Testimony of Winfield Brown
Before the Joint Standing Committee on Health and Human Services
of the 132nd Maine Legislature
In opposition to LD 2103, "An Act Requiring Hospitals to Adopt Cybersecurity Plans
February 24, 2026

Senator Ingwersen, Representative Meyer, and the distinguished members of the Committee on Health and Human Services, my name is Win Brown, and I am the president of St. Mary's Health System in Lewiston. I am here to express opposition to LD 2103.

Before I begin, I do wish to thank Rep. McCabe for bringing attention to this important matter and meeting with us to discuss her initial draft and the experience of Covenant Hospitals in Maine in confronting issues such as those that this bill seeks to address. We appreciate the spirit in which Rep. McCabe brings this proposed legislation forward, out of concern for her constituents and the continuity and quality of the health care they receive – concerns which are always foremost in our minds at Covenant as well. We oppose this bill only because we respectfully submit that it would, at a practical level, impose new administrative costs and uncertainty without advancing the underlying objective of protecting patients.

Last year on Memorial Day weekend our health system was the victim of a cyber-attack. To protect our patients and their data, we immediately turned off our electronic medical record and switched over to paper charting. Our staff were trained ahead of time to do this, and they did this well. Over the course of two weeks, we worked to eliminate the threat from our system and were able to turn our electronic medical record back on.

First and foremost, during the attack we were focused on our patients. As a result, our patients were able to access information, access care, keep their appointments, get necessary referrals and have prescriptions refilled. We continued to provide care, phone lines and facilities remained open and staff communicated with patients to coordinate care.

That said, the cyber-incident was very disruptive, no doubt about it. Responding required a tremendous amount of staff time, expensive consultants, and anxiety and stress. It was definitely challenging for patients, as well. Every day we worked 24/7 to resolve the problem, always with a focus on our patients and our staff.

So, if there is anyone who would like to see the likelihood of a cyber-incident reduced to zero, it is me. The thing is, we at St. Mary's and at our parent organization, Covenant Health, took all of the protective and planning measures required by existing federal law prior to our cyber-security incident, and the attack still took place. We did these things because they are already required by federal law and we believed they were the right things to do. Simply put, HIPAA already requires hospitals to have in place stringent administrative, technical and physical security safeguards to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered [hospital] . . . creates, receives, maintains, or transmits"; to "protect against any reasonably anticipated threats or hazards to the security or integrity of such information'; to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [HIPAA]"; and to "ensure compliance with [the HIPAA Security Rule]." 45 C.F.R. Section 164.306(a)(1)-(4).

We respectfully submit that no practical benefit would be gained by a state statute mandating essentially the same plans as the federal government already requires, while introducing uncertainty and duplication of effort arising from differences between the federal and state provisions. There is no need to impose reporting requirements, as there already is a federal requirement in place for reporting. Indeed, we did just that when we were the victims of such an attack.

While in general this bill seeks to impose state requirements that in many instances are already required by the federal government, parts of the bill contain provisions that would be new and not covered directly by federal law. I want to share my concerns about one of the most troubling of these new proposed requirements of the bill.

In part 2(B)(2)(a)-(c), three new requirements are laid out, all under the rubric of "backup communication response." While laudable, two of these provisions impose overly burdensome requirements.

- First, this mandates that hospitals being attacked by a third-party must have a process in place by which patients will be provided same day access to paper

copies of medical records. If the hospital, as we did, has been forced to turn off access to its electronic medical records in order to protect all its patients, it will not be able to pull up copies to share with its patients. Forcing the hospital to turn on its records to comply with this requirement would put at risk the entire database and possibly cause greater harm to all patients. So, while the goal of this is laudable and the desire for it is understandable, the requirement would do more harm than good.

- Second, the bill imposes a complaint process for patients who are experiencing challenges to receive a response within mandated timeframes. Of course, this sounds reasonable, but based on having to experience an actual cyber-attack, I can assure you that everyone on the care team is focused on providing care while the attack is happening, and everyone else is focused on supporting the care team and restoring full services and access. Having to be governed by a state-mandated complaint response system under such circumstances will take away from efforts to resolve the underlying issues. Again, this will do more harm than good.

- The third provision, which mandates that hospitals integrate into the hospital's electronic medical record all manually charted records in a "timely" manner, is unnecessary. This is not a harmful requirement like the two items already noted, but it is not necessary. After our electronic medical record became available for us to use last summer, we promptly integrated the paper charts into our electronic medical record because we knew it was necessary for ensuring quality patient care. I cannot imagine any hospital not doing this, and it is consistent with existing documentation standards enforced by payors and licensing and certification authorities. Mandating this in LD 2103 is unnecessary.

I am here to answer any questions you might have.