Julie McCabe
207-287-1430
Julia.McCabe@legislature.maine.gov

HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

February 24, 2026

Testimony of Rep. Julie McCabe introducing

LD 2103, An Act Requiring Hospitals to Adopt Cybersecurity Plans

Before the Joint Standing Committee on Health and Human Services

Good afternoon, Senator Ingwersen, Representative Meyer and my esteemed colleagues on the Health and Human Services Committee. My name is Julie McCabe and I am honored to represent House District 93, part of Lewiston. I am here today to present **LD 2103, An Act Requiring Hospitals to Adopt Cybersecurity Plans**. The goals of this bill are straightforward; 1) to help prevent cybersecurity attacks on our hospital systems and 2) to ensure continuity of patient care when future cyberattacks inevitably occur.

This legislation was born out of two separate cyber-incidents last spring, impacting five Maine hospitals: Covenant Health's St. Mary's hospital in Lewiston and St. Joseph's hospital in Bangor as well as Central Maine Medical Center's (CMMC) hospitals in Lewiston, Bridgton and Rumford. In addition, outpatient doctor's offices were also compromised, meaning more than 400,000 patients, nearly a third of all Mainers, were impacted. These impacts exposed wide-ranging and serious breakdowns in hospitals' communication and triage protocols, which ultimately threatened patient care.

The cyberattacks on CMMC crippled basic communication services. Because networks were down, you could not place a call to your doctor's office or send a portal message. Because you could not call outpatient offices, the number of missed appointments significantly increased – including for vital preventative care like mammograms and colonoscopies. As you will read in one doctor's testimony, due to the communication disruptions, access to critical prescription medication was also undermined.

Instead of calling the office for a prescription refill as one would routinely do, you had to physically go to the office to pick up a paper script. And as we know, transportation to the doctor's office can be challenging to obtain in the best of times, notwithstanding a cyberattack. I spoke with one Auburn resident for whom this delay created life threatening circumstances where she was forced to ration her insulin medication. I remind you, this communication outage continued not for days, but weeks on end.

Not only was preventative care impacted, but other highly acute healthcare needs were not met during this period as well. For instance, oncology care for cancer patients came to a halt because the technology used for radiation treatment could not be safely deployed due to the ongoing network breach. Meaning for several weeks last June, cancer patients could not begin or continue their time-sensitive radiation treatment.

Additionally, basic imaging and monitoring technologies, that many of us take for granted and assume will always be there, were also forced offline. That meant that in the labor and delivery unit, the central fetal monitoring system which tracks newborn babies' heart rates was down. Nurses had to monitor individual patients at the bedside creating inefficiencies and forcing patients to be diverted from their local maternity unit to hospitals further away.

Patients that required CT scans to monitor aneurysms, strokes or other potentially fatal conditions could not access past imaging or get new imaging done. Because of the inability to provide these critical services, some were diverted to other hospitals. But often this diversion depended on patients' transportation access and tenacious self-advocacy. And for other patients, diversion to different healthcare facilities simply did not take place leading to further delays in care.

What is plain is that there were severe breakdowns in patient care caused by the two cyberattacks last spring. As I learned about this issue, it became clear to me that this is not a one-off or some fluke but part of a trend of bad actors increasingly targeting hospitals. Cyberattacks on hospitals have doubled since the pandemic and in one year alone, the number of exposed patient records grew from 5 million in 2024 to over 15 million in 2025.[1] Threats to our hospitals are not a problem that we can outrun.

This legislation calls for the following commonsense steps to harden hospital cybersecurity systems and strengthen post-incident response plans to ensure that patient care continues to the maximum extent possible. These include:

- Mandating annual training for all staff, conducting annual penetration testing and requiring that hospitals run "table-top" simulations of cyberattacks.
- Requiring that hospitals write cybersecurity plans and that these plans be externally audited by professionals who will be able to assess vulnerabilities.
- Requiring planning for restoring the most critical networks and medical technology based on patient acuity and census.

Measures in the bill focused on improving the post-incident response include:

- Requiring that hospitals and nearby healthcare organizations engage in mutual aid compacts and create plans together to facilitate care continuity.
- Annual training for downtime charting and annual review of downtime documents to ensure they are up to date and correspond to best medical practices.
- Annual input on the post-incident response plan from frontline workers and publicly available instructions for employees on how to file a complaint to DHHS.
- Back up communication plan for hospital personnel to enable workflows between patients and doctors, and between staff, to facilitate continuity of care.

---

[1] Susan Li, Kamalakar Surineni, Nishant Prabhakaran, Cyber-Attacks on Hospital Systems: A Narrative Review, The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice, Volume 7, 2025, Pages 30-39, ISSN 2950-3868, https://doi.org/10.1016/j.osep.2025.03.002.

- A dedicated triage line in which patients are responded to based on their level of need to ensure timely access to medications, testing, imaging and treatment.

I also included a provision by which the Maine CDC's Public Health Emergency Preparedness Medical Response team can be activated during a cyberattack if deemed necessary by the Maine CDC. Currently, the Maine CDC's Medical Response team, comprised of volunteer healthcare providers, must be invited in to aid in a public health emergency. I believe that the government should be able to assert its authority in an emergent situation to ensure patient care continues to the fullest extent possible.

Finally, we do not yet know the true impact on patient health caused by last spring's cyberattacks. We do not know how many appointments were delayed, how many prescriptions went unfilled or how many radiation treatments were missed. Accordingly, this bill calls for a full accounting of that impact as well as of future cyber incidents. We cannot expect to become better prepared and more resilient without conducting a thorough analysis of what worked and what did not.

It is easy to become inured to the data breaches of personal information that we have all experienced; they are part and parcel of modern life. However, when breaches cripple basic healthcare services and become life-threatening we cannot afford to be complacent. We must take immediate action to ensure hospitals are prepared and patient health is protected.

I thank the committee for their thoughtful consideration of this bill and am happy to answer any questions.