTABLISH MINIMUM SECURITY STANDARDS FOR EACH OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICE BASED ON THE LEVEL OF SECURITY RISK FOR EACH DEVICE, INCLUDING SECURITY RISKS ASSOCIATED WITH SUPPLY CHAINS; AND~~

~~(4) ON OR BEFORE JANUARY 1, 2026, AND EVERY 2 YEARS THEREAFTER:~~

~~(I) UNDERGO A THIRD–PARTY AUDIT TO EVALUATE THE ENTITY'S CYBERSECURITY PRACTICES AND RESOURCES BASED ON THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS–SECTOR CYBERSECURITY PERFORMANCE GOALS OR A MORE STRINGENT STANDARD BASED ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FRAMEWORK; AND~~

~~(II) SUBMIT TO THE ADMINISTRATION A REPORT THAT INCLUDES:~~

~~1. THE RESULTS AND RECOMMENDATIONS FROM THE AUDIT;~~

~~2. THE DATE OF THE CYBERSECURITY AUDIT;~~

~~3. THE STANDARD USED TO EVALUATE THE ENTITY; AND~~

~~4. THE NAME OF THE THIRD–PARTY THAT CONDUCTED THE AUDIT.~~

~~(D) ON OR BEFORE JULY 1, 2026, AND EVERY 2 YEARS THEREAFTER, THE ADMINISTRATION SHALL COLLECT CERTIFICATION OF A HEALTHCARE ECOSYSTEM ENTITY'S COMPLIANCE WITH THE STANDARD USED IN THE AUDIT CONDUCTED UNDER SUBSECTION (C)(4) OF THIS SECTION FOR CYBERSECURITY–RELATED POLICIES AND PROCEDURES.~~

~~(E) ON OR BEFORE JANUARY 1, 2027, AND EVERY 2 YEARS THEREAFTER, THE ADMINISTRATION SHALL SUBMIT A REPORT TO THE STATE CHIEF INFORMATION SECURITY OFFICER OR THE OFFICER'S DESIGNEE THAT INCLUDES:~~

~~(1) A GENERAL OVERVIEW OF CYBERSECURITY TECHNOLOGY AND POLICIES USED BY HEALTHCARE ECOSYSTEM ENTITIES IN THE STATE, GROUPED IN THE FOLLOWING MANNER:~~

~~(I) INSURERS AUTHORIZED TO SELL HEALTH INSURANCE;~~

~~(II) NONPROFIT HEALTH SERVICE PLANS;~~

~~(III) HEALTH MAINTENANCE ORGANIZATIONS;~~

~~(IV) DENTAL PLAN ORGANIZATIONS;~~

~~(V) PHARMACY BENEFITS MANAGERS; AND~~

~~(VI) ANY OTHER ENTITY PROVIDING A PLAN OF HEALTH INSURANCE, HEALTH BENEFITS, OR HEALTH SERVICES AUTHORIZED UNDER THIS ARTICLE OR THE AFFORDABLE CARE ACT;~~

~~(2) INFORMATION ABOUT EACH CERTIFICATION COLLECTED, INCLUDING:~~

~~(I) THE NAME OF THE HEALTHCARE ECOSYSTEM ENTITY;~~

~~(II) THE DATE OF THE HEALTHCARE ECOSYSTEM ENTITY'S MOST RECENT CYBERSECURITY AUDIT;~~

~~(III) THE CYBERSECURITY STANDARD USED IN THE CYBERSECURITY AUDIT OF THE HEALTHCARE ECOSYSTEM ENTITY; AND~~

~~(IV) THE NAME OF THE THIRD–PARTY THAT COMPLETED THE CYBERSECURITY AUDIT;~~

~~(3) AN OVERVIEW OF ESSENTIAL CAPABILITIES PROVIDED BY THE HEALTHCARE ECOSYSTEM ENTITY;~~

~~(4) RECOMMENDATIONS FOR ENSURING THE CONTINUOUS DELIVERY OF ESSENTIAL CAPABILITIES DURING AND FOLLOWING A DISRUPTION TO THE HEALTHCARE ECOSYSTEM; AND~~

~~(5) RECOMMENDATIONS TO IMPROVE CYBERSECURITY FOR THE GROUPS OF HEALTHCARE ECOSYSTEM ENTITIES IDENTIFIED IN ITEM (1) OF THIS SUBSECTION.~~

