

Policy #: DHHS-05-16

Issue Date: April 14, 2016

I. SUBJECT

HIPAA: Risk Management Policy

II. POLICY STATEMENT

The Maine Department of Health and Human Services (the Department), in collaboration with the Office of Information Technology (OIT), which serves as our technology partner, will comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requiring the Department to conduct a Risk Analysis regarding its protected health information (PHI). Additionally, the Department will use commercially reasonable efforts to keep PHI and other confidential consumer information (together, "Protected Information" or "PI") maintained in electronic format (all together, "ePI") confidential and secure. The Department will reasonably and appropriately address risks to the confidentiality, integrity and accessibility of its ePI through this Risk Management Policy and all related policies protecting the privacy or security of PI in any format.

III. RATIONALE

HIPAA and good business practices require that the Department make efforts to reduce the risks to ePI to a reasonable level.

IV. PROCEDURE STATEMENT

A. Risk Management Process

As required by HIPAA, the Department will conduct, and will periodically update, a risk analysis to identify and address the risks to our PHI in electronic format. Additionally, with regard to all ePI, the Department will:

1. Implement action steps to address privacy or security compliance concerns;
2. Develop and implement a risk management plan that supplements and builds upon those action steps;

3. Implement administrative, technical and physical security measures;
4. Evaluate, update and maintain security measures.

B. Administrative Safeguards

Appointment of our Privacy and Security Officials is one of the first requirements under the HIPAA requirements. The Department has such leaders in place. The Privacy/Security Liaisons, who report to the Director of Healthcare Privacy, will collaborate to develop policies and procedures for our workforce regarding the reasonable protection of our PI in any format.

1. Workforce Education - Our workforce will review the policies and receive yearly training, at minimum, on issues of privacy and security surrounding the protection of our PI and ePI.
2. Sanction Policy - Our workforce will agree to comply with our policies, and will sign the attachment to our Privacy and Security Sanctions Policy, agreeing to comply with our policies and processes intended to reasonably maintain the confidentiality, integrity and accessibility of our PI in any format.
3. Audits, Complaints - Along with the implementation of our policies and procedures, our Privacy/Security Liaisons will conduct periodic mock audits in a reasonable effort to ensure that our workforce maintains privacy and security awareness, and to reinforce that only authorized users should access our consumer information, on a minimum necessary, need-to-know basis. Our Privacy/Security Liaisons will alert the Director of Healthcare Privacy regarding any known or potential security incidents involving our consumers' PI in any format, and promptly investigate reported concerns or issues arising from such periodic reviews. All workforce members will comply with and assist in the investigative process, where requested.
4. Walk-Through Reviews - Likewise, our Privacy/Security Liaisons, as appropriate, will conduct walk-through evaluations of the privacy and security safeguards in the Department, using a checklist tool, and will follow up on all concerns.
5. Mitigation - HIPAA requires that the Department mitigate any harmful effect of a use or disclosure of PI/ePI that violates our policies and procedures or the Privacy or Security Rules, to the extent practicable. The Director of Healthcare Privacy or his/her designee will ensure that any findings of a violation will be addressed promptly to lessen any potential harm to the PHI. Mitigation may include changes in policies, procedures, as well as targeted education or counseling. The Department's Breach Notification Policy will also be implemented where appropriate.

6. Notice of Privacy Practices - The Privacy/Security Liaison of each covered entity will ensure that the applicable Notice of Privacy Practices is updated with material changes to the use or disclosure of PHI. With regard to the Department's providers/facilities, appropriate Department workforce members will make a good faith effort to obtain the acknowledgement that the Notice of Privacy Practices was received. Such acknowledgement, or refusal, shall be maintained in the consumer's file.
7. Authorization Form - The Department will have a valid HIPAA and state law compliant authorization for use and disclosure of PI.
8. Maintenance of Documentation – HIPAA related documents will be maintained for a minimum of six years, including data involving amendments, policies, or other written HIPAA related communications.

C. Physical Safeguards

The Department has implemented a variety of physical safeguards, and a Physical Safeguards Policy, in a reasonable effort to comply with federal and state law requirements to protect our PI and ePI. Our ongoing efforts will include:

1. Securing doors and drawers [wherever possible] when an office containing or displaying PI is empty;
2. Protecting paper-based documents that contain consumer information from unauthorized access;
3. Securing laptops or other portable media securely when not in use;
4. Storing keys to locked areas and cabinets in a reasonable and secure location;
5. Ensuring that unique identifiers and passwords to systems containing ePI are maintained in a secure location, and not publicly visible;
6. Turning computer screens away from the public and keep voices low when discussing consumer identifiable information;
7. Keeping fax machines, copiers and scanners in a non-public area;
8. Installing and securing hardware technology protections where appropriate;
9. Ensuring that consumers and non-workforce members are escorted to and from offices.

D. Technical Safeguards

Through our partnership with OIT, the Department has implemented technical safeguards in a reasonable effort to comply with federal and state law requirements to protect our ePI from inappropriate access, alteration, use or disclosure. Our continuing efforts will include:

1. Reviewing the audit trail associated with our electronic health record systems containing ePI to ensure appropriate access, use and disclosure of our ePI, and following up on any concerns;
2. Ensuring that workforce members are only granted access to PHI and ePI as appropriate to their role;
3. Ensuring that workforce members use password protection to properly authenticate their identities, do not share their passwords unless authorized by the Privacy/Security Liaison for continuity of care purposes;
4. Installing encryption on portable media containing ePI laptop and flash drives;
5. Utilizing firewall and anti-virus software and other technical protection on our computers and computer systems to prevent corruption or damage to our hardware and our ePI;
6. Ensuring that technical protection for hardware, systems and software are kept up to date.

V. EVALUATE AND MAINTAIN

Along with our regular access monitoring, walk-throughs, and periodic training, our Privacy/Security Liaison(s) will work with the Director of Healthcare Privacy to implement, and update as necessary, our administrative, physical and technical security measures where required by changes in the laws, regulations and rules. These measures will be taken in an effort to reduce risks to our PI and ePI.

VI. ADDITIONAL ORGANIZATIONAL REQUIREMENTS

1. In addition to our privacy and security standards, the Department will conduct a scheduled review of our business associate, vendor and other associations or affiliations which impact our PI or ePI.
2. The Department will act to ensure that there are no gaps in Business Associate Agreement coverage, where applicable.

VII. DEFINITIONS:

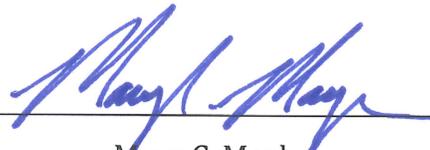
Protected Health Information is information about a consumer, including demographic information that may identify a consumer, which relates to the consumer's past, present or future physical or mental health or condition, related health care services or payment for health care services.

VIII. DISTRIBUTION

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

4/14/14

Date



Mary C. Mayhew
Commissioner