

# SENATE BILL 691

S2, J3, J5

5lr0886

---

By: **Senator Hester**

Introduced and read first time: January 26, 2025

Assigned to: Finance and Education, Energy, and the Environment

---

## A BILL ENTITLED

1 AN ACT concerning

2 **Cybersecurity – Healthcare Ecosystem**

3 FOR the purpose of requiring the Maryland Health Care Commission and the Maryland  
4 Insurance Administration to include a cybersecurity expert as staff to perform  
5 certain functions and submit to the State Chief Information Security Officer a report  
6 on the cybersecurity practices and policies of certain healthcare ecosystem entities  
7 on a certain basis; requiring healthcare ecosystem entities to take certain actions  
8 related to cybersecurity, including adopting and implementing certain cybersecurity  
9 standards, undergoing a third-party cybersecurity audit on a certain basis, and  
10 reporting cybersecurity incidents to the State Security Operations Center in the  
11 Department of Information Technology; requiring the Center to notify certain  
12 agencies of a cybersecurity incident reported under this Act; requiring the  
13 Commission to convene a workgroup to review cybersecurity practices, threats,  
14 responses to disruptions, and emerging issues in the healthcare ecosystem; requiring  
15 the Commission to convene a workgroup to study and make recommendations to  
16 improve the cybersecurity of the healthcare ecosystem; and generally relating to  
17 cybersecurity and the healthcare ecosystem.

18 BY repealing and reenacting, without amendments,  
19 Article – Health – General  
20 Section 19–101  
21 Annotated Code of Maryland  
22 (2023 Replacement Volume and 2024 Supplement)

23 BY adding to  
24 Article – Health – General  
25 Section 19–113  
26 Annotated Code of Maryland  
27 (2023 Replacement Volume and 2024 Supplement)

28 BY repealing and reenacting, without amendments,

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Article – Insurance  
2 Section 1–101(a), (b), and (k)  
3 Annotated Code of Maryland  
4 (2017 Replacement Volume and 2024 Supplement)

5 BY adding to  
6 Article – Insurance  
7 Section 2–117  
8 Annotated Code of Maryland  
9 (2017 Replacement Volume and 2024 Supplement)

10 BY repealing and reenacting, without amendments,  
11 Article – State Finance and Procurement  
12 Section 3.5–101(a) and (c), 3.5–2A–01, and 3.5–301(a) and (c)  
13 Annotated Code of Maryland  
14 (2021 Replacement Volume and 2024 Supplement)

15 BY adding to  
16 Article – State Finance and Procurement  
17 Section 3.5–2A–07  
18 Annotated Code of Maryland  
19 (2021 Replacement Volume and 2024 Supplement)

20 BY adding to  
21 Article – Health – General  
22 Section 19–113(f) and (g)  
23 Annotated Code of Maryland  
24 (2023 Replacement Volume and 2024 Supplement)  
25 (As enacted by Section 1 of this Act)

26 BY adding to  
27 Article – Insurance  
28 Section 2–117(f)  
29 Annotated Code of Maryland  
30 (2017 Replacement Volume and 2024 Supplement)  
31 (As enacted by Section 1 of this Act)

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

34 **Article – Health – General**

35 19–101.

36 In this subtitle, “Commission” means the Maryland Health Care Commission.

37 **19–113.**

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

3           (2) “CYBERSECURITY” HAS THE MEANING STATED IN § 3.5–301 OF  
4 THE STATE FINANCE AND PROCUREMENT ARTICLE.

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

9           (4) “HEALTHCARE ECOSYSTEM” MEANS THE ENTITIES AND  
10 RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER TREATMENT,  
11 PAYMENT, AND HEALTH CARE OPERATIONS.

12           (5) (I) “HEALTHCARE ECOSYSTEM ENTITY” INCLUDES:

13                           1. AN ELECTRONIC DATA INTERCHANGE  
14 CLEARINGHOUSE;

15                           2. A FREESTANDING MEDICAL FACILITY, AS DEFINED IN  
16 § 19–3A–01 OF THIS TITLE;

17                           3. A HEALTH INFORMATION EXCHANGE, AS DEFINED IN  
18 § 4–301 OF THIS ARTICLE;

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

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

23           (II) “HEALTHCARE ECOSYSTEM ENTITY” DOES NOT INCLUDE:

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

26                           2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN §  
27 15–1601 OF THE INSURANCE ARTICLE.

