SB 691

Department of Legislative Services

Maryland General Assembly
2025 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 691 (Senator Hester)

Finance and Education, Energy, and the Environment

Cybersecurity - Healthcare Ecosystem

This bill establishes new responsibilities related to the cybersecurity of healthcare ecosystems, including staffing, reporting, auditing, and the establishment of a workgroup for healthcare ecosystem entities (as defined by the bill), the Maryland Health Care Commission (MHCC), the Maryland Insurance Administration (MIA), the Department of Information Technology (DoIT), and the Maryland Department of Emergency Management (MDEM). **The bill generally takes effect July 1, 2025; however, provisions related to adoption of regulations by MHCC and MIA take effect July 1, 2028, and provisions related to the healthcare ecosystem stakeholder workgroup terminate June 30, 2029.**

Fiscal Summary

State Effect: General fund expenditures increase by $559,500 and special fund expenditures increase by $420,800 in FY 2026 for additional staff needed by MHCC, MIA, and DoIT to implement the bill. Future years reflect annualization and the elimination of one-time costs. State-owned healthcare facilities may incur costs to meet the bill's requirements; however, this potential impact is not shown below. Revenues are not affected.

(in dollars)	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
Revenues	$0	$0	$0	$0	$0
GF Expenditure	559,500	676,600	706,500	737,800	769,400
SF Expenditure	420,800	514,400	537,000	560,800	584,900
Net Effect	($980,300)	($1,191,000)	($1,243,500)	($1,298,600)	($1,354,300)

Note: () = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

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

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Healthcare Ecosystem Entities

"Healthcare Ecosystem" means the entities and relationships among entities that are necessary to deliver treatment, payment, and health care operations. With respect to MHCC, a healthcare ecosystem entity includes an electronic data interchange clearinghouse, a freestanding medical facility, a health information exchange, a hospital, and any entity defined by MHCC in regulations to be included in the healthcare ecosystem. With respect to MIA, a healthcare ecosystem entity means an insurance carrier (as defined by the bill) or a pharmacy benefits manager. With respect to DoIT, a healthcare ecosystem entity includes all of the above listed entities.

A healthcare ecosystem entity must:

- adopt and implement cybersecurity standards that are equal to or exceed any standards adopted by MHCC or MIA, as specified;
- adopt a zero-trust cybersecurity approach for on-premises and cloud-based services;
- meet minimum security standards set by MHCC, in consultation with the Office of Security Management (OSM) within DoIT, for each operational technology and information technology device based on the level of security risk for each device, as specified;
- by January 1, 2026, and every two years thereafter, undergo a third-party cybersecurity audit that meets specified requirements and submit to MHCC or MIA, as specified, a report with information about the audit findings; and
- report, in accordance with the process established by DoIT, any cybersecurity incident, including an attack on a system being used by the healthcare ecosystem entity, to the State Security Operations Center in DoIT, as specified.

Maryland Health Care Commission and Maryland Insurance Administration

MHCC and MIA must each include on its staff at least one employee who is an expert in cybersecurity to (1) advise the chairman and members of MHCC and the Insurance Commissioner, respectively, on measures to improve oversight of the cybersecurity practices of healthcare ecosystem entities; (2) consult with OSM on cybersecurity issues related to health care regulation; and (3) represent MHCC and MIA on any workgroup,

task force, or similar entity that is focused on cybersecurity and on which representation is requested or required.

By July 1, 2026, and every two years thereafter, MHCC and MIA must collect certification of their respective healthcare ecosystem entities' compliance with the standard used in the required cybersecurity audits. By January 1, 2027, and every two years thereafter, MHCC and MIA must each submit a report to the State Chief Information Security Officer (SCISO) or the SCISO's designee that includes specified cybersecurity information about healthcare ecosystem entities in the State and related recommendations.

Effective July 1, 2028, MHCC and MIA must each, in consultation with DoIT, adopt regulations to implement cybersecurity standards and procedures to prevent disruptions to the healthcare ecosystem, enable the delivery of essential capabilities by the healthcare ecosystem, and support recovery from an incident that disrupts the healthcare ecosystem.

Department of Information Technology

OSM must consult with MHCC and MIA to establish a process for a healthcare ecosystem entity to report a cybersecurity incident, including the criteria for determining the circumstances under which an incident must be reported, the manner in which an incident must be reported, and the time period within which an incident must be reported. The State Security Operations Center must immediately notify appropriate State and local agencies of any such incident.

Beginning July 1, 2026, OSM must report annually to the Governor, the Maryland Cybersecurity Coordinating Council, and the General Assembly on the number and types of cybersecurity incidents reported in the immediately preceding calendar year. The report may not identify a healthcare ecosystem entity that reported an incident or was directly affected by an incident reported to the center.

Required Workgroups

In conjunction with MDEM, DoIT, and MIA, MHCC must regularly convene a stakeholder workgroup to review cybersecurity practices, threats, responses to disruptions, and emerging issues affecting the healthcare ecosystem.

