

**Department of Legislative Services**  
Maryland General Assembly  
2025 Session

**FISCAL AND POLICY NOTE**  
**Third Reader - Revised**

Senate Bill 691

(Senator Hester)

Finance and Education, Energy, and the  
Environment

Health and Government Operations

---

**Healthcare Ecosystem Stakeholder Cybersecurity Workgroup**

---

This bill establishes the Healthcare Ecosystem Stakeholder Cybersecurity Workgroup to develop strategies to (1) prevent cybersecurity disruptions to healthcare ecosystem operations; (2) ensure the continuous delivery of essential healthcare ecosystem services; and (3) enhance recovery efforts of the healthcare ecosystem following a cybersecurity incident. The Maryland Health Care Commission (MHCC) and the Maryland Insurance Administration (MIA) must staff the workgroup. By January 1, 2026, the workgroup must submit an interim report and by December 1, 2026, the workgroup must submit a final report to the Governor, the General Assembly, and the heads of specified units of State government. **The bill takes effect July 1, 2025, and terminates June 30, 2027.**

---

**Fiscal Summary**

**State Effect:** MHCC and MIA can staff the workgroup using existing budgeted resources. Reimbursements for workgroup members are assumed to be minimal and absorbable within existing budgeted resources. Revenues are not affected.

**Local Effect:** The bill does not directly affect local government operations or finances.

**Small Business Effect:** Potential minimal.

---

**Analysis**

**Bill Summary:** The Healthcare Ecosystem Stakeholder Cybersecurity Workgroup must:

- identify essential capabilities required for the delivery of health care during a cybersecurity attack;

- identify functional requirements for the healthcare ecosystem to be capable of providing those essential capabilities;
- identify and map all healthcare ecosystem entities in the State against the essential health care capabilities and identified functional requirements;
- identify which healthcare ecosystem entities are needed, directly or indirectly, to provide the essential capabilities;
- develop an ecosystem cybersecurity threat and risk assessment based on the essential health care capabilities and supporting functions;
- examine cybersecurity challenges affecting the healthcare ecosystem based on the threat and risk assessment;
- review best practices for cybersecurity and processes used in the healthcare ecosystem, including specified cybersecurity guidance documents;
- make recommendations for adopting and maintaining cybersecurity regulatory standards; and
- make recommendations for ensuring that essential capabilities and supporting functions are resilient to disruption.

A workgroup member may not receive compensation as a member of the workgroup but is entitled to reimbursement for expenses under standard State travel regulations.

### **Current Law:**

#### *Cybersecurity – Generally*

Chapters 241, 242, and 243 of 2022 substantially expanded and enhanced the State's regulatory framework for State and local government cybersecurity, which is primarily governed and regulated by the Office of Security Management (OSM) (within the Department of Information Technology) and the Maryland Department of Emergency Management (MDEM). Among other things, the Acts required additional funding for cybersecurity, established leadership positions in State government for cybersecurity, codified existing cybersecurity requirements from a previous executive order, and require State and local governments to perform cybersecurity preparedness assessments with the assistance of OSM and MDEM.

#### *Maryland Health Care Commission*

MHCC is an independent commission within the Maryland Department of Health with a mission to plan for health system needs, promote informed decision making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policymakers, purchasers, providers, and the public.

MHCC does not appear to have any current statutory responsibilities related to the cybersecurity of the State's health care system.

*Maryland Insurance Administration*

MIA is an independent State agency responsible for oversight and regulation of the industry in the State. MIA's regulatory role extends to all aspects of the industry, including oversight over insurance companies, insurance producers, and other entities and insurance professionals engaged in the business of insurance, as well as the insurance products offered. Its regulatory functions include, among other things, performing actuarial evaluations; determining eligibility for and issuing certificates of authority to insurance companies; reviewing rates, policy and contract forms, manuals, and endorsements; and resolving consumer complaints about insurance coverage.

Chapter 231 of 2022 adopted National Association of Insurance Commissioners model legislation to establish data security and cybersecurity standards for insurance regulators, insurers, and other specified carriers.

**Additional Comments:** MHCC advises that hospitals and other health care entities are currently required to conduct third-party audits and to provide the results to the National Coordinator for Health Information Technology. These audits are required by federal law, and the results of the audits are considered confidential proprietary information.

---

## Additional Information

**Recent Prior Introductions:** Similar legislation has not been introduced within the last three years.

**Designated Cross File:** HB 333 (Delegate Kerr, *et al.*) - Health and Government Operations.

**Information Source(s):** Department of Information Technology; Maryland Department of Emergency Management; Maryland Department of Health; Maryland Insurance Administration; Department of Legislative Services

**Fiscal Note History:** First Reader - February 25, 2025  
km/mcr Third Reader - April 2, 2025  
Revised - Amendment(s) - April 2, 2025

---

Analysis by: Richard L. Duncan

Direct Inquiries to:  
(410) 946-5510  
(301) 970-5510