FAVORABLE

TESTIMONY PRESENTED TO THE HEALTH AND GOVERNMENT OPERATIONS COMMITTEE

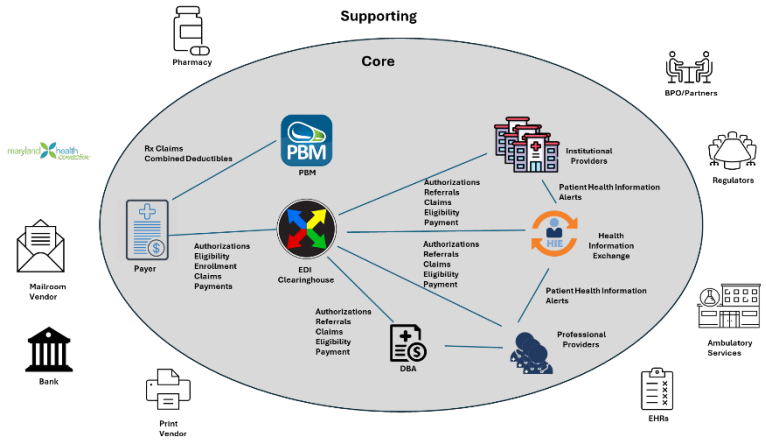
HB 333
CYBERSECURITY - HEALTHCARE ECOSYSTEM

MR. CLAY HOUSE 5221
BORDEAUX CV
ELLICOTT CITY, MD 21043
March 10, 2025

Committee Chairs, Vice Chairs, and members of the committee, good afternoon and thank you for the opportunity to testify in favor of HB 333. 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] 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]

As this diagram illustrates, 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 (EDI Clearinghouse) that connects insurers, providers, Pharmacy Benefit Managers (PBMs), and hospitals together supporting the flow of authorizations, eligibility, claims submission, payments, and statuses.

When Change Healthcare was taken down in February of 2024, these transactions stopped for their customers as well as for any other entity needing to exchange data with their customers. The impact was immediate, nationwide, and lasted for months.

---

[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% reported patient difficulty accessing care
- 82% of hospitals reported financial impacts – 33% impacted >50% of revenue and 60% reported 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. AHA's National Advisor on Cybersecurity and Risk, John Riggi, warns: "Cyber adversaries have mapped our sector – we must plan regionally—incident-response plans cannot be developed in silos".[7] The diagram above shows why the siloed approach fails because no insurer, hospital, provider, etc. operates in isolation. Effective incident response must address the interdependencies.

You will likely hear opposing testimony that entities already have incident response plans and already conduct assessments. The problem is that these are done in the silos that AHA warns are inappropriate. If these were sufficient, then the Change Healthcare attack would not have had the impact reflected in AHA's and AMA's surveys.

You will also likely hear that this work is redundant. As a former CISO, I understand the demands on resources and was assessed against multiple frameworks with overlapping requirements. To minimize the impact, we conducted our assessments concurrently mapping results to the respective criteria. The incremental effort and costs were minimal. Standardized assessments against the same benchmarks are essential for identifying system-wide risks.

HB 333 breaks the siloed approach by consolidating the required assessments into a system-wide view of risks and gaps and forms an industry-led workgroup to review the results. It also forms an industry-led workgroup to identify the essential healthcare capabilities that must function to ensure care delivery, making recommendations to mitigate the impact of an attack.

There is an adage that you can't manage what you can't see. Without HB 333, we have no visibility of the risks to the overall healthcare system. Unless we take the proactive steps outlined in HB 333, we will have similar, or potentially worse, impacts the next time the healthcare system is attacked.

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 with a system-wide view of the risks is the only way to drive the resilience of our healthcare system.

The next cyberattack is a matter of when, not if. The decision before the committee is whether we accept the status quo or we recognize its deficiencies and proactively manage the risk planning for healthcare resiliency. Without these actions, Maryland's healthcare system remains dangerously exposed, and its citizens remain at risk. I strongly urge your support for HB 333 to protect patients, providers, and the integrity of our healthcare system.

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