28           (6) “ZERO–TRUST” MEANS A CYBERSECURITY APPROACH:

1                   **(I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION;**  
2 **AND**

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

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

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

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

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

15           **(C) A HEALTHCARE ECOSYSTEM ENTITY SHALL:**

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

18                   **(2) ADOPT A ZERO-TRUST CYBERSECURITY APPROACH FOR**  
19 **ON-PREMISES SERVICES AND CLOUD-BASED SERVICES;**

20                   **(3) MEET MINIMUM SECURITY STANDARDS SET BY THE COMMISSION,**  
21 **IN CONSULTATION WITH THE OFFICE OF SECURITY MANAGEMENT, FOR EACH**  
22 **OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICE BASED ON**  
23 **THE LEVEL OF SECURITY RISK FOR EACH DEVICE, INCLUDING SECURITY RISKS**  
24 **ASSOCIATED WITH SUPPLY CHAINS; AND**

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

27                   **(I) UNDERGO A THIRD-PARTY AUDIT TO EVALUATE THE**  
28 **ENTITY'S CYBERSECURITY PRACTICES AND RESOURCES BASED ON THE**  
29 **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS-SECTOR**  
30 **CYBERSECURITY PERFORMANCE GOALS OR A MORE STRINGENT STANDARD BASED**  
31 **ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FRAMEWORK;**  
32 **AND**

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

2                   1.     **THE RECOMMENDATIONS OF THE AUDIT;**

3                   2.     **THE DATE OF THE CYBERSECURITY AUDIT;**

4                   3.     **THE CYBERSECURITY FRAMEWORK USED TO**  
5 **EVALUATE THE ENTITY; AND**

6                   4.     **THE NAME OF THE THIRD PARTY THAT CONDUCTED**  
7 **THE AUDIT.**

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

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

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

19                   **(I) HOSPITALS;**

20                   **(II) FREESTANDING MEDICAL FACILITIES;**

21                   **(III) ELECTRONIC DATA INTERCHANGE CLEARINGHOUSES;**

22                   **(IV) HEALTH INFORMATION EXCHANGES; AND**

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

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

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

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

3                   **(III) THE CYBERSECURITY FRAMEWORK USED IN THE**  
 4 **CYBERSECURITY AUDIT OF THE HEALTHCARE ECOSYSTEM ENTITY; AND**

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

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

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

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

15   **Article – Insurance**

16 1–101.

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

18           (b) “Administration” means the Maryland Insurance Administration.

19           (k) “Commissioner” means the Maryland Insurance Commissioner.

20 2–117.

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

23                   **(2) “CARRIER” MEANS:**

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

25                                   **(II) A NONPROFIT HEALTH SERVICE PLAN;**

26                                   **(III) A HEALTH MAINTENANCE ORGANIZATION;**

27                                   **(IV) A DENTAL PLAN ORGANIZATION; AND**

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

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

8           (4) “HEALTHCARE ECOSYSTEM” MEANS THE ENTITIES AND  
9 RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER TREATMENT,  
10 PAYMENT, AND HEALTH CARE OPERATIONS.

11           (5) (I) “HEALTHCARE ECOSYSTEM ENTITY” MEANS:

12                           1. A CARRIER; OR

13                           2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN §  
14 15-1601 OF THIS ARTICLE.

15           (II) “HEALTHCARE ECOSYSTEM ENTITY” DOES NOT INCLUDE A  
16 GOVERNMENTAL PAYOR.

17           (6) “ZERO-TRUST” MEANS A CYBERSECURITY APPROACH:

18                           (I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION;  
19 AND

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

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

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

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

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

4           **(C) A HEALTHCARE ECOSYSTEM ENTITY SHALL:**

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

7           **(2) ADOPT A ZERO-TRUST CYBERSECURITY APPROACH FOR**  
8 **ON-PREMISES SERVICES AND CLOUD-BASED SERVICES;**

9           **(3) MEET MINIMUM SECURITY STANDARDS SET BY THE MARYLAND**  
10 **HEALTH CARE COMMISSION, IN CONSULTATION WITH THE OFFICE OF SECURITY**  
11 **MANAGEMENT, FOR EACH OPERATIONAL TECHNOLOGY AND INFORMATION**  
12 **TECHNOLOGY DEVICE BASED ON THE LEVEL OF SECURITY RISK FOR EACH DEVICE,**  
13 **INCLUDING SECURITY RISKS ASSOCIATED WITH SUPPLY CHAINS; AND**

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

16           **(I) UNDERGO A THIRD-PARTY AUDIT TO EVALUATE THE**  
17 **ENTITY'S CYBERSECURITY PRACTICES AND RESOURCES BASED ON THE**  
18 **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS-SECTOR**  
19 **CYBERSECURITY PERFORMANCE GOALS OR A MORE STRINGENT STANDARD BASED**  
20 **ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FRAMEWORK;**  
21 **AND**

22           **(II) SUBMIT TO THE ADMINISTRATION A REPORT THAT**  
23 **INCLUDES:**

- 24                   1.    **THE RECOMMENDATIONS FROM THE AUDIT;**
- 25                   2.    **THE DATE OF THE CYBERSECURITY AUDIT;**
- 26                   3.    **THE CYBERSECURITY FRAMEWORK USED TO**  
27 **EVALUATE THE ENTITY; AND**
- 28                   4.    **THE NAME OF THE THIRD PARTY THAT CONDUCTED**  
29 **THE AUDIT.**

30           **(D) ON OR BEFORE JULY 1, 2026, AND EVERY 2 YEARS THEREAFTER, THE**  
31 **ADMINISTRATION SHALL COLLECT CERTIFICATION OF A HEALTHCARE ECOSYSTEM**



1 ENTITY'S COMPLIANCE WITH THE STANDARD USED IN THE AUDIT CONDUCTED  
2 UNDER SUBSECTION (C)(4) OF THIS SECTION FOR CYBERSECURITY-RELATED  
3 POLICIES AND PROCEDURES.

