TESTIMONY IN SUPPORT OF SB691- CYBERSECURITY - HEALTHCARE ECOSYSTEM

EDUCATION, ENERGY AND THE ENVIRONMENT

FEBRUARY 27, 2025

Chair Feldman, Vice Chair Kagan, and members of the Committee - thank you for the opportunity to testify in support of SB691 – Cybersecurity – Healthcare Ecosystem.

My name is Ben Yelin, and I am the Program Director for Public Policy & External Affairs at the University of Maryland Center for Health and Homeland Security. During the interim, we worked with Senator Hester on a report detailing the frequency and impact of cyber-attacks on the entities making up the healthcare ecosystem: hospitals, insurance companies, community health centers and more. An analysis of this threat landscape was sobering. Healthcare is an attractive target for cyber criminals for several reasons. First, the system contains valuable data, including patient protected health information (PHI) and personal identifying information (PII). This valuable data can be sold on the dark web for amounts far exceeding, for example, stolen credit card information. Second, the disruption to health systems is devastating in its impact to communities. It can cause downstream effects that lead to bad patient outcomes. Cyber criminals are fully aware that the potential for this catastrophic disruption may be an incentive for these healthcare entities to pay significant ransoms.

The numbers back up the nature of this threat. Nationally, there has been a 254% increase in cyber attacks on health systems over the past five years.[1] In the last year for which data were available, 3.5 million Maryland residents were impacted by hacking/IT incidents in the health care sector. With the frequency of these attacks, we've seen both significant kinetic and financial impacts to not just the health systems themselves, but to our communities. According to one recent study[2], of the 68% of hospitals impacted by ransomware attacks, 28% reported an increase in the mortality rate, 59% reported delays in procedures and tests leading to poor outcomes, and 44% reported increases in complications during medical procedures. In terms of financial impacts, a 2024 study indicated that hospitals suffering a cyber incident lost an average of $1.47 million in revenue.

What makes attacks in healthcare unique is that an attack on one part of the ecosystem has a cascading impact in the entire ecosystem. When Change Health Care, a subsidiary of UnitedHealth Group, suffered a cyber attack, the impacts were devastating, even though the attack had **no direct impact** on hospitals, providers or insurers. But because Change Health Care served as an intermediary to facilitate important functions like eligibility checks, insurance claims submissions and billing services for care centers and pharmacies, the entire ecosystem suffered. 74% of affected hospitals suffered impacts to patient care, while 94% reported a significant or substantial impact.

The breadth and depth of this problem highlights the need for a comprehensive, common-sense policy framework to protect the healthcare ecosystem in Maryland. SB691 represents such an approach.

---

[1] Data Breach Statistics, https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] 2024 Ponemon Healthcare Cybersecurity Report, https://assets.turtl.co/customer-assets/tenant%3Dteam/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report-2024%20(1).pdf

Under this bill, healthcare entities must adopt cybersecurity standards that are equal to or exceed industry standards as outlined by the National Institute of Standard and Technology (NIST) framework. To ensure compliance with these standards, entities would be subject to third party audits to evaluate the entity's practices and resources. Upon completion of these audits, entities would submit a report to the Maryland Health Care Commission (MHCC), who would aggregate the data and draft a report outlining the system's current cybersecurity posture, to be submitted to the State Chief Information Security Officer. This critical information will ensure that the State can identify gaps and issue recommendations to improve cybersecurity for the entire ecosystem. The bill also includes other valuable provisions, including incident reporting requirements, and the creation of a stakeholder workgroup to resolve outstanding issues.

SB691 is not an entirely novel approach. In 2023, the General Assembly enacted SB800/HB969 which instituted similar obligations for another critical infrastructure sector: state utilities. That bill also included a requirement that entities adopt cybersecurity standards incorporating NIST standards and guidance, a provision requiring third party cybersecurity audits, and another mandating incident reporting. While obligations under this bill and SB800/HB969 may at times seem inconvenient for individual entities, the General Assembly has recognized that when it comes to critical infrastructure, a holistic regulatory framework that makes there are no vulnerability weak points can prevent the kinetic and financial impacts of a cyber incident.

For these reasons, I respectfully request a favorable report on SB691.