Maryland Institute for Emergency Medical Services Systems		
Policy: Health Insurance Portability and Accountability Act		
Originator: Attorneys General Office		
Policy Number	Effective Date	Revision Date
310.01	April 9, 2014	n/a

Purpose: The Maryland Institute for Emergency Medical Services Systems (MIEMSS) is committed to protecting the health information of Maryland citizens. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations require that MIEMSS adopt certain policies on specific issues.

The Executive Director shall designate one individual as the MIEMSS Security Officer. The MIEMSS Security Officer shall coordinate HIPAA activities with the Attorney General's Office.

This policy explains the administrative and organizational requirements for privacy in the HIPAA and HITECH standards including MIEMSS need to develop conforming relationships with business associates, a complaint process, sanctions against members of the workforce who violate privacy policies or practices, mitigation procedures should a violation occur, protection for whistleblowers, practices to safeguard health information, and retention of documentation otherwise required under the law.

Background: In adopting this policy, MIEMSS is demonstrating due diligence toward compliance with the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009, and their implementing regulations. This policy also incorporates requirements of the Maryland Confidentiality of Medical Records Act of 1990 and other applicable laws and regulations. These mandates protect and enhance the rights of patients by providing restrictions over how their health information is used or disclosed. From a broader perspective, they also provide for improved efficiency and effectiveness in the healthcare system through a more uniform nationwide privacy framework.

Those Federal and State laws and regulations that are more stringent than the HIPAA and HITECH requirements, will generally remain in effect and will not be preempted by HIPAA or HITECH. In addition, some state laws requiring disclosure of health information remain in effect. Certain exceptions from the HIPAA and HITECH privacy requirements may be identified in the policy or subsequently published guidance.

Policy Statements

A) Authority

1) The Health Insurance Portability and Accountability Act (HIPAA); Public Law 104-191 authorizes and mandates MIEMSS to issue this policy.

2) The Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recoveries and Reinvestment Act of 2009; Public Law 111-5 amends the privacy requirement in part.

B) Roles and Responsibilities

1) Security Officer

a) The Executive Director shall designate a MIEMSS Security Officer for the Agency.

b) The MIEMSS Security Officer is responsible for:

(1) Developing and assisting in the implementation of all policies, procedures, and guidelines that affect an individual's health information.

(2) Assuring that practices are adopted by MIEMSS to protect health information consistent with Federal and State law

C) Organizational Designation

1) MIEMSS is a Business Associate with respect to certain functions in connection with Emergency Medical Services Operational Programs (EMSOPS), subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations. MIEMSS is not a Covered Entity.

2) MIEMSS and its employees are also subject to other Federal and State Laws and regulations concerning the confidentiality, privacy and security of health information, including the Maryland Confidentiality of Medical Records Act of 1990.

D) Business Associate Agreements

1) With assistance from the Office of the Attorney General, MIEMSS will adopt MIEMSS business associate agreements.

2) MIEMSS may disclose health information to a Covered Entity or another business associate, or allow a covered entity or business associate to create or receive health information if MIEMSS first obtains adequate assurance that the business associate will appropriately safeguard the health information. This requirement does not apply to:

a) MIEMSS activities in connection with its public health oversight duties under Education Article §§ 13-501 to 13-517, COMAR Title 30 and/or the EMS Plan;

b) Use or disclosure made to another governmental agency for the purpose of public benefit eligibility or enrollment determinations where the agency is authorized by law to make these determinations; or,

c) Use or disclosure otherwise authorized by law.

3) If the business associate is another governmental entity, whether internal or external to MIEMSS, MIEMSS may execute a Memorandum of Understanding (MOU) or like document covering the required terms, or rely on other law that imposes upon the business associate the requirements otherwise authorized.

4) Oversight Responsibilities:

a) If MIEMSS becomes aware of a pattern or practice of a business associate that amounts to a material violation of the agreement, MIEMSS must attempt to cause the Business Associate to cure the breach or end the violation, and if such attempt is unsuccessful, MIEMSS shall terminate the agreement if feasible, and if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

5) MIEMSS shall report all breaches of a business associate agreement or MOU involving a violation of privacy practices to the Privacy Office within one State business day of notice of the violation or potential violation.

