

Policy #: DHHS-04-13

Issue Date: 11/04/13

Revised Date:

I. SUBJECT

HIPAA, Privacy and Security Sanctions Policy

II. POLICY STATEMENT

The Maine Department of Health and Human Services (the Department) will comply with Federal and State laws regarding the appropriate use and disclosure of Protected Health Information (PHI). As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we will take appropriate disciplinary action against any member of our workforce who fails to use reasonable safeguards to protect our patients', clients' or members' PHI in any format, or who intentionally violates any policy, or any state or federal law, involving the privacy or security of PHI or electronic PHI (ePHI).

This policy applies to our entire workforce.

III. RATIONALE

As required by law, the Department will ensure that intentional or repeated actions taken in violation of our information privacy and security policies will be addressed by this policy, regardless of professional status of the workforce member.

IV. PROCEDURE STATEMENT

A. Workforce Obligations

Members of our workforce are expected to maintain the privacy, security and integrity of PHI in any format and only use the minimum necessary PHI to perform his/her role within the organization, consistent with our Minimum Necessary Policy. Workforce members, including, but not limited to all employees, permanent or temporary staff, students, medical or other clinical residents, volunteers, and contractors will comply with all privacy and security policies, and also agree to maintain the confidentiality of the Department's confidential business information to which they have access.

B. Prohibition on Unauthorized Access, Use or Disclosure

No member of our workforce may access, use or disclose PHI or ePHI unless it is necessary to fulfill that workforce member's role within the Department. Additionally, workforce members agree that they will not share user names, passwords or other identification that permits access to the Department's computer systems or ePHI; leave computers unsecured or unattended while logged into an electronic medical record, billing record, or other electronic system or document containing ePHI; or fail to assist the Department in complying with a privacy or security requirement or obligation.

C. Duty to Report

Members of our workforce, as well as our Business Associates, are required to report known or suspected violations of patient privacy, security, and/or any actual or potential breach of PHI in any format to their Privacy or Security Officer, their Director, or the Director of Healthcare Privacy. Workforce members who fail to report known or suspected breaches or violations of privacy or security policies may be subject to disciplinary action.

D. No Retaliation for Good Faith Reports

The Department will not retaliate against a workforce member who makes a good faith report of a violation of any law, regulation or policy that protects PHI in any format, whether or not a violation is found to have occurred.

E. Investigation and Enforcement of this Policy

The Department will enforce this Privacy and Security Sanctions Policy consistently, regardless of the role of the Department workforce member. Alleged violations will be investigated by the Director of Healthcare Privacy together with the General Counsel and the Director of the appropriate Department office, for presentation to the Commissioner. The investigation may include:

1. Documentation of the alleged violation;
2. Communication with the person who allegedly committed the violation;
3. Documentation of whether the person who allegedly committed the violation has been reviewed previously for a privacy or security violation;
4. Interviews with appropriate workforce members and other individuals as necessary;
5. Engagement of and/or consultation with appropriate department specialists (e.g., Human Resources, Audit) or consultants (legal, technology, etc.) as needed;

6. Review of all circumstances surrounding the violation, including, but not limited to:
 - Degree of seriousness and impact of the violation
 - Loss of or unlawful access to PHI in any format
 - Negative publicity to the Department
 - Potential fines or other penalties
 - State and federal reporting requirements and potential regulatory investigations and business injury
 - Intentional or willful nature of the violation

F. Disciplinary Action - Sanctions

In collaboration with Human Resources, the Commissioner will determine disciplinary sanctions on a case-by-case basis, taking into account the circumstances of each alleged violation. Sanctions may be up to, and including, termination of employment.

In light of state and federal regulations requiring notification of individuals of the breach of their unsecured PHI (essentially PHI that has not been encrypted or destroyed) in certain circumstances, and the potential for widespread media exposure, as well as follow up audits, financial penalties and other potential sanctions against the Department by governmental entities, Department disciplinary sanctions may also depend on the intention of, and degree of harm caused by, the workforce member to individual patients and to the Department.

G. Confidentiality and Security Statement

Each member of the Department's workforce shall sign a Workforce Confidentiality and Security Statement (Attachment A) certifying that the workforce member has read, understands and agrees to comply with this policy, and to policies and laws relating to the protection of the Department's patient information. The signed statement will be maintained in the workforce member's employment file.

V. DEFINITIONS

Protected Health Information - Information, including demographic and billing information, which may identify the client, which relates to:

- The past, present or future physical or mental health or condition of an individual,
- The provision of health care to an individual, or
- The past, present or future payment for the individual's health care services that identifies or could reasonably be used to identify the individual.

VI. DISTRIBUTION

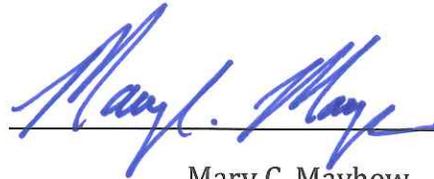
All Staff via e-mail and posting on the DHHS Intranet.

VII. ATTACHMENT

Attachment A - Workforce Confidentiality Statement and Acknowledgement of Sanctions for Violations

November 4, 2013

Date



Mary C. Mayhew
Commissioner

Maine Department of Health and Human Services

**Workforce Confidentiality Statement and Acknowledgement
of Sanctions for Violations**

I, _____, have read and understand the Privacy and Security Sanction Policy and the other policies of the Maine Department of Health and Human Services (the Department) referring to the protection of Protected Health Information. I understand that I must comply with this policy, as well as with federal and state laws, regulations and rules, and the Department's other policies and processes that protect such information, as a condition of my employment.

I agree to maintain the privacy, security, and integrity of patient information in any format.

I agree only to use, access, create, maintain or disclose such information for the purpose of performing my work for the Department

I will comply with these policy requirements for the protection of a) PHI in any format and b) our confidential business assets, whether working on site or off-site.

I will never a) reveal or independently suggest that a particular individual receives Department services, b) forward ePHI to a non-work-related email address, or c) post information related to a patient, member, client or other individual receiving services or in Department custody to a social media or other website.

I will use reasonable and appropriate safeguards to avoid causing any harm to PHI in any format, whether held in an electronic record system, on paper records, film, or other medium, including on portable devices. I will immediately report the loss of, or technical concern regarding portable media or mobile devices, or suspicion of unauthorized access, use or disclosure of PHI or electronic PHI, to my director and/or the Director of Healthcare Privacy.

I understand and agree that failing to comply with any of the policies or requirements mentioned in this statement, or violating a policy that relates to the protection of an individual's information or the confidential business information of the Department could lead to disciplinary sanctions, up to and including termination of employment.

Date: _____

Printed Name: _____

Signature: _____

Witness: _____