



132nd MAINE LEGISLATURE

SECOND REGULAR SESSION-2026

Legislative Document

No. 2103

H.P. 1418

House of Representatives, January 7, 2026

An Act Requiring Hospitals to Adopt Cybersecurity Plans

Approved for introduction by a majority of the Legislative Council pursuant to Joint Rule 203.

Reference to the Committee on Health and Human Services suggested and ordered printed.

A handwritten signature in cursive script that reads "Robert B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative MCCABE of Lewiston.

Cosponsored by Representatives: ABDI of Lewiston, FAIRCLOTH of Bangor, LAJOIE of Lewiston, LEE of Auburn, WEBB of Durham.

1 **Be it enacted by the People of the State of Maine as follows:**

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3 repealed and the following enacted in its place:

4 **§1832. Safety and security in hospitals; cybersecurity**

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

12 **2. Cybersecurity plan.** A hospital licensed under this chapter shall adopt and submit
13 to the department a cybersecurity plan. The hospital shall update the plan at least once per
14 year and submit the updated plan to the department. The department shall keep the plan
15 on file.

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

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

20 (2) "Cybersecurity intrusion" means an unwanted intrusion into a computer
21 system.

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

23 (1) A provision for the timely notification of a cybersecurity intrusion to
24 appropriate parties, including, but not limited to, law enforcement agencies,
25 hospital patients, health care providers, municipalities and state regulators;

26 (2) A backup communication response provision that ensures continuity of care for
27 patients, including providing for the protection of patients' rights;

28 (3) A provision for triage based on system capacities and patient needs to ensure
29 continuity of care;

30 (4) A provision for the diversion of hospital services, including the provision of
31 transportation services, and regional partnerships with other hospitals to ensure
32 continuity of care;

33 (5) A complaint process for patients who, as a result of a cybersecurity intrusion,
34 are experiencing challenges accessing medical care; and

35 (6) A provision for cybersecurity training for hospital employees and board
36 members and organizations affiliated with the hospital.

37 A hospital licensed under this chapter shall annually perform a test run of the cybersecurity
38 plan to assess the implementation of the plan.

39 **3. Rules.** The department may adopt routine technical rules as defined in Title 5,
40 chapter 375, subchapter 2-A to implement this section.

Sec. 2. 22 MRSA §8752, sub-§4-A, ¶C-1, as enacted by PL 2025, c. 305, Pt. B, §4, is amended to read:

C-1. The suicide of a patient within 48 hours of receiving health care services in a health care facility; and

Sec. 3. 22 MRSA §8752, sub-§4-A, ¶D, as amended by PL 2025, c. 305, Pt. B, §4, is further amended to read:

D. Other serious and preventable events as identified by using the most recent version of a nationally recognized quality forum; and

Sec. 4. 22 MRSA §8752, sub-§4-A, ¶E is enacted to read:

E. Cybersecurity intrusions, as defined in section 1832, subsection 2, paragraph A, subparagraph (2), impacting patients' access to medical care.

SUMMARY

This bill requires hospitals to adopt and submit to the Department of Health and Human Services a cybersecurity plan that includes provisions related to notifications, communications, continuity of care for patients and patient complaint processes in the event of a cybersecurity intrusion. The cybersecurity plan must include a provision for cybersecurity training for hospital employees and board members and organizations affiliated with the hospital. The bill also adds cybersecurity intrusions impacting patients' access to medical care to the definition of "sentinel event" in the laws governing required reporting of sentinel events.