Hello Senator Ingwersen, Representative Meyer, and distinguished members of the Health and Human Services committee. My name is Dr. Cassie Dove, and I am a resident of West Baldwin, Maine, as well as a cybersecurity instructor at the University of Southern Maine.

A few weeks ago, Ms. McCabe and I discussed with a few other members what happened in Lewiston at the Central Maine Medical Center last year. Unfortunately, I was one of those patients in the Emergency Room after a fall, and I was unable to obtain an MRI. While this was not a life-or-death emergency, we had to move to another facility much farther from my home. In addition, there was no way for hospital personnel to obtain any previous information on my visits or health issues.

As a disabled veteran, this can be distressing, as I know Central Maine Medical Center can view veterans' files and vice versa. Many other hospitals do not have timely access. Not everyone is able to travel further distances away from their local medical institution to receive necessary care. While I was able to do so, hospitals need plans in place to ensure patients are able to access both healthcare AND the transportation to get there, when they are unable to provide it due to downed systems.

I was informed by medical personnel that there was no previous access to records for that entire month, June-July 2025. The Central Maine Medical Center and its other health care institutions did not have access for all patients during that outage. While the problem is well known that CMMC had this issue with their patient records being exposed, CMMC instead chose to shut down their entire patient record network to protect other patients' information from being leaked further. Letters were sent to patients in the network, and they were told that CMMC was doing everything it could to protect patients' information.

As a cybersecurity instructor at the University of Southern Maine, this is one of those scenarios that are dangerous, and we dread every day as CS professionals. While many institutions have cyber education for new employee hires, there needs to be more training for all employees every year. All people who use the electronic health record systems for patient care, including other providers, will need to be educated on how to always manage patient records securely. Especially AFTER a security breach, like the one that happened at CMMC last year.

Not only does this training need to take place yearly for all personnel, but there needs to be a solid backup system and plan, so all health care professionals can access patients' data without putting their own workstation at risk. This type of system will need to be a standalone system that will not tie into the mainframe that may have been exposed until restoration is completed. Lessons learned should be shared, and all actions should be reported to all shareholders as well as all patients, so they all understand the records are now safe and no longer exposed to unethical personnel.

A cybersecurity plan is essential for all medical centers, as well as audits performed to ensure pen testing, security protocols, as well as all training is performed annually as described in LD 2103.

Thank you for your time and I welcome any questions.

Dr. Cassie Dove