JOHNS HOPKINS
UNIVERSITY & MEDICINE

TO: The Honorable Pamela Beidle, Chair
Finance

SB691
Unfavorable

FROM: Brandon Floyd
Associate Director, Maryland Government Affairs

DATE: February 27, 2025

RE: SB691 Cybersecurity - Healthcare Ecosystem

Johns Hopkins opposes **SB691 Cybersecurity - Healthcare Ecosystem**. This bill requires hospitals every two years to undergo third party evaluation of cyber practices and resources. It also requires the Maryland Health Care Commission (MHCC) submit a report, providing a general overview of cybersecurity and technologies used by hospitals. The bill also requires the MHCC to establish a process for hospitals to report cyber incidents to adopt regulations to implement cybersecurity standards.

Johns Hopkins is an international organization that cares for patients and educates millions of people. It is paramount that all who come in contact with Johns Hopkins Health System receive proper care and proper patient protections. To ensure these protections, Johns Hopkins, like many other hospitals, must remain in compliance with numerous cyber standards. The National Institute of Standards and Technology (NIST), whose mission is to promote innovation, security, and industrial competitiveness, provides cyber and privacy frameworks for organizations to remain in compliance. Hopkins is current with other frameworks and regulations including federal HIPAA and American Hospital Association (AHA) security rules. The cyber requirements in this bill would duplicate the existing cyber safety measures.

We are very concerned with the bill provisions subjecting hospitals to an audit and requiring hospitals to report on the outcome of the audit. The information disclosed during an audit is highly proprietary and would require the State to have the proper safeguards to guarantee hospital inner workings are not being exposed. Providing the actual output of the audit may open the door for unintended consequences like sharing infrastructural vulnerabilities with cyber criminals and other bad actors.

Johns Hopkins spends over $20M annually in cyber, information technology, and information system protections. These protections are to ensure patient data and other confidential important information is secure. As written, hospitals must undergo a bi-annual audit which would be incredibly costly for hospitals and do not advance protections for hospitals. Without clear financial and operational support, this bill risks creating more challenges in the ongoing effort to strengthen cybersecurity.

The bill includes third-party cybersecurity vendors into the aforementioned hospital auditing process. Cybersecurity vendors, by nature, generate revenue by providing cyber service lines and products to organizations. Bill language like “zero-trust” is ambiguous terminology that supports cyber vendors business efforts who have a financial interest in providing services to hospitals. It is unclear why a third-party vendor would need to be a part of this process, when their motives cannot be guaranteed.

Furthermore, the bill shifts control from in-house experts to external vendors. This approach does not reflect the nuanced needs of individual hospitals, with varying infrastructure. Hospitals must have the flexibility to determine the most effective protections based on their risk assessments, rather than being required to implement vendor-driven solutions that may not address their unique threats.

Cybersecurity is an evolving industry, this bill places unnecessary obstacles on hospitals are prioritizing patients – virtually and in person – every day. Accordingly, Johns Hopkins respectfully requests an **UNFAVORABLE** committee report on SB691.