Comments on LD 2103 (Sponsor's Amendment)

An Act Requiring Hospitals to Adopt Cybersecurity Plans

Maine Legislature, Committee on Health and Human Services

March 2026

To: Rep. Julie McCabe, prime sponsor of LD 2103

Submitted by:
Uday Madasu, Chief Information Officer
Covenant Health, Inc., Andover, MA

Thank you for your continued, thoughtful conversations with my colleagues at Covenant Health, a health care organization that operates St. Mary's Hospital in Lewiston, Maine, and St. Joseph Hospital in Bangor.

I believe this legislation reflects genuine concern for patient safety and a recognition that cybersecurity threats to hospitals are real, consequential, and growing. However, I also want to offer important and practical concerns that I urge you to consider. Community health care providers like ours operate with constrained resources—limited staff, limited budgets, and limited access to specialized cybersecurity expertise. Any legislation this Committee advances must account for that reality if it is to achieve its intended goals.

Who We Are and Why It Matters

Community hospitals and critical access hospitals are not large academic medical centers with dedicated security operations centers, full-time cybersecurity teams, and multi-million-dollar IT budgets. We are, in many cases, the only hospital within a significant geographic area. We serve elderly populations, rural communities, and patients who have few or no alternatives for care. When our systems go down—for any reason—the impact on patient safety is immediate and direct.

Covenant has a strong commitment to patient privacy and information security, but it manages cybersecurity within the organization with a finite team. We are responsible for protecting electronic health records, medical devices, clinical workflows, and business operations. We already operate under the comprehensive requirements of HIPAA and HITECH, the Medicare Conditions of Participation, and Maine's existing health information confidentiality laws. We take those obligations seriously and invest in compliance to the best of our ability within the scope of the IT staff, budgets, and technical resources available to us.

What the Amended Bill Gets Right

The proposed amendments to LD 2103 reflect a thoughtful approach, and I want to acknowledge the elements I believe are sound policy.

Focus on Resilience and Response Planning

The bill's proposed amendments emphasize resilience, continuity of care, and incident response planning, which is exactly the right focus. The cybersecurity incident we experienced around May 2025 underscored the ongoing need to review, reassess, and improve cyber-specific downtime procedures as required by the federal HIPAA privacy and security rules. An enterprise-wide cyberattack lasting weeks is categorically different from a brief system outage. Planning for it requires deliberate, practiced, and tested preparation. The requirement in proposed § 1832(2)(B)(6) that hospitals perform annual test runs of downtime procedures—across all shifts and units—is a meaningful and reasonable requirement, although practically speaking annual security and preparedness assessments are already a best practice for complying with existing federal requirements and the expectations of cybersecurity insurance carriers.

Alignment with CISA Best Practices

Anchoring the cybersecurity plan to best practices established by federal agencies with expertise in cybersecurity in a health care context is a reasonable and adaptive approach. Rather than codifying specific technical controls that will quickly become outdated, referencing a living body of guidance allows hospitals to implement controls appropriate to their size and risk profile. While the Cybersecurity and Infrastructure Security Agency (CISA) is a recognized source for analysis of cybersecurity threats and protections, its work and guidance as applied to health care is reflected in the guidance materials issued by the US DHHS Office of Civil Rights (OCR), which enforces HIPAA and regulations adopted under HIPAA. OCR's guidance on HIPAA security rules refers to the standards established by the National Institute of Standards and Technology (NIST), which in turn draws upon the work of the CISA. Therefore, I would recommend that the bill be further amendment to substitute compliance with current HIPAA Security Rule requirements (which will doubtless evolve as research and experience continues) for compliance with CISA "best practices," which may not always align with the health care specific requirements of HIPAA rules or the guidance issued for compliance with those rules by OCR. This will avoid confusion and duplication of effort, as health care providers must directly comply with HIPAA, and CISA guidance will not always be health care specific and will overlap substantially with HIPAA requirements,

