L.D. 2103

Date: (Filing No. H-)

HEALTH AND HUMAN SERVICES

Reproduced and distributed under the direction of the Clerk of the House.

STATE OF MAINE

HOUSE OF REPRESENTATIVES

132ND LEGISLATURE

SECOND REGULAR SESSION

COMMITTEE AMENDMENT " " to H.P. 1418, L.D. 2103, "An Act Requiring Hospitals to Adopt Cybersecurity Plans"

Amend the bill by striking out everything after the enacting clause and inserting the following:

'**Sec. 1. 22 MRSA §1832,** as enacted by PL 2011, c. 254, §1 and affected by §2, is repealed and the following enacted in its place:

§1832. Safety and security in hospitals; cybersecurity

1. Safety and security plan. A hospital licensed under this chapter shall, on an annual basis, adopt a safety and security plan to protect the patients, visitors and employees of the hospital from aggressive and violent behavior. The safety and security plan must include a process for hospitals to receive and record incidents and threats of violent behavior occurring at or arising out of employment at the hospital. The safety and security plan must prohibit a representative or employee of the hospital from interfering with a person making a report as provided in the plan.

2. Cybersecurity plan. A hospital licensed under this chapter shall adopt a cybersecurity plan. The cybersecurity plan must be consistent with best practices established by the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency; the United States Department of Commerce, National Institute of Standards and Technology; and the Healthcare and Public Health Sector Coordinating Council or its successor organization. The cybersecurity plan must be consistent with applicable federal laws and regulations, including the federal Health Insurance Portability and Accountability Act of 1996. The hospital shall review the cybersecurity plan at least once per year and, if requested by the department, immediately submit the most current plan to the department.

A. As used in this subsection, the following terms have the following meanings.

(1) "Cybersecurity" means the process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use, of information that is stored, accessed or transferred from an electronic device to an external recipient.

(2) "Cybersecurity intrusion" means an unwanted intrusion into a computer system that impacts patient care, protected health information or hospital security.

(3) "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in a computer system.

(4) "Security incident response plan" means the part of a cybersecurity plan adopted by a hospital detailing how a hospital employee must report suspected or known security incidents and how a hospital will respond to suspected or known security incidents.

B. The cybersecurity plan must include, at a minimum:

(1) A provision for the timely notification, by electronic means and by mail, of a cybersecurity intrusion to appropriate parties, including, but not limited to, law enforcement agencies, patients, municipalities, state regulators, media and hospital employees. The hospital shall include in all public communications related to the cybersecurity intrusion information regarding patient rights and the contact information for registering a patient complaint;

(2) A backup communication response provision that ensures continuity of care for patients in the event of a disruption of hospital computer systems caused by a cybersecurity intrusion or a natural or human-made disaster and that includes a complaint process for patients who are experiencing challenges accessing medical care and a system to triage patient complaints, including:

(a) A requirement that emergent concerns receive a response within 48 hours of the submission of the complaint and that nonemergent concerns receive a response within 7 days of the submission of the complaint. For the purposes of this division, "emergent concern" means a condition that requires immediate attention or action due to its serious or life-threatening nature; and

(b) A requirement for the timely management of complaints related to prescriptions;

(3) A provision requiring that all manually charted records be timely integrated into the hospital's electronic record system;

(4) A provision to ensure proper triage of hospital services in the event of a disruption of hospital computer systems, including:

(a) A provision for the appropriate triage of all hospital services, including elective procedures, based on hospital capacities and patient needs;

(b) A provision for the diversion of hospital services as necessary, including assisting patients in arranging emergency and nonemergency transportation services to access health care not available at the hospital as a result of the cybersecurity intrusion; and

(c) A requirement for the hospital to enter into written agreements with a sufficient number of other health care providers to facilitate continuity of care for patients during the disruption;

(5) A written security incident response plan documenting how hospital employees are to report suspected or known security incidents and how the hospital will respond clinically to suspected or known security incidents. The security incident response plan must include provisions detailing how hospital employees can effectively communicate with one another and with outside medical providers in the event hospital electronic systems are not operative. The security incident response plan must be made available to all hospital employees;

