FAVORABLE

TESTIMONY PRESENTED TO THE
HEALTH AND GOVERNMENT OPERATIONS COMMITTEE

SB 691
CYBERSECURITY - HEALTHCARE ECOSYSTEM

MR. CLAY HOUSE
5221 BORDEAUX CV
ELLICOTT CITY, MD 21043
February 27, 2025

Madam Chair, Mister Vice Chair, and members of the committee, good afternoon and thank you for the opportunity to testify in favor of SB 691. I am Clay House, a 20-year Maryland resident who recently retired as Vice President/Chief Information Security Officer at CareFirst.

The financial and patient safety threats of cyberattacks against the healthcare ecosystem are clear. Financially, the healthcare industry experiences the highest average cost per breach at $9.8M. [1] As bad as that is, now imagine being a patient, or a family member of a patient, needing care only to have it delayed because of a system outage somewhere in the healthcare ecosystem. These attacks do more than disrupt the business – they put lives at risk. They create barriers to care, leading to adverse healthcare outcomes and increased mortality rates. [2][3][4]

The healthcare system is not a single entity. Rather it is a collection of organizations and vendors who must continually interoperate to ensure the delivery of care and patient safety. If any key participants of this ecosystem are impacted, those impacts ripple across the other participants. There is no better example of this than the Change Healthcare incident.

Change Healthcare is a health information exchange that connects insurers, providers, Pharmacy Benefit Managers (PBMs), and hospitals supporting the flow of authorizations, eligibility, claims submission, payments, and statuses. When Change Healthcare was taken down by hackers in February of 2024, these transactions stopped for their customers impacting the entire system – even those who weren't their customers.

[1] Average cost of healthcare data breach nearly $10M in 2024: report | Healthcare Dive
[2] AHA Change Healthcare Cyberattack Having Significant Disruptions on Patient CAre, Hospital's Finances
[3] Change Healthcare cyberattack impact: Key takeaways from informal AMA follow-up survey
[4] The Devastating Impacts of Ransomware Attacks in Healthcare

An American Hospital Association (AHA) survey of hospitals highlights both the financial as well as the patient care impact noting[5]

- 74% of hospitals reported patient difficulty accessing care
- 82% of hospitals reported financial impacts – 33% impacted >50% of revenue and 60% reporting impacts of $1M+/day

Similarly, the American Medical Association (AMA) reported that in April, 2024,

- 90% of practices continued losing money
- 62% using personal funds for expenses
- 60% of practices reported challenges confirming patient eligibility
- 30% issues with authorizations.

Even though Change Healthcare was the only entity directly attacked, the impacts were felt across the nation. Hackers have noticed this leading AHA's National Advisor on Cybersecurity and Risk, John Riggi to assert "cyber adversaries have mapped our sector" targeting key central services calling it "one-stop hacking". In an interview, he supported programs such as HHS 405(d)[6] stating "we need to plan regionally for highly disruptive ransomware - incident-response plans cannot be developed in a silo".[7]

You may hear opposing testimony today that current regulations are sufficient and with new regulations overly burdensome. However current regulations are intentionally ambiguous in certain areas and lack prescriptiveness in defining controls. This has led to CISA creating the Cross-Sector Cybersecurity Performance Goals (CPGs), HHS creating the 405(d) Healthcare Organization Goals, and the proposed HIPAA Security Rule currently out for public comment.

Current regulatory processes perpetuate the silos by ignoring the risks driven by the interconnectedness of the healthcare system. As evidenced by the Change Healthcare incident, this siloed approach failed to identify and mitigate system-wide impacts.

In fairness to the regulators, it is impossible for them to identify the threats to the ecosystem and to foresee the impacts of outages. To do so requires active participation of industry stakeholders to assess the system-wide risk, identity essential services, and design for resiliency.

SB 691 takes a proactive approach to securing Maryland's healthcare ecosystem by implementing the following key measures:

- Mandates independent audits based on CISA Cross-Sector Performance Goals for Critical Infrastructure and the NIST framework
- Mandates compiling these audits into a system-wide view to assess the risk to the system as a whole vs silos
- Establishes an industry-led workgroup to review the system-wide audit results and make recommendations regarding cybersecurity controls
- Establishes an industry-led workgroup to
    - Identify essential services across the healthcare ecosystem
    - Recommend necessary steps to ensure the resiliency of these services

The threat is clear. We have empirical evidence of the financial and patient impact as well as a clear example of an attack rippling across the healthcare sector. These are not hypothetical. This will happen again.

I agree with Mr. Riggi. Criminal and Nation State actors understand that they can cripple our healthcare system by attacking common services. A n industry-led workgroup to address this vulnerability and a system-wide view of the risks is the only way to drive the resilience of our healthcare system.

Without these actions, Maryland's healthcare system remains dangerously exposed, and its citizens remain at risk. I strongly urge your support for SB 691 to protect patients, providers, and the integrity of our healthcare infrastructure.

Thank you for the opportunity to testify.

---

[5] AHA Change Healthcare Cyberattack Having Significant Disruptions on Patient CAre, Hospital's Finances
[6] Government should go on offense against healthcare cyberattacks, says AHA | Healthcare IT News
[7] Government should go on offense against healthcare cyberattacks, says AHA | Healthcare IT News