~~**Article – State Finance and Procurement**~~

~~3.5–101.~~

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

~~(e) "Department" means the Department of Information Technology.~~

~~3.5–2A–01.~~

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

~~(b) "Council" means the Maryland Cybersecurity Coordinating Council.~~

~~(c) "Office" means the Office of Security Management.~~

~~**3.5–2A–07.**~~

~~**(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**~~

~~**(2) "HEALTHCARE ECOSYSTEM" MEANS THE ENTITIES AND RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER HEALTH CARE TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS.**~~

~~**(3) "HEALTHCARE ECOSYSTEM ENTITY" INCLUDES:**~~

~~**(I) A CARRIER;**~~

~~**(II) AN ELECTRONIC DATA INTERCHANGE CLEARINGHOUSE;**~~

~~**(III) A FREESTANDING MEDICAL FACILITY;**~~

~~**(IV) A HOSPITAL;**~~

~~**(V) A PHARMACY BENEFITS MANAGER;**~~

~~(VI) A HEALTH INFORMATION EXCHANGE; AND~~

~~(VII) ANY OTHER ENTITY IDENTIFIED BY THE MARYLAND HEALTH CARE COMMISSION OR THE MARYLAND INSURANCE ADMINISTRATION IN REGULATIONS TO BE INCLUDED IN THE HEALTHCARE ECOSYSTEM.~~

~~(B) (1) A HEALTHCARE ECOSYSTEM ENTITY SHALL REPORT, IN ACCORDANCE WITH THE PROCESS ESTABLISHED UNDER PARAGRAPH (2) OF THIS SUBSECTION, A CYBERSECURITY INCIDENT, INCLUDING AN ATTACK ON A SYSTEM BEING USED BY THE HEALTHCARE ECOSYSTEM ENTITY, TO THE STATE SECURITY OPERATIONS CENTER IN THE DEPARTMENT.~~

~~(2) THE OFFICE, IN CONSULTATION WITH THE MARYLAND HEALTH CARE COMMISSION AND THE MARYLAND INSURANCE ADMINISTRATION, SHALL ESTABLISH A PROCESS FOR A HEALTHCARE ECOSYSTEM ENTITY TO REPORT A CYBERSECURITY INCIDENT UNDER PARAGRAPH (1) OF THIS SUBSECTION, INCLUDING:~~

~~(I) THE CRITERIA FOR DETERMINING THE CIRCUMSTANCES UNDER WHICH A CYBERSECURITY INCIDENT MUST BE REPORTED;~~

~~(II) THE MANNER IN WHICH A CYBERSECURITY INCIDENT MUST BE REPORTED; AND~~

~~(III) THE TIME PERIOD WITHIN WHICH A CYBERSECURITY INCIDENT MUST BE REPORTED.~~

~~(3) THE STATE SECURITY OPERATIONS CENTER IMMEDIATELY SHALL NOTIFY APPROPRIATE STATE AND LOCAL AGENCIES OF A CYBERSECURITY INCIDENT REPORTED UNDER THIS SUBSECTION.~~

~~(4) (I) ON OR BEFORE JULY 1 EACH YEAR, BEGINNING IN 2026, THE OFFICE SHALL REPORT TO THE GOVERNOR, THE COUNCIL, AND, IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY ON THE NUMBER OF CYBERSECURITY INCIDENTS AND TYPES OF CYBERSECURITY INCIDENTS REPORTED UNDER PARAGRAPH (1) OF THIS SUBSECTION IN THE IMMEDIATELY PRECEDING CALENDAR YEAR.~~

~~(II) A REPORT SUBMITTED IN ACCORDANCE WITH SUBPARAGRAPH (I) OF THIS PARAGRAPH MAY NOT IDENTIFY A HEALTHCARE ECOSYSTEM ENTITY THAT REPORTED AN INCIDENT TO THE OFFICE OR A HEALTHCARE ECOSYSTEM ENTITY THAT WAS DIRECTLY AFFECTED BY AN INCIDENT REPORTED TO THE CENTER.~~

~~3.5–301.~~

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

~~(c) "Cybersecurity" means processes or capabilities wherein systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation.~~

~~SECTION 2. AND BE IT FURTHER ENACTED, That the Laws of Maryland read as follows:~~

