

# HOUSE BILL 333

S2, J3, J5

5lr0887  
CF 5lr0886

---

By: **Delegate Kerr**

Introduced and read first time: January 13, 2025

Assigned to: Health and Government Operations

---

## 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; authorizing the  
13 Maryland Department of Emergency Management to convene a workgroup to review  
14 cybersecurity practices, threats, and emerging issues in the healthcare ecosystem;  
15 requiring the Maryland Department of Emergency Management to convene a  
16 workgroup to study and make recommendations to improve the cybersecurity of the  
17 healthcare ecosystem; and generally relating to cybersecurity and the healthcare  
18 ecosystem.

19 BY repealing and reenacting, without amendments,  
20 Article – Health – General  
21 Section 19–101  
22 Annotated Code of Maryland  
23 (2023 Replacement Volume and 2024 Supplement)

24 BY adding to  
25 Article – Health – General  
26 Section 19–113  
27 Annotated Code of Maryland  
28 (2023 Replacement Volume and 2024 Supplement)

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



- 1 BY repealing and reenacting, without amendments,  
2 Article – Insurance  
3 Section 1–101(a), (b), and (k)  
4 Annotated Code of Maryland  
5 (2017 Replacement Volume and 2024 Supplement)
- 6 BY adding to  
7 Article – Insurance  
8 Section 2–117  
9 Annotated Code of Maryland  
10 (2017 Replacement Volume and 2024 Supplement)
- 11 BY repealing and reenacting, without amendments,  
12 Article – State Finance and Procurement  
13 Section 3.5–101(a) and (c), 3.5–2A–01, and 3.5–301(a) and (c)  
14 Annotated Code of Maryland  
15 (2021 Replacement Volume and 2024 Supplement)
- 16 BY adding to  
17 Article – State Finance and Procurement  
18 Section 3.5–2A–07  
19 Annotated Code of Maryland  
20 (2021 Replacement Volume and 2024 Supplement)
- 21 BY adding to  
22 Article – Health – General  
23 Section 19–113(f)  
24 Annotated Code of Maryland  
25 (2023 Replacement Volume and 2024 Supplement)  
26 (As enacted by Section 1 of this Act)
- 27 BY adding to  
28 Article – Insurance  
29 Section 2–117(f)  
30 Annotated Code of Maryland  
31 (2017 Replacement Volume and 2024 Supplement)  
32 (As enacted by Section 1 of this Act)
- 33 BY repealing and reenacting, without amendments,  
34 Article – Public Safety  
35 Section 14–101(a) and (b)  
36 Annotated Code of Maryland  
37 (2022 Replacement Volume and 2024 Supplement)
- 38 BY adding to  
39 Article – Public Safety  
40 Section 14–104.3

1 Annotated Code of Maryland  
2 (2022 Replacement Volume and 2024 Supplement)

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

5 **Article – Health – General**

6 19–101.

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

8 **19–113.**

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

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

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

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

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

21 1. AN ELECTRONIC DATA INTERCHANGE  
22 CLEARINGHOUSE;

23 2. A FREESTANDING MEDICAL FACILITY, AS DEFINED IN  
24 § 19–3A–01 OF THIS TITLE;

25 3. A HEALTH INFORMATION EXCHANGE, AS DEFINED IN  
26 § 4–301 OF THIS ARTICLE;

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

1                   **5. AN ENTITY IDENTIFIED BY THE COMMISSION IN**  
2 **REGULATIONS TO BE INCLUDED IN THE HEALTHCARE ECOSYSTEM.**

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

4                   **1. A CARRIER, AS DEFINED IN § 2-117 OF THE**  
5 **INSURANCE ARTICLE; OR**

6                   **2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN §**  
7 **15-1601 OF THE INSURANCE ARTICLE.**

8                   **(6) "ZERO-TRUST" MEANS A CYBERSECURITY APPROACH:**

9                   **(I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION;**  
10 **AND**