Regional Coordination Requirements

The requirement for written agreements with other hospitals and healthcare providers within 150 miles to facilitate continuity of care reflects a practical and important measure to strengthen hospitals' capacity to manage the aftermath of a cyberattack. In a cyberattack, patient diversion is not hypothetical—it is a clinical reality. St. Mary's, for example, has mutual aid agreements in place that have been recently renewed. Having pre-established arrangements in place before an incident occurs dramatically improves the safety outcomes for patients who cannot receive care from an impaired facility. This mirrors lessons learned from real-world incidents, but the bill should be revised to avoid

any implication each hospital must reach agreements with every health care provider within a 150-mile radius, which would be unduly complicated, burdensome and, effectively, would allow the non-hospital providers in the region to dictate the terms of any such agreements, since having them would be mandatory. Covenant recommends that this language provide instead that hospitals must make reasonable efforts to enter into agreements with a sufficient number of nearby hospitals and other providers to facilitate continuity of care during hospital downtime.

Confidentiality of Submitted Plans

The provision making submitted cybersecurity plans and audit results confidential is essential. A hospital's cybersecurity plan is, in effect, a roadmap of its defenses. Public disclosure of such plans would create serious security vulnerabilities and could actively assist threat actors in targeting Maine hospitals. I support this provision but urge the Committee to ensure it is airtight in the final language. As recommended by the Department in its testimony, plans should not be filed with the department as matter of course but should be provided upon request, and a clear exemption from Maine's public records law should apply to any copies submitted to and kept on file by the department.

Significant Concerns Requiring the Committee's Attention

While I support the intent of Amended LD 2103, I have serious operational and practical concerns about several provisions that, if not addressed, will impose significant burdens on resource-constrained community hospitals without materially improving patient safety.

1. Regulatory Duplication Creates Cost Without Benefit

Many of the bill's requirements duplicate obligations Maine hospitals already carry under HIPAA, HITECH, Medicare Conditions of Participation, and Maine's existing health information confidentiality statute. As a CIO, I can confirm this from lived experience: we already maintain security incident response plans, conduct security awareness training, perform contingency planning, and carry out periodic risk analyses—all required under HIPAA.

Duplicative compliance requirements do not improve security outcomes. They consume staff time, create competing documentation obligations, and divert resources away from actual security improvements. I urge you to restructure the bill to focus exclusively on the areas that genuinely go beyond existing federal mandates. Our counsel will propose some revisions to the current amended version to substitute references to HIPAA requirements for parallel but potentially conflicting or duplicative mandates and definitions.

2. Annual Independent Cybersecurity Audits Are Cost-Prohibitive for Small Hospitals

Section 1832(2)(E) requires an annual audit by an independent, certified cybersecurity auditor. Covenant hospitals in Maine already conduct such audits, but I urge you to consider what this requirement could mean, in practice, for a critical access hospital or small community hospital: an independent cybersecurity audit from a qualified firm

typically costs between $50,000 and $150,000 or more, depending on the scope and size of the organization. For a community or critical access hospital already operating on thin margins, this is not a negligible line item.

Moreover, care should be taken not to phrase this audit requirement in such a way that duplicative audits would be required – one to comply with existing federal law and insurance carrier requirements and a second one to comply with this new law.

I am not opposed to the concept of external validation. But I would ask the Committee to consider tiered compliance options. For smaller hospitals, a structured self-assessment against HIPAA-compliant frameworks, combined with periodic—rather than annual—independent audits, could achieve the same accountability goals at a fraction of the cost. Alternatively, the State could negotiate a shared audit program or grant funding mechanism to assist smaller hospitals in meeting this requirement.

3. Same-Day Paper Medical Records Access Is Operationally Infeasible

Section 1832(2)(B)(2)(a) requires hospitals to provide patients with same-day access to paper copies of medical records during a cybersecurity intrusion. I appreciate the intent—patients should not be left without access to critical information. However, this requirement as written, is operationally problematic during an active cyberattack, which is precisely the scenario in which records are most difficult to access and reproduce.

During a ransomware event, for example, electronic systems may be entirely unavailable. Producing paper copies requires functional systems, printer access, staff availability, and proper authorization controls—all of which are compromised in a major cyber incident.