~~**Article – Health – General**~~

~~19–113.~~

~~**(F) THE COMMISSION SHALL ADOPT REGULATIONS TO IMPLEMENT CYBERSECURITY STANDARDS AND PROCEDURES TO:**~~

~~**(1) PREVENT DISRUPTIONS TO THE HEALTHCARE ECOSYSTEM;**~~

~~**(2) ENABLE THE DELIVERY OF ESSENTIAL CAPABILITIES BY THE HEALTHCARE ECOSYSTEM; AND**~~

~~**(3) SUPPORT RECOVERY FROM AN INCIDENT THAT DISRUPTS THE HEALTHCARE ECOSYSTEM.**~~

~~**Article – Insurance**~~

~~2–117.~~

~~**(F) THE ADMINISTRATION SHALL ADOPT REGULATIONS TO IMPLEMENT CYBERSECURITY STANDARDS AND PROCEDURES TO:**~~

~~**(1) PREVENT DISRUPTIONS TO THE HEALTHCARE ECOSYSTEM;**~~

~~**(2) ENABLE THE DELIVERY OF ESSENTIAL CAPABILITIES BY THE HEALTHCARE ECOSYSTEM; AND**~~

~~**(3) SUPPORT RECOVERY FROM AN INCIDENT THAT DISRUPTS THE HEALTHCARE ECOSYSTEM.**~~

~~**Article – Public Safety**~~

~~14–101.~~

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

~~(b) "Department" means the Maryland Department of Emergency Management.~~

~~**14–104.3.**~~

~~**(A) THE DEPARTMENT SHALL PROVIDE GUIDANCE TO THE MARYLAND HEALTH CARE COMMISSION AND THE MARYLAND INSURANCE ADMINISTRATION REGARDING THE IMPLEMENTATION AND MONITORING OF CYBERSECURITY REGULATORY STANDARDS FOR HEALTHCARE ECOSYSTEM ENTITIES.**~~

~~**(B) THE DEPARTMENT MAY CONVENE A WORKGROUP TO REVIEW CYBERSECURITY PRACTICES, THREATS, AND EMERGING ISSUES AFFECTING THE HEALTHCARE ECOSYSTEM.**~~

~~SECTION 3. AND BE IT FURTHER ENACTED, That:~~

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That:

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

(2) "Cybersecurity" has the meaning stated in § 3.5–301 of the State Finance and Procurement Article.

(3) "Essential capabilities" means the services that must be available in the healthcare ecosystem to ensure the continuity of critical care and patient safety, including during an incident diminishing the capacity of the healthcare ecosystem.

(4) "Healthcare ecosystem" means the entities and relationships among entities that are necessary to deliver treatment, payment, and health care operations.

(5) (i) "Healthcare ecosystem entity" includes:

1. a carrier, as defined in § 2–117 of the Insurance Article;

2. an electronic data interchange clearinghouse;

3. a freestanding medical facility, as defined in § 19–3A–01 of the Health – General Article;

4. a health information exchange, as defined in § 4–301 of the Health – General Article;

5. a hospital, as defined in § 19–301 of the Health – General Article; and

6. a pharmacy benefits manager, as defined in § 15–1601 of the Insurance Article.

(ii) "Healthcare ecosystem entity" does not include a governmental payor.

(6) "Health care operations" has the meaning stated in 45 C.F.R. § 164.501.

(7) "Payment" has the meaning stated in 45 C.F.R. § 164.501.

(8) "Treatment" has the meaning stated in 45 C.F.R. § 164.501.

(9) "Workgroup" means the Healthcare Ecosystem Stakeholder Cybersecurity Workgroup.

(b) (1) ~~The Maryland Department of Emergency Management shall convene a healthcare ecosystem stakeholder workgroup to study and make recommendations to improve the cybersecurity of the healthcare ecosystem in the State~~ There is a Healthcare Ecosystem Stakeholder Cybersecurity Workgroup.

(2) The purpose of the Workgroup is to develop strategies to:

(i) prevent cybersecurity disruptions to healthcare ecosystem operations;

(ii) ensure the continuous delivery of essential healthcare ecosystem services; and

(iii) enhance recovery efforts of the healthcare ecosystem following a cybersecurity incident.

~~(2) The workgroup shall include:~~

~~(i) one representative of the Maryland Health Care Commission;~~

~~(ii) one representative of the Maryland Insurance Administration;~~

~~(iii) one representative of the Office of Security Management within the Department of Information Technology;~~

~~(iv) representatives from healthcare ecosystem entities selected by the Maryland Department of Emergency Management; and~~

~~(v) any other stakeholders or experts selected by the Maryland Department of Emergency Management.~~

~~(3) The Maryland Department of Emergency Management may convene subgroups considered appropriate to focus on specific concerns facing the healthcare ecosystem or specific aspects of the healthcare ecosystem.~~

(c) The Workgroup consists of the following members:

(1) one member of the Senate of Maryland, appointed by the President of the Senate;

(2) one member of the House of Delegates, appointed by the Speaker of the House;

(3) the Chairman of the Maryland Health Care Commission, or the Chairman's designee;

(4) the Maryland Insurance Commissioner, or the Commissioner's designee;

