Maryland Institute for Emergency Medical Services Systems		
Policy: Personal Information Security Policy		
Originator: Attorneys General Office		
Policy Number	Effective Date	Revision Date
310.02	June 24, 2014	n/a

Purpose: The Maryland Institute for Emergency Medical Services Systems (MIEMSS) is committed to protecting the personal information of individuals. Effective July 1, 2014, State Government Article Subtitle 13 requires that MIEMSS adopt certain practices and policies regarding personal information.

This policy explains the administrative and organizational requirements for reasonable security procedures and policy standards including MIEMSS' need to develop conforming relationships with third parties, practices to safeguard personal information, and retention of documentation otherwise required under the law.

Background: This policy is adopted in accordance with the requirements of chapter 304 of the Acts of 2013.

Definitions:

A) "Breach of the Security of a System"

1) "Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal or private information maintained by MIEMSS.

2) "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of MIEMSS for the purposes of the MIEMSS, provided that the personal or private information is not used or subject to further unauthorized disclosure.

B) "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

1) A social security number;
2) A driver's license number, state identification card number, or other individual identification number issued by a unit;
3) A passport number or other identification number issued by the united states government;
4) An individual taxpayer identification number; or
5) A financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

C) "Security Officer"

1) The Security Officer designated by the Executive Director for the purposes of HIPAA shall be the Security Officer for the purposes of this personal information policy.

Policy:

A) Security Officer

1) The Security Officer is responsible for:

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

   b) Assuring that practices are adopted by MIEMSS to protect personal information consistent with applicable law

B) Nonaffiliated Third Party Agreements

1) With assistance from the Office of the Attorneys General, MIEMSS will adopt agreements with nonaffiliated third parties who perform services for MIEMSS which involve disclosure of personal information about an individual to implement and maintain reasonable security procedures and practices that:

   a) Are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and

   b) Are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction

2) If MIEMSS personal information has been misused by a nonaffiliated third party, MIEMSS shall:

   a) Investigate the misuse of the personal information.

   b) Determine if the misuse was serious.

   c) Determine if the misuse is repeated.

   d) Counsel the nonaffiliated third party on the misuse of personal information.

e) Monitor the nonaffiliated third party's performance to ensure that the wrongful behavior has been remedied.

f) Reserve the right to terminate a nonaffiliated third party agreement in the event the misuse of personal information continues despite counseling.

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

C) 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 personal 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 Attorneys General 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 which limit access to confidential personnel information.

D) Safeguards

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

1) MIEMSS will take reasonable steps to safeguard personal 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) Following Department of Information Technology Security policy with regard to computerized personal information.

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

c) Implementing records management processes for protecting personal information consistent with privacy policies.

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

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

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

E) Breach of the Security of a System

1) If MIEMSS discovers or is notified of a breach of the security of a system, MIEMSS shall conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information has resulted in or is likely to result in the misuse of the information. MIEMSS shall give notice of the breach to the Office of the Attorneys General and the Department of Information Technology.

2) Except as provided in subparagraph (a) of this paragraph, if after the investigation is concluded, MIEMSS determines that the misuse of the individual's personal information has occurred or is likely to occur, MIEMSS or the nonaffiliated third party, if authorized under a written agreement with MIEMSS, shall notify the individual of the Breach.

a) Unless MIEMSS or the nonaffiliated third party know that the encryption key has been broken, MIEMSS or the nonaffiliated third party is not required to notify an individual under paragraph 4 above if:

(1) The personal information of the individual was secured by encryption or redacted; and

(2) The encryption key has not been compromised or disclosed.

3) Except as provided in Section 6 below, the required notice shall be given as soon as reasonably practicable after MIEMSS conducts the required investigation.

4) If, after the investigation is concluded, MIEMSS determines that notification is not required, MIEMSS shall maintain records that reflect its determination for three years after the determination is made.

5) A nonaffiliated third party that maintains computerized data that includes personal information provided by MIEMSS shall notify MIEMSS of a breach of the security of a system if the unauthorized acquisition of the individual's personal information has occurred or is likely to occur as soon as reasonably practicable after the nonaffiliated third party discovers or is notified of the breach. The nonaffiliated third party shall share with MIEMSS all information relating to the breach.

6) Notification of a breach of the security of a system may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security. In that case, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that the notification is no longer an impediment to an investigation or security.

7) Notification to an individual required under this policy may be given:

a) By written notice sent to the most recent address of the individual in MIEMSS records; or

b) By electronic mail to the most recent electronic mail address of the individual in MIEMSS records.

c) By telephone to the most recent telephone number of the individual in MIEMSS records; or

d) By substitute notice if:

(1) The cost of providing notice would exceed $100,000 or the affected class of individuals exceeds 175,000 or MIEMSS lacks sufficient information to supply another form of notice.

8) Substitute notice consists of:

   a) Electronic notice to an individual if MIEMSS has an electronic mail address for the individual;

   b) Conspicuous posting of the notice on the MIEMSS website; and

   c) Notification to appropriate media.

9) Notice required under this policy shall include:

   a) A description of the categories of information that were, or are reasonably believed to have been acquired by an unauthorized person including which of the elements of personal information were, or are reasonably believed to the be acquired;

   b) The following contact information:

      Maryland Institute for Emergency Medical Services Systems
      653 West Pratt Street
      Baltimore, Maryland 21201
      410-706-5070

   c) The toll free telephone numbers addresses of the major consumer reporting agencies; and

   d) The statement that an individual can obtain information from the following sources about steps that can be taken to avoid identity theft:

      (1) Federal Trade Commission
      600 Pennsylvania Avenue, NW
      Washington, DC 20580
      Telephone: (202) 326-2222
      http://www.ftc.gov/contact

      (2) The Office of the Attorneys General
      200 St. Paul Place,
      Baltimore, MD 21202
      (1 (888) 743-0023)
      http://www.oag.state.md.us/

e) If MIEMSS is required to notify 1,000 or more individuals in connection with a breach, MIEMSS shall notify each consumer reporting agency that complies and maintains files on consumers on a nationwide basis, as defined by 15 USC § 1681A(P) of the timing, distribution, and content of the notices. MIEMSS is not required to include the names or other personal identifying information of recipient of notices of a breach.

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

Policy approved by MIEMSS:

Signature: Patricia Gainer Date: 6-24-14
Pat Gainer, JD, MPA
Acting Co-Executive Director

Signature: Richard L Alcorta MD Date: 06/24/14
Richard Alcorta, MD
Acting Co-Executive Director