What we can realistically commit to is a plan for providing access to medical information as quickly as practicable, given system status, not a hard same-day guarantee that cannot be reliably met in the scenarios that matter most. I recommend that this requirement be revised to reflect a “reasonable and practicable” standard consistent with HIPAA’s existing access timeframe provisions.

4. Continuous Vulnerability Scanning Requires Clarification and Resources

Section 1832(2)(B)(7)(c) requires hospitals to “perform continuous vulnerability scans and annual penetration testing.” I support both of these practices—they are genuinely valuable security tools. However, the word “continuous” is undefined in the bill. In a cybersecurity context, “continuous” scanning can mean automated tools running in real time, or it can be interpreted to mean recurring manual scans. For smaller hospitals without dedicated security tooling, purchasing and operating enterprise vulnerability scanning platforms represents a significant ongoing cost.

I recommend that the bill clarify this requirement, and that the State consider providing smaller hospitals access to shared vulnerability scanning resources through Maine DHHS or a state-negotiated contract, similar to how CISA provides free cybersecurity assessments to critical infrastructure entities.

5. The Maine CDC Coordination Requirement Lacks a Clear Rationale

Section 1832(2)(G) requires hospitals to coordinate with Maine CDC personnel and allow them facility access during a cybersecurity intrusion. Based on my knowledge. Maine CDC's public health mission does not naturally encompass cybersecurity incident response. During an active cyber incident, hospitals are simultaneously managing clinical operations, law enforcement coordination, cyber insurance notification, forensic investigation, and media communications. Adding coordination requirement with a state agency that lacks cybersecurity expertise could introduce confusion and distraction at a critical moment.

If the Legislature wishes to establish a state-level support function for hospital cyber incidents, I would strongly support that—but it should be housed in an agency with actual cybersecurity capability, and it should be structured as a support resource rather than a compliance obligation.

Recommendations for Strengthening the Bill

I offer the following recommendations for the Committee's consideration as the bill moves forward:

- Explicitly recognize HIPAA compliance as satisfying parallel requirements in LD 2103 to eliminate duplicative documentation burdens. Better yet, remove duplicative and potentially conflicting language where HIPAA provides adequate protection under existing law.
- Create a tiered compliance framework that scales requirements to hospital size and resources, with Critical Access Hospitals and small community hospitals receiving proportionate obligations.
- Pair mandates with state resources: establish a cybersecurity grant program, a cyber navigator program, or shared services through DHHS to help smaller hospitals meet new requirements without diverting clinical resources.
- Replace the same-day paper records requirement with a "reasonable and practicable" standard, consistent with existing HIPAA access provisions and reflective of real incident conditions.
- Clarify that "continuous vulnerability scanning" means recurring automated scanning appropriate to the hospital's size and technology environment, and consider a state-negotiated scanning resource for smaller facilities.
- Replace the Maine CDC coordination requirement with an opt-in state cybersecurity support resource housed in an appropriate agency with actual cybersecurity expertise, modeled on successful state-level programs in other jurisdictions.
- Align the bill's definitions—particularly "security incident" and "cybersecurity intrusion"—with HIPAA's established definitions to avoid confusion and potential conflict between state and federal compliance obligations.

Closing

The cybersecurity threats facing Maine's hospitals are not theoretical. They are real, they are escalating, and they directly threaten the safety of the patients we serve. Community hospitals are on the front lines of this threat every day, often with far fewer resources than larger health systems. We want to be more secure. We want to be more resilient. We want to protect our patients.

LD 2103, as amended, reflects a genuine effort to advance those goals, and I appreciate the Legislature's attention to this critical issue. With targeted amendments to address the concerns I have raised here—particularly around duplicative requirements, resource constraints for small hospitals, and the practical challenges of incident response—I believe this bill can be strengthened into legislation that meaningfully improves patient safety without creating compliance burdens that consume the very resources needed to build real security.

I am happy to answer any questions that you or your colleagues on the Health and Human Services Committee may have.

Respectfully submitted,

Uday Madasu
Chief Information Officer
Covenant Health, Inc., Andover, MA

Charles Dingman
Covenant Health
LD 2103

For the Committee's file, a copy of comments provided earlier this week to Rep. McCabe from Uday Madasu, CIO of Covenant Health