M|H|A
Maine Hospital Association

MAINE'S LEADING
VOICE FOR HEALTHCARE

TESTIMONY OF THE MAINE HOSPITAL ASSOCIATION

In Opposition To

LD 2103 - *An Act Requiring Hospitals to Adopt Cybersecurity Plans*

February 24, 2026

Senator Ingwersen, Representative Meyer, and distinguished members of the Joint Standing Committee on Health and Human Services, I am Jeffrey Austin with the Maine Hospital Association testifying **in opposition to LD 2103.** The Maine Hospital Association (MHA) represents 32 community-governed hospitals including 29 non-profit general acute care hospitals, 2 private psychiatric hospitals, and 1 acute rehabilitation hospital. In addition to acute-care hospital facilities, we also represent home health agencies, skilled nursing facilities, nursing facilities, residential care facilities, and physician practices.

Overview

Cybersecurity attacks, particularly against the healthcare sector are a serious concern.

The primary message from our members when we discussed the bill (as originally drafted) is that they are trying to address this challenge. All the hospitals on the call indicated that they both had plans and cybersecurity insurance.

The presence of insurance is important to understand. These insurance companies are agreeing to take on financial risk in the event of a cybersecurity incident. As such, the insurance policies cover many of the same topics as are found in the legislation.

Furthermore, law enforcement, particularly the FBI, are heavily involved when there is an incident. In these cases, the FBI and the insurance companies, which are exposed to financial risk, are largely in charge. Furthermore, all of your electronically connected partners have extensive demands to re-establish connections. A lot happens, from a lot of directions. And there is a fair amount of federal law on this topic, and the federal government is actively in the process of updating and expanding those requirements. So, the FBI, your insurer, your e-partners and federal law are all out there.

The state is not broadly involved in cybersecurity regulation, and we are unaware of any cybersecurity expertise at the Maine DHHS. We don't believe state mandates will make this very challenging issue any better. That said, the general "emergency preparedness" obligations that are in the State Operations Manual would apply and much of this bill is redundant to those existing requirements.

A cybersecurity attack is a crime. Hospitals that suffer these attacks are victims of crimes. Hospitals are committed to helping their communities during these difficult events. But these are crimes and they have impacts. There will be disruptions.

Federal Laws

There are many laws and regulations implicated by the topics covered by LD 2103.

CMS Emergency Preparedness (42 CFR 482.15). Hospitals must maintain **a comprehensive all-hazards emergency preparedness program** (emergency plan, policies/procedures, communication plan, training/testing program).

While this is not targeted to cybersecurity, it still applies. Whether its an earthquake, terror attack, blizzard or cybersecurity event, hospitals must have plans in place to respond.

Furthermore, the **Joint Commission** (which is the entity that determines compliance with the CMS standards) also provides guidance and is surveying (auditing) on this issue.

The **Health Insurance Portability and Accountability Act (HIPAA) Security Rule** is the central federal regulation imposing cybersecurity-related requirements on hospitals, health systems, and other "covered entities" and their business associates:

- **Scope:** Applies to any health care provider that transmits health information electronically in connection with HIPAA transactions, as well as their business associates.
- **Core Cybersecurity Requirements:** Requires covered entities to implement administrative, physical, and **technical safeguards** to ensure the **confidentiality, integrity, and availability** of electronic protected health information (ePHI).
    - Risk analysis and risk management processes
    - Access controls and authentication
    - Audit controls and activity monitoring
    - Data encryption and integrity protections (as appropriate)
    - Workforce training and sanction policies
    - Security incident procedures and documentation requirements
- **Regulatory Text:** Found in **45 CFR Part 160 and Subparts A & C of Part 164**; key standards in Subpart C (General Rules, Administrative, Physical, and Technical Safeguards).

Enforcement: The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces this Rule, including civil monetary penalties for non-compliance.

