APPROVED | CHAPTER
APRIL 6, 2014 | 528
BY GOVERNOR | PUBLIC LAW

STATE OF MAINE

IN THE YEAR OF OUR LORD

TWO THOUSAND AND FOURTEEN

H.P. 1246 - L.D. 1740

An Act To Amend Laws Relating to Health Care Data

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

Sec. 1. 22 MRSA §1711-C, sub-§6, ¶F-3 is enacted to read:

F-3. To the Maine Health Data Organization as required by and for use in accordance with chapter 1683. Health care information, including protected health information, as defined in 45 Code of Federal Regulations, Section 160.103 (2013), submitted to the Maine Health Data Organization must be protected by means of encryption;

Sec. 2. 22 MRSA §8702, sub-§1-B is enacted to read:

1-B. Business associate. "Business associate" has the same meaning as under 45 Code of Federal Regulations, Section 160.103 (2013).

Sec. 3. 22 MRSA §8702, sub-§2-A is enacted to read:

2-A. Covered entity. "Covered entity" has the same meaning as under 45 Code of Federal Regulations, Section 160.103 (2013).

Sec. 4. 22 MRSA §8702, sub-§4-B is enacted to read:

4-B. HIPAA. "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996.

Sec. 5. 22 MRSA §8702, sub-§8-C is enacted to read:

8-C. Protected health information. "Protected health information" includes:

A. "Protected health information" as defined in 45 Code of Federal Regulations, Section 160.103 (2013);

B. Individually identifiable health information:

(1) That is demographic information about an individual reported to the organization that relates to the past, present or future physical or mental health or condition of the individual;

(2) That pertains to the provision of health care to an individual; or

(3) That relates to the past, present or future payment for the provision of health care to an individual and that identifies, or with respect to which there is a reasonable basis to believe the information could be used to identify, the individual; and

C. "Health care information" as defined in section 1711-C, subsection 1, paragraph E.

Sec. 6. 22 MRSA §8705-A, first ¶, as enacted by PL 2003, c. 659, §2, is amended to read:

The board shall adopt rules to ensure that payors and providers file data as required by section 8704, subsection 1; that users that obtain health data and information from the organization safeguard the identification of patients and health care practitioners as required by section ~~8707~~ 8714, subsections ~~1 and~~ 2, 3 and 4; and that payors and providers pay all assessments as required by section 8706, subsection 2.

Sec. 7. 22 MRSA §8705-A, sub-§3, as amended by PL 2007, c. 136, §4, is further amended to read:

3. Fines. The following provisions apply to enforcement actions under this section except for circumstances beyond a person's or entity's control.

A. When a person or entity that is a health care facility or payor violates the requirements of this chapter, except for section ~~8707~~ 8714, that person or entity commits a civil violation for which a fine of not more than $1,000 per day may be adjudged. A fine imposed under this paragraph may not exceed $25,000 for any one occurrence.

B. A person or entity that receives data or information under the terms and conditions of section ~~8707~~ 8714 and intentionally or knowingly uses, sells or transfers the data in violation of the board's rules for commercial advantage, pecuniary gain, personal gain or malicious harm commits a civil violation for which a fine not to exceed $500,000 may be adjudged.

C. A person or entity not covered by paragraph A or B that violates the requirements of this chapter, except for section ~~8707~~ 8714, commits a civil violation for which a fine of not more than $100 per day may be adjudged. A fine imposed under this paragraph may not exceed $2,500 for any one occurrence.

Sec. 8. 22 MRSA §8707, as amended by PL 2011, c. 524, §4, is repealed.

Sec. 9. 22 MRSA §8708, sub-§7, as enacted by PL 1995, c. 653, Pt. A, §2 and affected by §7, is amended to read:

7. Authority to obtain information. Nothing in this section may be construed to limit the board's authority to obtain information that it considers necessary to carry out its duties. The board shall adopt rules regarding the definition, collection, use and release of clinical data before collecting any type of clinical data that it did not collect as of March 1, 2014. Rules adopted pursuant to this subsection are major substantive rules as defined in Title 5, chapter 375, subchapter 2-A.

Sec. 10. 22 MRSA §§8714 to 8717 are enacted to read:

§8714. General public access to data; rules

The board shall adopt rules to provide for public access to data allowed under this chapter and to implement the requirements of this section.

