# MAINE STATE LEGISLATURE

The following document is provided by the

**LAW AND LEGISLATIVE DIGITAL LIBRARY**

at the Maine State Law and Legislative Reference Library

http://legislature.maine.gov/lawlib


Reproduced from electronic originals

(may include minor formatting differences from printed original)

# LAWS

## OF THE

# STATE OF MAINE

**AS PASSED BY THE**

**ONE HUNDRED AND THIRTY-SECOND LEGISLATURE**

**SECOND REGULAR SESSION**
**JANUARY 7, 2026 to APRIL 29, 2026**

**THE GENERAL EFFECTIVE DATE FOR**
**SECOND REGULAR SESSION**
**NONEMERGENCY LAWS IS**
**JULY 29, 2026**

**PUBLISHED BY THE REVISOR OF STATUTES**
**IN ACCORDANCE WITH THE MAINE REVISED STATUTES,**
**TITLE 3, SECTION 163-A, SUBSECTION 4.**

**Augusta, Maine**
**2026**

~~If a person required to report notifies either the person in charge of the institution, agency or facility or the designated agent, the notifying person shall acknowledge in writing that the institution, agency or facility has provided confirmation to the notifying person that another individual from the institution, agency or facility has made a report to the department. The confirmation must include, at a minimum, the name of the individual making the report to the department, the date and time of the report and a summary of the information conveyed. If the notifying person does not receive the confirmation from the institution, agency or facility within 24 hours of the notification, the notifying person immediately shall make a report directly to the department.~~

This subsection may not be construed to prohibit a person required to report under this subsection from seeking consultation to determine if a report to the department is required.

An employer may not take any action to prevent or discourage an employee from making a report.

**Sec. 5. 22 MRSA §4011-A, sub-§1-A,** as enacted by PL 2007, c. 139, §2, is repealed.

**Sec. 6. 22 MRSA §4011-A, sub-§2,** as amended by PL 2015, c. 117, §2, is repealed and the following enacted in its place:

**2. Required report to district attorney.** When a mandated report is made to the department under subsection 1, the department shall report to the appropriate district attorney's office any instance in which the reported child abuse or neglect or suspicious child death is caused by a person not responsible for the child. A person required to report under subsection 1 may also report directly to the appropriate district attorney's office.

**Sec. 7. 22 MRSA §4011-A, sub-§4,** as amended by PL 2007, c. 586, §13, is repealed.

**Sec. 8. 22 MRSA §4011-A, sub-§4-A** is enacted to read:

**4-A. Mental health treatment.** When a licensed mental health professional is required to report under subsection 1 and the reportable information comes from the treatment of a person responsible for the child or the child who is the subject of the report, the licensed mental health professional may include in the licensed mental health professional's report a request that the department consider the impact of any resulting investigation or action on the licensed mental health professional's ongoing treatment of the person who is the subject of the report. The department shall take reasonable steps to engage with the licensed mental health professional to avoid impairing, to the extent possible, the licensed mental health professional's ongoing ability to treat the person who is the subject of the report.

**Sec. 9. 22 MRSA §4011-A, sub-§8,** as enacted by PL 2015, c. 274, §7, is repealed.

**Sec. 10. 22 MRSA §4011-A, sub-§9,** as enacted by PL 2015, c. 407, §1, is amended to read:

**9. Training requirement.** A person required to make a report under subsection 1 shall complete at least once every ~~4~~ 2 years mandated reporter training approved by the department.

**Sec. 11. 22 MRSA §4011-A, sub-§10** is enacted to read:

**10. Authority of licensing board.** This section may not be construed to limit the authority of an appropriate licensing board to take action related to a violation of this section.

**Sec. 12. 22 MRSA §4011-C, sub-§2,** as enacted by PL 2025, c. 353, §5, is amended to read:

**2. Report.** When a health care provider suspects that an infant has been abused or neglected, the provider shall report to the department in accordance with section 4011-A, subsection 1, paragraph ~~A~~ A-1. If the infant has a family care plan developed under section 4004-C, subsection 2, a copy of the family care plan must accompany the report.