Note: As of January 2025, HHS has proposed (and published for comment) an update to **strengthen cybersecurity obligations** under the Security Rule — potentially making more explicit and stringent requirements (e.g., eliminate "addressable" flexibilities, require multi-factor authentication, inventorying, and more rigorous risk assessments).

The **Health Information Technology for Economic and Clinical Health (HITECH) Act** amends HIPAA by:

- Extending direct HIPAA Security Rule obligations and liability to **business associates.**
- Strengthening enforcement authority and increasing potential penalties for breaches of ePHI.

Under the **Cyber Incident Reporting for Critical Infrastructure Act of 2022**, the **Cybersecurity and Infrastructure Security Agency (CISA)** is required to publish regulations that will **mandate covered entities (including healthcare critical infrastructure) to report certain cyber incidents and ransom payments** within specified timeframes.

- When fully implemented, many hospitals and health systems (as critical infrastructure owners/operators) will be required to **report cyber incidents** to CISA.

Note: CIRCIA regulations are in **rulemaking and phased implementation**; final requirements are expected in coming years.

There are voluntary guidelines referenced in government policy and often used to help demonstrate compliance with federal expectations:

- **NIST Cybersecurity Framework (CSF)** — widely recognized baseline for risk management and cybersecurity processes (used in HHS/CISA guidance and federal strategy).
- **HHS & CISA Healthcare Sector Cybersecurity Implementation Guides** — support adoption of best practices in line with national strategies, but are **voluntary guidance**.

There is a lot of regulatory work happening.

And this week, the **Senate HELP Committee** is holding a mark-up of healthcare-related cybersecurity legislation.

LD 2103

We have a number of concerns with the draft.

First, it is an expensive, unfunded, administrative mandate. In addition to adopting a cybersecurity plan, hospitals must do:

1. Annual updates of the plan;
2. Annual cybersecurity trainings for all hospital employees, board members and "*organizations affiliated with the hospital*" which literally number in the hundreds if not thousands;
3. Annual "test Runs" for all hospital shifts and units;
4. Annual analyses of the criticality of IT systems and technology assets;
5. Retroactive reviews of all cybersecurity incidents since 2024;
6. Annual audits by independent experts.

Presumably, some of these provisions are already being done pursuant to federal law (rendering those portions of this bill superfluous) and insurance policy requirements. But others are seemingly new, and very expensive unfunded mandates. The bill contains no ongoing state funding to cover any of these administrative costs. Medicaid is not adjusting its reimbursement rates to cover Medicaid's share of these costs. As such, hospitals will be forced to turn to the commercial market to shift these costs.

Other mandates include:

1. Same-day access for all patients to paper copies of medical records;
2. A complaint process;
3. Written agreements with every hospital within 150 miles;
4. Coordination with labor unions.

Additionally, we think it very unwise, and unhelpful, to submit very sensitive information to DHHS. Hospitals have to provide DHHS with:

1. A copy of the plan and each annual update;
2. The results of all testing of the cybersecurity plan pursuant to section (B)(7)
3. All independent audits – including the findings of weakness.

The bill contains no funding for the state to do anything with all this information. The bill contains no provisions for what security steps the state must take to secure this very sensitive information. Imagine a file with every hospital's cybersecurity weakness identified. Why would you ever even compile such a file?

Conclusion. This is a real issue and Lewiston residents bore the brunt of two recent attacks. These attacks will continue and even intensify.

Mike Tyson, the great boxer, was once asked by a reporter about an upcoming opponent's plan to beat Tyson. Tyson's famous response was: "*Everyone has a plan until they get punched.*"

Hospitals are trying. Undoubtedly, they could do more. For cybersecurity, there probably is never enough that one can do to try and prevent, plan and respond to cybersecurity threats.

Plans and training and audits are very important. But no amount of state laws will perfectly insulate us from the negative effects of these crimes.

For these reasons, the Maine Hospital Association opposes LD 2103, and I would be happy to answer any questions that you may have.