1. Confidentiality. All data collected by the organization that contain protected health information are confidential. Data of the organization may be collected, stored and released only in accordance with this chapter and rules adopted pursuant to this chapter. Data of the organization containing protected health information may not be open to public inspection, are not public records for purposes of any state or federal freedom of access laws and may not be examined in any judicial, executive, legislative, administrative or other proceeding as to the existence or content of any individual's identifying health information except that an individual's identifying health information may be used to the extent necessary to prosecute civil or criminal violations regarding information in the organization database. Decisions of the organization or employees and subcommittees of the organization on data release are not reviewable.

2. General public access; confidentiality. The board shall adopt rules making information provided to the organization under this chapter, except protected health information and other confidential information, available to any person upon request.

3. Release of data. The board shall adopt rules for the release of data governing all levels of information in the form of de-identified data, limited data sets and protected health information. All uses of released data are governed by the following principles of release:

A. Release of protected health information must be limited to only information that is necessary for the stated purpose of the release;

B. Data releases must be governed by data use agreements that provide adequate privacy and security measures that include appropriate accountability and notification requirements as required of business associate agreements under HIPAA;

C. Follow-up must be provided to ensure data are used as specified and that no protected health information is publicly revealed. The board shall adopt rules providing for any necessary data suppression; and

D. Release of more protected health information than a limited data set as described in 45 Code of Federal Regulations, Section 164.514(e) must be approved by the board consistent with state and federal laws.

4. Certain practitioners. The board shall adopt rules to protect the identity of certain health care practitioners, as it determines appropriate, except that the identity of practitioners performing abortions as defined in section 1596 must be designated as confidential and may not be disclosed.

5. Notice and comment period. The board shall adopt rules to establish criteria for determining whether information is confidential clinical data, confidential financial data or other protected health information and specify procedures to give affected health care practitioners and payors notice and opportunity to comment in response to requests for information that may be considered confidential.

6. Identifying information. The board shall adopt rules to provide that individuals may be directly or indirectly identified, including through a linking or reidentification process, only as provided in this chapter and the rules of the board. Any protected health information may be used only for the purposes for which the organization releases it.

7. Minimum use. The board shall adopt rules to provide that persons gaining access to protected health information may use that information to the minimum extent necessary to accomplish the purposes for which approval was granted and for no other purpose.

8. Limitation on release. The board may not grant approval for release of data if the board finds that the proposed identification of or contact with individuals would violate any state or federal law or diminish the confidentiality of health care information or the public's confidence in the protection of that information in a manner that outweighs the expected benefit to the public of the proposed investigation.

9. Release; publication and use of data. The board shall adopt rules to govern the release, publication and use of analyses, reports and compilations derived from the health data made available by the organization. The rules must apply to all data collected, stored and released by the organization, including reports under section 8712.

10. Other privacy protections. Individually identifiable data submitted to the organization that would be protected by Title 5, sections 19203 and 19203-D, Title 34-B, section 1207 or 42 United States Code, Section 290dd-2 may not be linked or reidentified in any way that identifies an individual or in any way for which there is a reasonable basis to believe the information could be used to identify an individual. The board shall adopt rules to ensure privacy and security protections of the data that are at least equivalent to the privacy and security requirements of HIPAA.

11. Choice regarding disclosure of information. The board shall adopt rules to address the provisions for requirements regarding the disclosure of information in section 8717, subsection 3.

12. Oversight and notification to individuals. Rules developed pursuant to this section must include a definition of "breach" and a procedure for notification to affected individuals that is equivalent to those of HIPAA. If a breach requiring notification to affected individuals has occurred, the board shall notify the joint standing committee of the Legislature having jurisdiction over health and human services matters within 30 days

of the breach. Information provided pursuant to this subsection must maintain the confidentiality of all individuals affected by the breach.

13. Individual complaints. The board shall adopt rules to establish a process for an individual to file a complaint if the individual believes that the individual's protected health information has been released by the organization, the board or an employee of the organization, in violation of the board's rules.

14. Rulemaking. The board shall adopt rules as necessary to implement this section. Rules adopted pursuant to this section are major substantive rules as described in Title 5, chapter 375, subchapter 2-A.

§8715. Public health

1. Permitted use and disclosure to public health authorities. The organization may disclose protected health information, without an individual's authorization, to a public health authority for public health purposes mandated by state or federal law.