MHCC must convene a healthcare ecosystem stakeholder workgroup to study and make recommendations to improve the cybersecurity of the healthcare ecosystem in the State. The workgroup must:

- identify essential capabilities;
- identify functional requirements for the healthcare ecosystem to be capable of providing these essential capabilities;
- identify and map all healthcare ecosystem entities in the State;
- identify which healthcare ecosystem entities are needed, directly or indirectly, to provide the essential capabilities;
- identify other issues related to cybersecurity in the healthcare ecosystem;
- review best practices for cybersecurity and processes used in the healthcare ecosystem, including specified cybersecurity guidance documents; and
- provide guidance for MHCC and MIA regarding the adoption and maintenance of cybersecurity regulatory standards.

By July 1, 2026, MHCC must submit an interim report defining the scope and contents of the State's healthcare ecosystem to the Governor, General Assembly, and other specified entities. By July 1, 2028, MHCC must submit a final report of the findings and recommendations of the workgroup to the same entities.

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 OSM (within DoIT) and 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 healthcare 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.

State Expenditures: The bill establishes new requirements and responsibilities for MHCC, MIA, DoIT, and MDEM. Except for MDEM, which can handle the bill's requirements using existing budgeted resources, each State agency requires additional staff that specialize in healthcare entity cybersecurity to handle these duties. In summary, at least eight staff are needed across all three agencies with special fund expenditures totaling at least $420,800 and general fund expenditures totaling $559,467 in fiscal 2026. The following sections include additional detail about the staff required for each agency. Notably, because cybersecurity personnel are in high demand and have specialized expertise, this analysis assumes a relatively high salary for each of the staff required to implement the bill.

In addition, the State owns and operates healthcare facilities, including inpatient psychiatric hospitals, regional institutes for children and adolescents, and developmental disabilities centers. Some of these facilities may incur costs to implement the cybersecurity technology, policies, and procedures required by the bill; however, any such impact cannot be reliably estimated at this time and is not otherwise included in this analysis.

Maryland Insurance Administration

Special fund expenditures for MIA increase by $140,262 in fiscal 2026, which assumes a 90-day start-up delay from the bill's July 1, 2026 effective date. This estimate reflects the cost of hiring one cybersecurity expert, pursuant to the bill's requirement that MIA include at least one cybersecurity expert on its staff. It includes a salary, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Position	1.0
Salary and Fringe Benefits	$132,893
Operating Expenses	7,369
Total FY 2026 MIA Expenditures	**$140,262**

Future year expenditures reflect a full salary with annual increases and employee turnover as well as annual increases in ongoing operating expenses.

Maryland Health Care Commission

Special fund expenditures for MHCC increase by $280,524 in fiscal 2026, which assumes a 90-day start-up delay from the bill's July 1, 2026 effective date. This estimate reflects the cost of hiring two cybersecurity experts to fulfill the bill's various responsibilities for MHCC, including the convening of the stakeholder workgroups required by the bill. It includes a salary, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	2.0
Salaries and Fringe Benefits	$265,786
Operating Expenses	14,738
Total FY 2026 MHCC Expenditures	**$280,524**

Future year expenditures reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses. Although the health ecosystem stakeholder workgroup ends in fiscal 2029, there is sufficient ongoing responsibilities for MHCC to warrant the retention of two regular staff after the workgroup terminates.

Indeed, MHCC advises that additional staff may be necessary due to the complex nature of the cybersecurity issues it is required to handle by the bill. The Department of Legislative Services recognizes that MHCC staff do not currently have the cybersecurity expertise required to meet the bill's requirements but advises that two staff may be sufficient to provide general cybersecurity expertise and support for the agency. Moreover, as discussed below, DoIT will have additional cybersecurity staff to assist MHCC and MIA in carrying out their duties. Nevertheless, to the extent that additional staff are needed with differing cybersecurity specializations, special fund expenditures for MHCC increase significantly as these staff salaries would be comparable to the staff discussed above.

Department of Information Technology

DoIT advises that OSM staff are currently fully subscribed and, therefore, DoIT cannot absorb the additional responsibilities established by the bill using existing staff and budgeted resources. Thus, general fund expenditures increase by $559,467 in fiscal 2026, which assumes a 90-day start-up delay from the bill's July 1, 2025 effective date. This

estimate reflects the cost of hiring (1) two cyber strategy and policy planners to establish and manage the process for health care ecosystem entities to report a cybersecurity incident and provide additional support to both MHCC and MIA in their duties; (2) two cyber defense analysts to work with healthcare ecosystem entities to collect, compile, and report on the information that must be provided to DoIT; and (3) one healthcare ecosystem cybersecurity director to oversee the new program. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	5.0
Salaries and Fringe Benefits	$522,623
Other Operating Expenses	36,844
Total FY 2026 DoIT Expenditures	**$559,467**

Future year expenditures reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses.

Small Business Effect: It is unclear whether small medical practices (*i.e.*, doctors' offices) are or will be considered healthcare ecosystem entities, as the bill allows MHCC to designate other entities through regulation that are not already included in the definition. As many medical practices are connected to hospitals and/or medical information networks, MHCC may decide that it must include them in efforts to stem cybersecurity threats to the healthcare ecosystem. To the extent they are included, they may experience significant costs to adopt and implement cybersecurity technology, policies, and procedures required by the bill, and to conduct biennial cybersecurity audits.

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: None.

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

Analysis by: Richard L. Duncan

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