



Paul R. LePage, Governor

Mary C. Mayhew, Commissioner

Office of the Commissioner
Privacy and Security Sanctions Policy

Policy #: DHHS-04-14

Issue Date: 4/2/14

I. SUBJECT

Privacy and Security Sanctions Policy

II. POLICY STATEMENT

The Maine Department of Health and Human Services (the Department) recognizes the business, financial, and quality needs and obligations of the Department's workforce to access, analyze, report on and work with a wide range of data, which may include identifiable patient, member, client or consumer information, in order to accomplish the Department's mission and goals. In carrying out its work, the Department and its workforce will act in good faith to comply with Federal and State laws regarding the use, disclosure, maintenance or transmission of Protected Health Information (PHI) as defined below, electronically maintained PHI, or any other personally identifiable or confidential business information of the Department (collectively, "Protected Information"), in any format. As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other applicable laws, any member of the Department's workforce who intentionally, willfully, knowingly or repeatedly violates any policy, or any state or federal law, involving the privacy or security of Protected Information, will be subject to the application of this policy.

This policy applies to the Department's entire workforce, including those working for both HIPAA-covered and non-HIPAA covered entities.

III. RATIONALE

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

IV. PROCEDURE STATEMENT

A. Workforce Obligations

Members of the Department's workforce are expected to maintain the privacy, security and integrity of Protected Information in any format and only use the minimum necessary Protected Information to perform his or her role within the organization, consistent with the Department's 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 business information to which they have access.

B. Prohibition on Unauthorized Access, Use or Disclosure

No member of the Department's workforce may access, use, disclose or transmit Protected Information 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 unauthorized access to the Department's Protected Information; forward Protected Information to a non-work related email address; reveal or independently suggest that an individual receives services from the Department; post Protected Information relating to an individual receiving services from the Department on social media or other websites without the individual's written authorization; leave computers unsecured or unattended while logged into an electronic medical record, billing record, or other electronic system or document containing Protected Information; leave Protected Information in any format in view in a vehicle, in an unlocked vehicle, or any unsecure location; or fail to assist the Department in complying with a privacy or security requirement or obligation.

C. Duty to Report

Members of the Department's workforce, as well as the Department's Business Associates, are required to report known or suspected violations of privacy, security, and/or any actual or potential breach of Protected Information in any format to their Privacy/Security Liaison, their Director and 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 regarding Protected Information 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 or status 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, and a report of the investigation will be submitted to the Commissioner for review and final determination. The investigation may include:

1. Development of documentation of the alleged violation;
2. Communication with the person who allegedly committed the violation;
3. Review of documentation to determine 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. Consultation with appropriate Department specialists (e.g., Human Resources, Audit) or consultants (legal, technology, forensic, 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 Protected Information in any format
 - 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 the Bureau of 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 include disciplinary actions up to, and including, termination of employment. The intention of, and degree of harm caused by, the workforce member to individual patients, members, clients or consumers of the Department may be considered when imposing disciplinary sanctions.

Factors that may be considered include: (a) Obligations of state and federal regulations requiring notification of individuals of the breach of their unsecured PHI or certain Protected Information circumstances; (b) mandatory notification to regulators, the media and consumer reporting agencies, depending on the type of Protected Information exposed and the number of consumers affected; (c) follow up audits of Department records; (d) financial penalties imposed on the Department; and (e) other potential sanctions against the Department by governmental entities.

G. Confidentiality and Security Statement

Each member of the Department's workforce shall sign a Workforce Confidentiality and Security Statement (See Attachment) 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, member, client or consumer information. The signed statement will be maintained in the workforce member's employment file.

V. DEFINITIONS

Protected Health Information - means information, including demographic and billing information that may identify the patient, member, client or consumer, and 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 - Workforce Confidentiality Statement and Acknowledgement of Sanctions for Violations

April 2, 2014

Date



Mary C. Mayhew
Commissioner

**Maine Department of Health and Human Services
Workforce Confidentiality Statement and Acknowledgement of Sanctions
For Privacy or Security Violations**

I, _____, have read and understand the Privacy and Security Sanction Policy of the Maine Department of Health and Human Services (the Department) referring to the protection of Protected Health Information and other identifiable or confidential 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 procedures that protect such identifiable or confidential information, as a condition of my employment.

I agree to maintain the privacy, security, and integrity of protected health information (PHI), electronic PHI, identifiable member, client or consumer information, or confidential business information (collectively, Protected Information) in any format, whether working on or off-site, as a condition of my employment.

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

I will comply with these policy requirements for the protection of Protected Information in any format whether working on site or off-site.

I will never (a) reveal or independently suggest that a particular individual receives Department services; (b) forward Protected Information to a non-work related email address such as a personal email address; (c) post Protected Information related to a patient, member, client, consumer or other individual receiving services or in Department custody to a social media or other website without written authorization of the individual; (d) leave Protected Information in any format in view in a vehicle; or (e) use, disclose or leave Protected Information in any format in any unsecure location, including an unlocked vehicle.

I will use reasonable and appropriate safeguards to avoid impacting the integrity of Protected Information 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 Protected Information to my Privacy/Security Liaison, my director and 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 Protected 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: _____