(5) the Secretary of Emergency Management, or the Secretary's designee;

(6) the State Chief Information Security Officer, or the State Chief Officer's designee;

(7) two representatives from the Subcommittee on Critical Infrastructure of the Maryland Cybersecurity Council, appointed by the Chair of the Maryland Cybersecurity Council;

(8) one representative from each of the following organizations, designated by the head of the organization:

(i) one representative of the Cooperative Exchange;

(ii) one representative of the Electronic Health Record Association;

(iii) one representative of the Maryland League of Life and Health Insurers;

(iv) one representative of the Maryland Hospital Association; and

(v) one representative of the Maryland Cybersecurity Association;

(9) one representative of a pharmacy benefits manager, appointed by the Maryland Insurance Commissioner;

(10) the following representatives appointed by the Chairman of the Maryland Health Care Commission:

(i) one representative of an electronic data interchange clearinghouse;

(ii) one representative of a freestanding medical facility;

(iii) one representative of a large hospital;

(iv) one representative of a small hospital;

(v) one representative of an inpatient psychiatric hospital; and

(vi) one representative of a health information exchange; and

(11) three representatives of a patient advocacy group, jointly appointed by the Chairman of the Maryland Health Care Commission and the Maryland Insurance Commissioner.

(d) The Chairman of the Maryland Health Care Commission, or the Chairman's designee, and the Maryland Insurance Commissioner, or the Commissioner's designee, shall cochair the Workgroup.

(e) The Maryland Health Care Commission and the Maryland Insurance Administration shall provide staff for the Workgroup.

(f) A member of the Workgroup:

(1) may not receive compensation as a member of the Workgroup; but

(2) is entitled to reimbursement for expenses under the Standard State Travel Regulations, as provided in the State budget.

~~(c)~~ (g) The ~~workgroup~~ Workgroup shall:

(1) identify essential capabilities required for the delivery of health care during a cybersecurity attack;

(2) identify functional requirements for the healthcare ecosystem to be capable of providing the essential capabilities identified under item (1) of this subsection;

(3) identify and map all healthcare ecosystem entities in the State against the essential health care capabilities and identified functional requirements;

(4) identify which healthcare ecosystem entities are needed, directly or indirectly, to provide the essential capabilities identified under item (1) of this subsection;

(5) ~~identify other issues related to cybersecurity in the healthcare ecosystem~~ develop an ecosystem cybersecurity threat and risk assessment based on the essential health care capabilities and supporting functions;

(6) examine cybersecurity challenges affecting the healthcare ecosystem based on the threat and risk assessment;

~~(6)~~ (7) review best practices for cybersecurity and processes used in the healthcare ecosystem, including NIST 800–207, NIST 800–207A, NIST 800–53A, the NIST Cybersecurity Framework, HICP Technical Volume 1, and HICP Technical Volume 2; ~~and~~

~~(7) provide guidance for the Maryland Health Care Commission and the Maryland Insurance Administration regarding the adoption and maintenance of cybersecurity regulatory standards.~~

(8) make recommendations for adopting and maintaining cybersecurity regulatory standards; and

(9) make recommendations for ensuring that essential capabilities and supporting functions are resilient to disruption.

~~(d)~~ (h) (1) On or before ~~July~~ January 1, 2026, the ~~Maryland Department of Emergency Management~~ Workgroup shall submit an interim report ~~defining the scope and contents of the State's healthcare ecosystem~~ of its findings and recommendations to the Governor, the Secretary of Emergency Management, the ~~Chair~~ Chairman of the Maryland Health Care Commission, the Maryland Insurance Commissioner, the State Chief Information Security Officer, and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

(2) On or before ~~July~~ December 1, ~~2028~~ 2026, the ~~Maryland Department of Emergency Management~~ Workgroup shall submit a final report of the findings and recommendations of the workgroup to the Governor, the Secretary of Emergency Management, the ~~Chair~~ Chairman of the Maryland Health Care Commission, the Maryland Insurance Commissioner, the State Chief Information Security Officer, and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

~~SECTION 4. AND BE IT FURTHER ENACTED, That Section 2 of this Act shall take effect July 1, 2028.~~

SECTION ~~5.~~ 2. AND BE IT FURTHER ENACTED, That~~, except as provided in Section 4 of this Act,~~ this Act shall take effect July 1, 2025. ~~Section 3 of this Act~~ It shall remain effective for a period of ~~4~~ 2 years and, at the end of June 30, ~~2029~~ 2027, ~~Section 3 of~~

this Act, with no further action required by the General Assembly, shall be abrogated and of no further force and effect.

Gubernatorial Veto Override, December 16, 2025.