MARYLAND Health Care Commission

Randolph S. Sergent, Esq., Chairman
Ben Steffen, Executive Director

2025 SESSION
POSITION PAPER

BILL NO: **HB 333**

COMMITTEE: **Health and Government Operations Committee**

POSITION: **Support as Amended**

TITLE: **Cybersecurity - Healthcare Ecosystem**

BILL ANALYSIS

HB 333 – Cybersecurity – Healthcare Ecosystem requires Maryland Health Care Commission (MHCC) to implement certain cybersecurity requirements for the healthcare ecosystem entities (entities). This includes adopting cybersecurity standards and requiring select entities undergo third-party cybersecurity audits and report certain information to MHCC. The bill requires MHCC to hire at least one cybersecurity expert to carry out specific functions and collaborate with the State Security Operations Center in the Department of Information Technology and Maryland Department of Emergency Management.

POSITION AND RATIONALE

The MHCC supports the bill as amended by the sponsor of the cross-filed bill (SB 691).[1] The MHCC has met with the sponsor to discuss select revisions to the bill. In particular, MHCC worked with the sponsor to amend the bill to establish a healthcare ecosystem stakeholder workgroup (workgroup), tasked with assessing and providing recommendations to strengthen cybersecurity resilience across the State's healthcare ecosystem.[2]

Cybersecurity is an enormous and complex issue, with growing challenges as technology continues to evolve and healthcare systems become more interconnected. The risk to the health system and patients is substantial, stemming from a wide range of external threats, including cyberattacks, data breaches, ransomware, and other malicious activities. These

[1] SB 691, Cybersecurity – Healthcare Ecosystem is available at: https://mgaleg.maryland.gov/2025RS/bills/sb/sb0691F.pdf.
[2] Digital Regulations Platform, Guiding Principles for Information and Communication Technologies Regulators To Enhance Cyber Resilience, Mary 2024. Available at: https://digitalregulation.org/guiding-principles-for-ict-regulators-to-enhance-cyber-resilience/.

threats not only jeopardize sensitive patient information but also disrupt critical healthcare services, potentially endangering lives and undermining trust in the healthcare system.

The MHCC is required by law to establish regulations that protect the privacy and security of electronic protected health information.[3] The regulations build on the federal requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[4] The MHCC believes that, given the scope and severity of cyber risks, MHCC and the Maryland Insurance Administration has an essential oversight role to play in ensuring the protection of the healthcare ecosystem.

The MHCC emphasizes that for this oversight to be effective, it must be grounded in a well-designed and thoughtful policy. The workgroup is critical to developing recommendations that will help strengthen the resilience of Maryland's healthcare ecosystem against evolving cyber risks.

The MHCC urges the Committee to support HB 333 as amended and we ask for a favorable report on HB 333.

[3] Chapters 534 and 535 (SB 723 | HB 535) of the 2011 laws of Maryland.
[4] U.S. Department of Health and Human Services, Summary of the HIPAA Security Rule available at: www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.