**Sec. 13. 22 MRSA §4011-C, sub-§3,** as enacted by PL 2025, c. 353, §5, is amended to read:

**3. Definition.** For purposes of this section, "health care provider" means a person ~~described in section 4011-A, subsection 1, paragraph A, subparagraphs (1) to (10), (15), (17) to (20) and (22)~~ licensed under Title 32, chapter 31, 36, 48, 56, 81 or 83 or any person who assists in the delivery or birth of a child for compensation, including, but not limited to, a midwife.

**Sec. 14. 22 MRSA §4021, sub-§3, ¶C,** as amended by PL 2023, c. 248, §3, is further amended by amending the first blocked paragraph to read:

~~Violation of this paragraph subjects any person involved in the violation, including individual school personnel, to the penalty provided in section 4009.~~ This section does not apply to out-of-home abuse and neglect allegations as covered under subchapter 18.

See title page for effective date.

## CHAPTER 668

## H.P. 1418 - L.D. 2103

### An Act Requiring Hospitals to Adopt Cybersecurity Plans

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

**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.

See title page for effective date.

## CHAPTER 669

## H.P. 1405 - L.D. 2090

### An Act to Modify Probationary Periods for Dispatchers

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

**Sec. 1. 5 MRSA §7051, sub-§5,** as corrected by RR 2023, c. 1, Pt. B, §21 and affected by §50, is amended to read:

**5. Probationary period; permanent appointments.** All original appointments to the classified service and all subsequent promotional appointments within the classified service must be for a probationary period. The duration of the probationary period, which may not be for less than 6 months in any case, is determined by the officer in consultation with the director or commissioner of the agency, ~~but in no case may it be for less than 6 months~~ except that in the case of dispatchers, the probationary period may be extended for more than 6 months as determined by the director or commissioner of the agency, unless otherwise provided for in a collective bargaining agreement. An agency that employs a dispatcher shall adopt a written policy regarding the length of the probationary period for dispatchers and disclose the policy to the dispatcher at the time of hire. For the purposes of this subsection, "dispatcher" has the same meaning as in section 18313, subsection 1.

A. An employee during the probationary period must be reviewed at the end of the employee's 3rd month of employment by the employee's supervisor. The supervisor and the employee shall mutually discuss the job tasks and the performance of the employee, including any necessary improvements.

B. An employee during the probationary period must be included in the payroll of the department in which the employee has been hired at the time of the commencement of the employee's duties. An employee during the probationary period must be compensated in the same manner as a permanent full-time employee, as long as the employee has been hired in accordance with all applicable laws and procedures.

C. During the probationary period, an employee is not entitled to a pre-disciplinary hearing and may be dismissed, suspended or otherwise disciplined without cause. Dismissal, suspension or any other disciplinary action against an employee during the probationary period is not subject to the grievance and arbitration provision of the collective bargaining agreement.

**Sec. 2. 30-A MRSA §2701, first ¶,** as amended by PL 1993, c. 744, §15, is further amended to read:

Except as specifically provided otherwise by charter or ordinance, any reference to cause and hearing in this Part only applies to an employee who has completed a reasonable probation period established by the municipality. Periods of probation may not exceed 6 calendar months or the length of time in effect in a municipality on January 1, 1984, whichever is greater, except in the case of police officers, who upon being hired shall complete an employment probationary period that lasts for at least one year after graduation from the Maine Criminal Justice Academy or the date the board waives the basic training requirement~~.~~, and except in the case of dispatchers, who upon being hired shall complete an employment probationary period that lasts for at least 6 months except as otherwise provided for in a collective bargaining agreement. An agency that employs a dispatcher shall adopt a written policy regarding the length of the probationary period for dispatchers and disclose the policy to the dispatcher at the time of hire. For the purposes of this paragraph, "dispatcher" has the same meaning as in Title 5, section 18313, subsection 1.

See title page for effective date.

## CHAPTER 670

## H.P. 1396 - L.D. 2081

### An Act to Provide Health Care Cost Reimbursement for Retired Law Enforcement Canines

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