Written Testimony in Support of LD 2103

An Act Requiring Hospitals to Adopt Cybersecurity Plans

Shaad Masood

Lewiston, Maine

February 24, 2026

Senator, Representative, and Members of the Committee:

My name is Shaad Masood. I live in Lewiston. I am an emergency department nurse by background and have worked in hospital operations and clinical informatics. I am writing in support of LD 2103. This is not primarily an IT issue. It is a patient safety issue.

What Happens When the System Goes Down

When hospital systems go down due to a cybersecurity intrusion, care does not simply slow. It fragments. Medication histories disappear from view. Imaging access is delayed. Transfers stall. Documentation becomes manual and inconsistent. Staff lose visibility into patient risk. Communication degrades across departments and across facilities. Patients lose access to their own records. In 2025, Lewiston experienced exactly that. Both Central Maine Healthcare and St. Mary's Regional Medical Center faced major cyber incidents that disrupted operations for weeks. Systems were shut down to protect data. Phone systems were affected. Downtime procedures were activated. Ambulances were diverted. Months later, it was publicly disclosed that over 145,000 individuals may have been impacted by unauthorized access to sensitive data. Inside the hospital walls, what people experience is uncertainty — uncertainty about whether the full clinical picture is visible, whether lab trends are complete, and whether the right information is reaching the right provider at the right time.

Why LD 2103 Matters

LD 2103 recognizes that a cybersecurity intrusion disrupting access to care is a patient safety event. The sponsor amendment strengthens this bill by requiring same-day paper access to records, designated patient communication contacts, structured complaint response timelines, 48-hour notification, 7-day updates, 21-day preliminary summaries, 45-day final reports, annual downtime drills across all shifts, biannual vulnerability scans, annual penetration testing, and independent cybersecurity audits. These provisions move hospitals from having policies on paper to demonstrating operational readiness.

The Core Problem: Vagueness

One of the most dangerous elements in healthcare regulation is vagueness. When expectations are broad but not measurable, what follows after a crisis is prolonged negotiation. Institutions debate definitions, impact thresholds, and reporting timelines while patients wait and staff operate under strain. LD 2103 defines what constitutes a cybersecurity intrusion impacting care, required notification timelines, required testing frequency, required auditing standards, and required public reporting milestones. Clarity protects patients.

The Governance Question

Oversight of cybersecurity readiness is fragmented. Federal reimbursement agencies evaluate compliance elements. Accreditation bodies evaluate safety standards. State licensing authorities oversee operations. Insurance carriers impose risk requirements. But no single entity is clearly accountable for statewide cybersecurity readiness as a coordinated patient safety system. Cyber events are systemic public safety risks. Hospitals may be nonprofit or private entities, but continuity of care is a public interest obligation.

Workforce Reality

Regulation alone will not solve this unless hospitals demonstrate adequate staffing of trained cybersecurity professionals, ongoing workforce education, realistic downtime simulations, paper charting competency, and clearly designated patient communication structures. Cybersecurity must be treated as a persistent threat environment, not an episodic compliance exercise.

Why This Matters in Lewiston

In Lewiston, hospital systems are access points for working families, elderly patients, behavioral health services, oncology, obstetrics, and emergency care. When systems fail, elective procedures are triaged, chronic disease management stalls, care coordination breaks down, and behavioral health continuity is disrupted. Even if no permanent injury occurs, instability itself creates harm. LD 2103 properly recognizes that cybersecurity intrusions impact access to medical care, not merely digital infrastructure.

Conclusion

This bill treats cyber incidents as patient safety events, requires measurable operational readiness, and establishes structured public accountability. In light of what Lewiston experienced in 2025, this approach is necessary. I respectfully urge the Committee to advance LD 2103. Thank you for your time and consideration.

Shaad Masood
Lewiston
LD 2103

Written Testimony in Support of LD 2103
An Act Requiring Hospitals to Adopt Cybersecurity Plans
Shaad Masood
Lewiston, Maine
February 24, 2026

Senator, Representative, and Members of the Committee:

My name is Shaad Masood. I live in Lewiston. I am an emergency department nurse by background and have worked in hospital operations and clinical informatics. I am writing in support of LD 2103. This is not primarily an IT issue. It is a patient safety issue.

What Happens When the System Goes Down

When hospital systems go down due to a cybersecurity intrusion, care does not simply slow. It fragments. Medication histories disappear from view. Imaging access is delayed. Transfers stall. Documentation becomes manual and inconsistent. Staff lose visibility into patient risk. Communication degrades across departments and across facilities. Patients lose access to their own records. In 2025, Lewiston experienced exactly that. Both Central Maine Healthcare and St. Mary's Regional Medical Center faced major cyber incidents that disrupted operations for weeks. Systems were shut down to protect data. Phone systems were affected. Downtime procedures were activated. Ambulances were diverted. Months later, it was publicly disclosed that over 145,000 individuals may have been impacted by unauthorized access to sensitive data. Inside the hospital walls, what people experience is uncertainty — uncertainty about whether the full clinical picture is visible, whether lab trends are complete, and whether the right information is reaching the right provider at the right time.

Why LD 2103 Matters

LD 2103 recognizes that a cybersecurity intrusion disrupting access to care is a patient safety event. The sponsor amendment strengthens this bill by requiring same-day paper access to records, designated patient communication contacts, structured complaint response timelines, 48-hour notification, 7-day updates, 21-day preliminary summaries, 45-day final reports, annual downtime drills across all shifts, biannual vulnerability scans, annual penetration testing, and independent cybersecurity audits. These provisions move hospitals from having policies on paper to demonstrating operational readiness.

The Core Problem: Vagueness

One of the most dangerous elements in healthcare regulation is vagueness. When expectations are broad but not measurable, what follows after a crisis is prolonged negotiation. Institutions debate definitions, impact thresholds, and reporting timelines while patients wait and staff operate under strain. LD 2103 defines what constitutes a cybersecurity intrusion impacting care, required notification timelines, required testing frequency, required auditing standards, and required public reporting milestones. Clarity protects patients.

The Governance Question

Oversight of cybersecurity readiness is fragmented. Federal reimbursement agencies evaluate compliance elements. Accreditation bodies evaluate safety standards. State licensing authorities oversee operations. Insurance carriers impose risk requirements. But no single entity is clearly accountable for statewide cybersecurity readiness as a coordinated patient safety system. Cyber events are systemic public safety risks. Hospitals may be nonprofit or private entities, but continuity of care is a public interest obligation.

Workforce Reality

Regulation alone will not solve this unless hospitals demonstrate adequate staffing of

trained cybersecurity professionals, ongoing workforce education, realistic downtime simulations, paper charting competency, and clearly designated patient communication structures. Cybersecurity must be treated as a persistent threat environment, not an episodic compliance exercise.

Why This Matters in Lewiston

In Lewiston, hospital systems are access points for working families, elderly patients, behavioral health services, oncology, obstetrics, and emergency care. When systems fail, elective procedures are triaged, chronic disease management stalls, care coordination breaks down, and behavioral health continuity is disrupted. Even if no permanent injury occurs, instability itself creates harm. LD 2103 properly recognizes that cybersecurity intrusions impact access to medical care, not merely digital infrastructure.

Conclusion

This bill treats cyber incidents as patient safety events, requires measurable operational readiness, and establishes structured public accountability. In light of what

Lewiston experienced in 2025, this approach is necessary. I respectfully urge the Committee to advance LD 2103. Thank you for your time and consideration.