

Paul R. LePage, Governor

Mary C. Mayhew, Commissioner

Office of the Commissioner

HIPAA Executive Policy

Policy #: DHHS-01-13

Issue Date: 7/15/13

Revised Date:

I. SUBJECT

HIPAA Executive Policy

Healthcare Privacy and Security, Including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

II. POLICY STATEMENT

It is the policy of the Department of Health and Human Services (the Department) to fully comply with the requirements of HIPAA and its updates, including the Health Information Technology for Economic and Clinical Health Act (HITECH), as well as federal and state laws, regulations, rules and accreditation standards that govern confidentiality of the protected health information (PHI) of our patients and members. Department workforce members will use or disclose PHI only as required by our job descriptions or as permitted or required by law, and will limit the PHI used or disclosed to the minimum necessary to accomplish the intended purpose of our work. Violations of HIPAA/HITECH or state law confidentiality requirements will be investigated and may result in application of workplace sanctions up to and including termination from employment.

III. RATIONALE

The federal Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule, effective 2003, and the HIPAA Security Rule, effective 2005. The HITECH Omnibus Final Rule became effective in March 2013, which both updates and amends HIPAA. The Privacy Rule addresses how covered entities, such as our healthcare providers and payer (MaineCare), may use and disclose PHI, and grants certain privacy rights to individuals regarding their PHI. The Security Rule specifies a series of administrative, physical, and technical safeguards, as well as organizational requirements, to ensure the confidentiality, integrity, and availability of our electronic PHI (ePHI). HITECH Breach Notification and Enforcement Rules underscore the importance of our vigilance in protecting PHI, and state law, licensing rules and accreditation standards add another layer of protection.

Both HIPAA and HITECH mandate numerous step-by-step compliance requirements, and failure to meet these requirements could subject the Department to investigation, notice to the media and individual patients or members, substantial civil money (enforcement) penalties and, in certain cases, criminal prosecution.

IV. PROCEDURES

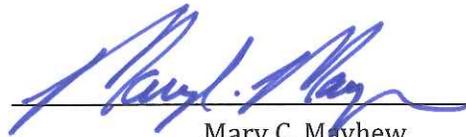
- A. **Responsibility** - The Director of Healthcare Privacy shall have overall responsibility for the administration of this policy. Office Directors and Hospital Superintendents shall have responsibility for the administration of this policy in their respective program areas and facilities.
- B. **Designation of Privacy Officers** - Directors shall appoint Privacy Officers for programs which are covered entities. Superintendents shall appoint Privacy Officers for their facilities.
- C. **Duties of the Privacy Officers** - The program and facility Privacy Officers shall:
- i. Implement Department privacy and confidentiality policies, forms and practices in their respective offices and entities;
 - ii. Reinforce and/or provide, as determined by the Director of Healthcare Privacy, program/facility specific training and otherwise act as an information resource for staff;
 - iii. Receive and address complaints regarding policy and compliance according to Department protocol;
 - iv. Monitor staff compliance and promptly report concerns, complaints, and actual or potential violations or security/privacy incidents to the Director of Healthcare Privacy;
 - v. Maintain program/facility compliance records, and provide periodic written and verbal reports to the Director of Healthcare Privacy at Privacy Officer and/or Steering Committee meetings.
- D. **Privacy Committees**: - The Director of Healthcare Privacy and Special Projects shall develop committees and hold periodic meetings with representatives of Department offices as required to review events, concerns, policies, processes, requirements and reports, and to provide education and updates as necessary to meet HIPAA, HITECH and state law privacy and security compliance standards.

V. DISTRIBUTION

All Department employees via e-mail and posting on the DHHS intranet.

July 15, 2013

Date



Mary C. Mayhew
Commissioner