(6) A provision for, at a minimum, annual cybersecurity training for hospital employees, hospital board members and organizations affiliated with the hospital, including new employee and annual training for all hospital employees who use electronic health record systems for patient care. The training must include information relating to the management of patient records in the event of unplanned downtime of the hospital's electronic health record system, including training on paper charting;

(7) A requirement that the hospital perform an annual test involving all hospital shifts and units of downtime procedures for the hospital's cybersecurity plan and a requirement that all downtime paperwork be reviewed and updated at the time of the annual test. This requirement is waived if the hospital experiences a security incident during the prior year and conducted a post-incident review in accordance with subparagraph (11). For the purposes of this subparagraph, "downtime paperwork" means documentation a hospital maintains to ensure care can be documented manually when a hospital's computer systems are not operative;

(8) Written procedures for testing and revising the cybersecurity plan, including:

(a) A requirement that the hospital perform an annual review of the criticality of its information systems and technology assets to determine the priority for restoration;

(b) A requirement that the hospital perform a tabletop simulation of a security incident resulting in the disruption of hospital computer systems; and

(c) A requirement that the hospital perform continuous vulnerability scans and annual penetration testing to identify network vulnerabilities;

(9) A provision for timely restoration of communication with the state-designated statewide health information exchange described in section 1711-C, subsection 18. This subparagraph does not impose additional duties, standards or regulatory obligations on the state-designated statewide health information exchange;

(10) A provision requiring the review of the hospital's response to any security incidents that have taken place at the hospital since January 1, 2024. As part of the review, the hospital shall produce a report that includes a part that describes the lessons learned from the security incidents and a description of any actions taken by the hospital to prevent future security incidents and to mitigate the harm caused by similar events. The report must include information regarding the involvement of security consultants, law enforcement and cybersecurity insurance providers; and

(11) A provision requiring the hospital to conduct a timely post-incident review of any security incident experienced by the hospital. The review must include an

evaluation of the effectiveness of the hospital's cybersecurity plan and timely revision of any required updates to the plan.

C. The cybersecurity plan must be developed and maintained with the input of an annual working group convened by the hospital that includes health care workers employed by the hospital and those workers' labor unions.

D. A hospital licensed under this chapter shall maintain physical copies of all forms and other paperwork required to maintain continuity of care during a disruption of hospital computer systems.

E. A hospital licensed under this chapter shall annually submit the hospital's cybersecurity plan to an audit by an independent, certified cybersecurity auditor or certified cybersecurity expert to determine the adequacy of the cybersecurity plan and identify any necessary improvements to the plan and processes. The hospital shall submit a high-level summary of the results of each audit to the department upon the request of the department.

F. A hospital licensed under this chapter shall make available to hospital employees and the public information regarding how to file a complaint under the complaint process developed pursuant to paragraph B, subparagraph (2), including by posting this information in public areas of the hospital.

G. In the event of a cybersecurity incident, a hospital licensed under this chapter shall coordinate with personnel from the Maine Center for Disease Control and Prevention and shall allow such personnel access to the hospital facility. The State shall indemnify and hold the hospital harmless for the actions of state personnel related to the cybersecurity incident response.

H. A cybersecurity plan submitted to the department under this section and the high-level summary of the results of an audit submitted to the department in accordance with paragraph E are confidential only to the extent that release of information contained in the record could reasonably be expected to jeopardize the physical safety of government personnel or the public, as determined by the department.

3. Statutory construction. This section may not be construed or applied to be less restrictive than or in a manner that conflicts with applicable federal law and related regulations. This section may be construed or applied to be more restrictive than federal law.

4. Effective date. This section takes effect January 1, 2027.'

Amend the bill by relettering or renumbering any nonconsecutive Part letter or section number to read consecutively.

SUMMARY

This amendment replaces the bill. The amendment requires hospitals, beginning January 1, 2027, to adopt a cybersecurity plan that is consistent with best practices established by the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency; the United States Department of Commerce, National Institute of Standards and Technology; and the Healthcare and Public Health Sector Coordinating Council or its successor organization. The amendment establishes

requirements regarding testing and revising such plans, training of employees, post-incident review, auditing and confidentiality.