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

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

10 (I) INSURERS AUTHORIZED TO SELL HEALTH INSURANCE;

11 (II) NONPROFIT HEALTH SERVICE PLANS;

12 (III) HEALTH MAINTENANCE ORGANIZATIONS;

13 (IV) DENTAL PLAN ORGANIZATIONS;

14 (V) PHARMACY BENEFITS MANAGERS; AND

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

18 (2) INFORMATION ABOUT EACH CERTIFICATION COLLECTED,  
19 INCLUDING:

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

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

23 (III) THE CYBERSECURITY FRAMEWORK USED IN THE  
24 CYBERSECURITY AUDIT OF THE HEALTHCARE ECOSYSTEM ENTITY; AND

25 (IV) THE NAME OF THE THIRD PARTY THAT COMPLETED THE  
26 CYBERSECURITY AUDIT;

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



1 (VI) A HEALTH INFORMATION EXCHANGE; AND

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

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

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

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

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

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

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

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

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

1 3.5–301.

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

3 (c) “Cybersecurity” means processes or capabilities wherein systems,  
4 communications, and information are protected and defended against damage,  
5 unauthorized use or modification, and exploitation.

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

8 **Article – Health – General**

9 19–113.

10 **(F) THE COMMISSION, IN CONSULTATION WITH THE DEPARTMENT OF**  
11 **INFORMATION TECHNOLOGY, SHALL ADOPT REGULATIONS TO IMPLEMENT**  
12 **CYBERSECURITY STANDARDS AND PROCEDURES TO:**

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

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

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

18 **(G) THE COMMISSION, IN CONJUNCTION WITH THE MARYLAND**  
19 **DEPARTMENT OF EMERGENCY MANAGEMENT, THE DEPARTMENT OF**  
20 **INFORMATION TECHNOLOGY, AND THE MARYLAND INSURANCE ADMINISTRATION,**  
21 **SHALL REGULARLY CONVENE A STAKEHOLDER WORKGROUP TO REVIEW**  
22 **CYBERSECURITY PRACTICES, THREATS, RESPONSES TO DISRUPTIONS, AND**  
23 **EMERGING ISSUES AFFECTING THE HEALTHCARE ECOSYSTEM.**

24 **Article – Insurance**

25 2–117.

26 **(F) THE ADMINISTRATION, IN CONSULTATION WITH THE DEPARTMENT OF**  
27 **INFORMATION TECHNOLOGY, SHALL ADOPT REGULATIONS TO IMPLEMENT**  
28 **CYBERSECURITY STANDARDS AND PROCEDURES TO:**

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

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

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

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

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

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

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

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

14           (5) (i) “Healthcare ecosystem entity” includes:

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

16                           2. an electronic data interchange clearinghouse;

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

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

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

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

25           (ii) “Healthcare ecosystem entity” does not include a governmental  
26 payor.

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

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

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

1 (b) The Maryland Health Care Commission shall convene a healthcare ecosystem  
2 stakeholder workgroup to study and make recommendations to improve the cybersecurity  
3 of the healthcare ecosystem in the State.

4 (c) The workgroup shall:

5 (1) identify essential capabilities;

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

8 (3) identify and map all healthcare ecosystem entities in the State;

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

11 (5) identify other issues related to cybersecurity in the healthcare  
12 ecosystem;

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

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

19 (d) (1) On or before July 1, 2026, the Maryland Health Care Commission shall  
20 submit an interim report defining the scope and contents of the State’s healthcare  
21 ecosystem to the Governor, the Secretary of Emergency Management, the Maryland  
22 Insurance Commissioner, the State Chief Information Security Officer, and, in accordance  
23 with § 2–1257 of the State Government Article, the General Assembly.

24 (2) On or before July 1, 2028, the Maryland Health Care Commission shall  
25 submit a final report of the findings and recommendations of the workgroup to the  
26 Governor, the Secretary of Emergency Management, the Maryland Insurance  
27 Commissioner, the State Chief Information Security Officer, and, in accordance with §  
28 2–1257 of the State Government Article, the General Assembly.

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

31 SECTION 5. AND BE IT FURTHER ENACTED, That, except as provided in Section  
32 4 of this Act, this Act shall take effect July 1, 2025. Section 3 of this Act shall remain  
33 effective for a period of 4 years and, at the end of June 30, 2029, Section 3 of this Act, with

1 no further action required by the General Assembly, shall be abrogated and of no further  
2 force and effect.