Maryland
Hospital Association

**House Bill 333- Cybersecurity - Healthcare Ecosystem**

**Position: *Oppose***
March 10, 2025
House Health & Government Operations Committee

**MHA Position**

On behalf of the Maryland Hospital Association (MHA) and our member hospitals and health systems across the state, we appreciate the opportunity to comment in opposition to House Bill 333. Maryland hospitals and health systems are committed to upholding the highest cybersecurity standards and safeguarding patient data. HB 333 mandates strict state-level cyber security standards and audit procedures that fail to account for the realities of data sharing across multiple states and constantly evolving technological standards.

Health care cybersecurity involves a complex, interconnected network of stakeholders—hospitals, insurers, health information exchanges, and other third parties—many of whom operate across multiple states. Several Maryland hospitals and health systems also have facilities outside the state. State-specific regulations risk creating conflicting or duplicative requirements, increasing administrative burdens, and potentially weakening cybersecurity efforts. Moreover, cyber threats are not confined by state lines.

Maryland hospitals already comply with rigorous federal cybersecurity standards designed to protect patient data and safeguard systems. The HIPAA Security Rule mandates administrative, physical, and technical safeguards to protect electronic protected health information (ePHI). Further, on Dec. 27, 2024, the U.S. Department of Health and Human Services proposed updates to HIPAA cybersecurity requirements, including mandates for written documentation of all cybersecurity policies and maintaining a comprehensive technology asset inventory. Hospitals also adhere to the National Institute of Standards and Technology (NIST) cybersecurity framework, which includes guidance on risk assessments to identify and mitigate cybersecurity threats and outlines security guidelines for access control, incident response, authentication, auditing, and cybersecurity training.

Additionally, Maryland hospitals conduct regular cybersecurity audits to identify vulnerabilities and ensure compliance. Federal regulations require ongoing HIPAA risk assessments, and hospitals proactively engage in third-party evaluations to maintain the highest cybersecurity standards. HB 333's broad incident reporting requirements could lead to excessive and unnecessary reporting of minor cybersecurity events, overwhelming state agencies and diverting

attention from truly critical threats. Over-reporting could create administrative inefficiencies that hinder timely responses to serious cyberattacks.

Since January 2020, Maryland hospitals have faced significant financial challenges, with operating expenses rising sharply. More than half of Maryland hospital systems have reported negative operating margins in most quarters over the past three years. In the third quarter of 2024, Maryland hospital system operating margins averaged just 0.3%, far below the 3% margin that experts consider necessary to sustain nonprofit health care systems. Over the past 11 years, Maryland hospital system margins have averaged only 1.6%, significantly lagging behind hospitals nationwide. Maryland's unique rate setting system limits hospitals' ability to cover unplanned costs. Mandating substantial new cybersecurity investments without a funding mechanism places additional financial strain on hospitals.

Given these concerns, MHA urges caution in adopting costly, unfunded cybersecurity mandates and advocates for a more strategic, federally aligned approach to health care cybersecurity.

For these reasons, we request a unfavorable report on HB 333.

For more information, please contact:
Jake Whitaker, Assistant Vice President, Government Affairs & Policy
Jwhitaker@mhaonline.org