E) State Pre-Emption

1) The HIPAA Privacy Rule, as modified, and HITECH preempts State law if:

a) That provision is more stringent than the State law, and

b) A covered entity could not possibly comply with both that provision of the State law and the final HIPAA Privacy Rule, as modified in HITECH; or

c) The State law creates an obstacle to accomplishment of the goals of the final HIPAA Privacy Rule, as modified or HITECH.

2) Upon request, the Attorney General's Office will provide guidance on the current analysis of pre-emption issues.

F) Complaints to MIEMSS

1) Individuals shall make complaints concerning requirements of this policy and the related privacy mandates, or MIEMSS compliance with these mandates to the MIEMSS HIPAA Security Officer or to the MIEMSS Office of the Attorney General.

2) The MIEMSS Security Officer shall arrange to document all complaints received and their disposition.

G) Changes in the Law

1) MIEMSS will update or revise its policies and procedures on health information as necessary to comply with changes in Federal or State laws or regulations dealing with privacy of health information.

H) Mitigation

1) MIEMSS shall attempt to mitigate, to the extent practical, any harmful effect known to MIEMSS of a use or disclosure of health information by an employee or business associate that is in violation of the privacy regulation or MIEMSS policies and procedures.

2) If MIEMSS health information has been misused by a business associate, MIEMSS shall:

a) Investigate the misuse of the health information.

b) Determine if the misuse was serious.

c) Determine if the misuse is repeated.

d) Counsel the business associate on the misuse of health information.

e) Monitor the business associate's performance to ensure that the wrongful behavior has been remedied.

f) Reserve the right to terminate a business associate agreement in the event the misuse of health information continues despite counseling.

g) Maintain a record, either written or electronically, of any communications, actions, or activities conducted to mitigate the harm.

I) Application of Sanctions by MIEMSS

1) MIEMSS will apply sanctions to members of its workforce who fail to comply with the policies and procedures on privacy of health information, consistent with the State Personnel System law and the procedures of the MIEMSS Office of Human Resources.

2) MIEMSS employees shall consult with the Attorney General's Office prior to applying any sanctions, including consistency with the State Personnel System law.

3) The MIEMSS Security Officer, in coordination with other offices, shall develop an appropriate method for acquiring and maintaining reports on sanctions that is compatible with other applicable Federal or State laws or contractual agreements which limit access to confidential personnel information.

J) Safeguards

MIEMSS shall ensure that appropriate administrative, technical, and physical safeguards are in place to protect the privacy of health information.

1) MIEMSS will take reasonable steps to safeguard health information from any intentional or unintentional use or disclosure that is in violation of privacy protection standards pursuant to MIEMSS policies and procedures.

2) Safeguards may include, but are not limited to the following:

   a) Shredding of documents that contain protected health information prior to disposal from offices or depositing documents with a document destruction contractor.

   b) Implement records management processes for protecting health information consistent with privacy policies.

   c) Requiring locking doors to medical records departments, or locking cabinets where medical records are kept, and limiting access to the keys or combinations to such locks.

   d) Placing facsimile machines and other office equipment that are used for processing, sending or receiving protected health information in an area with limited access, and limiting use of such equipment to those whose job functions include processing health information.

3) MIEMSS shall function under standard operating procedures that safeguard health information.

4) MIEMSS shall maintain awareness and adherence to other applicable MIEMSS policies and guidance related to technical and physical security, confidentiality, and privacy, including the following:

   a) E-mail Security Tips;

   b) Data Eradication Procedures;

   c) MIEMSS password standards; and

   d) Laptop, Portable, and Off-site Data Processing Equipment Protocol.

K) Whistleblowers

1) MIEMSS shall investigate allegations of misconduct of a member of the MIEMSS workforce or a business associate when health information is released.

2) Employees who in good faith report a possible violation to appropriate officials may not be subject to retaliation.

L) Documentation

1) MIEMSS shall maintain records, either written or electronic, of its privacy policies and procedures, communications required by privacy regulations, or any other actions, activities, or designations required by the privacy regulations.

2) Such documentation required under this policy will be retained for a period of at least six years.

Public/Private Designation: Public - This document is approved for publication and unrestricted distribution.

Policy approved by MIEMSS:

Signature: Pat Gainer Date: 4-9-14
Pat Gainer, JD, MPA
Acting Co-Executive Director

Signature: Richard L Alcorta MD Date: 04/14/14
Richard Alcorta, MD
Acting Co-Executive Director