2. Use by public health authority. A state or federal public health authority to which protected health information has been disclosed under subsection 1 may use that information for public health activities and may disclose that information for public health activities as allowed by state or federal law and in accordance with board rules on data release adopted pursuant to section 8714.

3. Data use agreement. Prior to disclosing any data under subsection 1, the organization shall enter into a data use agreement with a public health authority. The agreement must include protocols that have been approved by the board for safeguarding confidential information and for ensuring there will be no disclosures of protected health information. The protocols must include appropriate accountability and notification requirements as in the business associate agreements under HIPAA.

§8716. Health care improvement studies

The board may approve the disclosure of protected health information to persons conducting health care improvement studies, subject to the following conditions.

1. Disclosure to study entities. For health care improvement studies, regarding health care utilization, improvement, cost or quality and involving patients with whom the study entity has a treatment or payor relationship, whether the study is funded by the Federal Government or the State Government or private persons, the organization may disclose protected health information to a study entity who is a covered entity or to the covered entity's business associates if those persons conducting the study do not disclose protected health information to any person not directly involved in the study without consent from the subject of the protected health information.

2. Recipients of information. A person receiving protected health information under subsection 1 may use that information only to the minimum extent necessary to accomplish the purposes of the study for which approval was granted and for no other purpose.

3. Confidentiality; protocol. The protocol for any study entity receiving protected health information under subsection 1 must be designed to preserve the confidentiality of all health care information that can be associated with identified patients, to specify the manner in which contact is made with patients and to maintain public confidence in the protection of confidential information.

4. Additional protection. The board may not grant approval to a study entity under this section for the disclosure of protected health information if the board finds that the proposed identification of or contact with patients would violate any state or federal law or diminish the confidentiality of health care information or the public's confidence in the protection of that information in a manner that outweighs the expected benefit to the public of the proposed investigation.

5. Data use agreement. Prior to disclosing any data pursuant to subsection 1, the organization shall enter into a data use agreement with a study entity. The agreement must include protocols that have been approved by the board for safeguarding confidential information and for ensuring there will be no disclosures of protected health information. The protocols must include appropriate accountability and notification requirements as in business associate agreements under HIPAA.

§8717. Covered entities' access to protected health information

1. Permitted uses and disclosures; definitions. The organization may disclose protected health information without authorization by the subject of the information for the treatment activities of any health care provider, the payment activities of a covered entity and of any health care provider or the health care operations of a covered entity or its business associates involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if the covered entity has a relationship with the subject of the information and the protected health information pertains to the relationship. For the purposes of this section:

A. "Health care operations" means any of the following activities of a covered entity:

(1) Quality assessment and improvement activities, including case management and care coordination;

(2) Competency assurance activities, including provider or health plan performance evaluation, credentialing and accreditation;

(3) Conducting or arranging for medical reviews, audits or legal services, including fraud and abuse detection and compliance programs;

(4) Specified insurance functions, such as underwriting, risk rating and reinsuring risks;

(5) Business planning, development, management and administration; and

(6) Business management and general administrative activities of the covered entity, including but not limited to de-identifying protected health information, creating a limited data set and permissible fund-raising for the benefit of the covered entity;

B. "Payment activities" means activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual; and

C. "Treatment" means the provision, coordination or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding an individual and referral of an individual by one provider to another.

2. Minimum necessary. The board shall develop policies and procedures that reasonably limit disclosures of, and requests for, protected health information for payment activities and health care operations to the minimum extent necessary.

3. Choice regarding disclosure of information. Before approving the release of any protected health information under this chapter, the organization shall implement a mechanism that allows an individual to choose to not allow the organization to disclose and use the individual's health information under this chapter.

Sec. 11. Rule-making authority. The Board of Directors of the Maine Health Data Organization shall adopt rules as necessary to implement this Act. Rules adopted pursuant to this section are major substantive rules as described in the Maine Revised Statutes, Title 5, chapter 375, subchapter 2-A.

Sec. 12. Contingent effective date. Those sections of this Act that amend the Maine Revised Statutes, Title 22, section 1711-C, subsection 6, paragraph F-3 and sections 8702 and 8705-A, repeal Title 22, section 8707 and enact Title 22, sections 8714 to 8717 take effect upon the final adoption of major substantive rules required to implement the provisions of this Act. The Board of Directors of the Maine Health Data Organization shall notify the Revisor of Statutes when the major substantive rules authorized under this Act are finally adopted.