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

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

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

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

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

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

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

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

28                   **(3) ESTABLISH MINIMUM SECURITY STANDARDS FOR EACH**  
29 **OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICE BASED ON**

1 THE LEVEL OF SECURITY RISK FOR EACH DEVICE, INCLUDING SECURITY RISKS  
2 ASSOCIATED WITH SUPPLY CHAINS; AND

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

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

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

- 12 1. THE RESULTS AND RECOMMENDATIONS OF THE  
13 AUDIT;
- 14 2. THE DATE OF THE CYBERSECURITY AUDIT;
- 15 3. THE STANDARD USED TO EVALUATE THE ENTITY; AND
- 16 4. THE NAME OF THE THIRD PARTY THAT CONDUCTED  
17 THE AUDIT.

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

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

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

29 (I) HOSPITALS;

30 (II) FREESTANDING MEDICAL FACILITIES;

1 (III) ELECTRONIC DATA INTERCHANGE CLEARINGHOUSES;

2 (IV) HEALTH INFORMATION EXCHANGES; AND

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

5 (2) INFORMATION ABOUT EACH CERTIFICATION COLLECTED,  
6 INCLUDING:

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

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

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

12 (IV) THE NAME OF THE THIRD PARTY THAT COMPLETED THE  
13 CYBERSECURITY AUDIT;

14 (3) AN OVERVIEW OF ESSENTIAL CAPABILITIES PROVIDED BY  
15 HEALTHCARE ECOSYSTEM ENTITIES;

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

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

22 **Article – Insurance**

23 1–101.

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

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

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

27 2–117.

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

3                   (2) “CARRIER” MEANS:

4                           (I) AN INSURER AUTHORIZED TO SELL HEALTH INSURANCE;

5                           (II) A NONPROFIT HEALTH SERVICE PLAN;

6                           (III) A HEALTH MAINTENANCE ORGANIZATION;

7                           (IV) A DENTAL PLAN ORGANIZATION; AND

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

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

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

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

19                                   1. A CARRIER; OR

20                                   2. A PHARMACY BENEFITS MANAGER, AS DEFINED IN §  
21 15-1601 OF THIS ARTICLE.

22                           (II) “HEALTHCARE ECOSYSTEM ENTITY” DOES NOT INCLUDE A  
23 GOVERNMENTAL PAYOR.

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

25                           (I) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION;  
26 AND

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

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

3           **(1) ADVISE THE COMMISSIONER ON MEASURES TO IMPROVE**  
4 **OVERSIGHT OF THE CYBERSECURITY PRACTICES OF HEALTHCARE ECOSYSTEM**  
5 **ENTITIES;**

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

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

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

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

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

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

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

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

28           **(II) SUBMIT TO THE ADMINISTRATION A REPORT THAT**  
29 **INCLUDES:**

30                   **1. THE RESULTS AND RECOMMENDATIONS FROM THE**  
31 **AUDIT;**



- 1                                   **2. THE DATE OF THE CYBERSECURITY AUDIT;**
- 2                                   **3. THE STANDARD USED TO EVALUATE THE ENTITY; AND**
- 3                                   **4. THE NAME OF THE THIRD PARTY THAT CONDUCTED**
- 4 **THE AUDIT.**

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

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

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

16                                   **(I) INSURERS AUTHORIZED TO SELL HEALTH INSURANCE;**

17                                   **(II) NONPROFIT HEALTH SERVICE PLANS;**

18                                   **(III) HEALTH MAINTENANCE ORGANIZATIONS;**

19                                   **(IV) DENTAL PLAN ORGANIZATIONS;**

20                                   **(V) PHARMACY BENEFITS MANAGERS; AND**

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

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

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

27                                   **(II) THE DATE OF THE HEALTHCARE ECOSYSTEM ENTITY’S MOST**  
28 **RECENT CYBERSECURITY AUDIT;**

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

3 (IV) THE NAME OF THE THIRD PARTY THAT COMPLETED THE  
4 CYBERSECURITY AUDIT;

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

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

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

### 13 Article – State Finance and Procurement

14 3.5–101.

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

16 (c) “Department” means the Department of Information Technology.

17 3.5–2A–01.

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

19 (b) “Council” means the Maryland Cybersecurity Coordinating Council.

20 (c) “Office” means the Office of Security Management.

21 3.5–2A–07.

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

24 (2) “HEALTHCARE ECOSYSTEM” MEANS THE ENTITIES AND  
25 RELATIONSHIPS AMONG ENTITIES THAT ARE NECESSARY TO DELIVER HEALTH CARE  
26 TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS.

27 (3) “HEALTHCARE ECOSYSTEM ENTITY” INCLUDES:

- 1           **(I) A CARRIER;**
- 2           **(II) AN ELECTRONIC DATA INTERCHANGE CLEARINGHOUSE;**
- 3           **(III) A FREESTANDING MEDICAL FACILITY;**
- 4           **(IV) A HOSPITAL;**
- 5           **(V) A PHARMACY BENEFITS MANAGER;**
- 6           **(VI) A HEALTH INFORMATION EXCHANGE; AND**
- 7           **(VII) ANY OTHER ENTITY IDENTIFIED BY THE MARYLAND**  
8 **HEALTH CARE COMMISSION OR THE MARYLAND INSURANCE ADMINISTRATION IN**  
9 **REGULATIONS TO BE INCLUDED IN THE HEALTHCARE ECOSYSTEM.**

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

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

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

22           **(II) THE MANNER IN WHICH A CYBERSECURITY INCIDENT MUST**  
23 **BE REPORTED; AND**

24           **(III) THE TIME PERIOD WITHIN WHICH A CYBERSECURITY**  
25 **INCIDENT MUST BE REPORTED.**

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

29           **(4) (I) ON OR BEFORE JULY 1 EACH YEAR, BEGINNING IN 2026,**  
30 **THE OFFICE SHALL REPORT TO THE GOVERNOR, THE COUNCIL, AND, IN**  
31 **ACCORDANCE WITH § 2-1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL**

1 ASSEMBLY ON THE NUMBER OF CYBERSECURITY INCIDENTS AND TYPES OF  
2 CYBERSECURITY INCIDENTS REPORTED UNDER PARAGRAPH (1) OF THIS  
3 SUBSECTION IN THE IMMEDIATELY PRECEDING CALENDAR YEAR.

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

9 3.5–301.

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

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

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

16 **Article – Health – General**

17 19–113.

18 (F) THE COMMISSION SHALL ADOPT REGULATIONS TO IMPLEMENT  
19 CYBERSECURITY STANDARDS AND PROCEDURES TO:

20 (1) PREVENT DISRUPTIONS TO THE HEALTHCARE ECOSYSTEM;

21 (2) ENABLE THE DELIVERY OF ESSENTIAL CAPABILITIES BY THE  
22 HEALTHCARE ECOSYSTEM; AND

23 (3) SUPPORT RECOVERY FROM AN INCIDENT THAT DISRUPTS THE  
24 HEALTHCARE ECOSYSTEM.

25 **Article – Insurance**

26 2–117.

27 (F) THE ADMINISTRATION 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   **Article – Public Safety**

6 14–101.

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

8           (b) “Department” means the Maryland Department of Emergency Management.

9 **14–104.3.**

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

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

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

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

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

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

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

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

- 27                                   1. a carrier, as defined in § 2–117 of the Insurance Article;
- 28                                   2. an electronic data interchange clearinghouse;



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

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

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

6           (5) identify other issues related to cybersecurity in the healthcare  
7 ecosystem;

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

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

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

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

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

26           SECTION 5. AND BE IT FURTHER ENACTED, That, except as provided in Section  
27 4 of this Act, this Act shall take effect July 1, 2025. Section 3 of this Act shall remain  
28 effective for a period of 4 years and, at the end of June 30, 2029, Section 3 of this Act, with  
29 no further action required by the General Assembly, shall be abrogated and of no further  
30 force and effect.