	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<b>Policy: <i>Unauthorized Disclosure of Protected Health Information</i></b>		
	<b>Originator: <i>Information Technology</i></b>		
	Policy Number	Effective Date	Revision Date
	137.02	October 3, 2011	July 1, 2013

**Purpose:** Covered entities and business associates must provide notification of breaches of unsecured protected health information (PHI), including ambulance run sheets and electronic patient care reports, if the breach poses a significant risk of harm to the individual.

**Definitions:**

1. **Breach** - A breach is, generally, the unauthorized acquisition, access, use, or disclosure of protected health information in a manner that compromises the security or privacy of the protected health information such that the acquisition, access, use, or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
2. **Covered Entity** - a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. For MIEMSS purposes this means an EMS Operational Program or a Hospital.
3. **Unsecured Protected Health Information** - Covered entities and business associates must only provide the required notification if the breach involved unsecured protected health information. “Unsecured protected health information” is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in guidance issued by the U.S. Secretary of Health & Human Services. The guidance specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.
4. **Unauthorized Use or Disclosure** – A use or disclosure of PHI not authorized by federal regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH ACT).

**Procedures:**

1. Discovery of Breach
  - a. Every member of our workforce (including employees, contractors, volunteers, and trainees) shall immediately report to the agency Security Officer or the agency Assistant Attorney General any information regarding a breach, or potential breach, of PHI.



## Maryland Institute for Emergency Medical Services Systems

**Policy:** *Unauthorized Disclosure of Protected Health Information*

**Originator:** *Information Technology*

Policy Number	Effective Date	Revision Date
137.02	October 3, 2011	July 1, 2013

- b. A breach is considered discovered as of the first day on which the breach is known by MIEMSS or, by exercising reasonable diligence, would have been known to MIEMSS.
- c. MIEMSS is deemed to have knowledge of a breach if the breach is known or, by exercising reasonable diligence, would have been known, to any person (other than the person committing the breach) who is an employee or agent of MIEMSS. We do not consider a Business Associate to be an agent of MIEMSS.

### 2. Reporting a Breach

- a. Every breach of PHI must be reported to the Covered Entity who supplied the PHI unless the MIEMSS Data Access Committee determines and documents the reasons why a report of breach is not required. A report of breach is required unless:
  - i. The data was encrypted according to HHS guidance with strong passwords and the passwords are still secure;
  - ii. If the data was not encrypted:
    - 1. The disclosure was an unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, and such acquisition, access, or use was made in good faith and within the scope of authority and did not and will not result in further use or disclosure in a manner not permitted ;
    - 2. The disclosure was an inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement, in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
    - 3. The disclosure of protected health information involves a situation where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.





**Maryland Institute for Emergency Medical Services Systems**

**Policy: *Unauthorized Disclosure of Protected Health Information***

**Originator: *Information Technology***

Policy Number	Effective Date	Revision Date
137.02	October 3, 2011	July 1, 2013

iii. If the disclosure is not determined to satisfy requirements 3i or 3ii above, then the breach shall be reported unless there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:


1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated

b. Upon determining that the impermissible use of disclosure of PHI constituted a breach that requires notification, the agency Security officer shall inform the Executive Director and MIEMSS’s assistant attorney general and proceed to the notification procedures.

3. Notification Procedures

a. Timeliness of Notification

- i. Once a determination has been made that there is no valid exception to the breach notification requirement, notice of the breach shall be made promptly to the Covered Entity who submitted the data without unreasonable delay, and in no case later than sixty (60) days after discovery of the breach.
- ii. Delay of Notice for Law Enforcement Purposes – If a law enforcement official advises MIEMSS that a notification, notice or posting required under this policy would impede a criminal investigation MIEMSS shall take the following steps:
  - If the statement is in writing and specifies the time needed for delay, MIEMSS shall delay breach notification for the period of time specified in the writing;
  - If the statement is oral, MIEMSS will document the statement, including the identity of the law enforcement official, and shall delay breach notification temporarily, but no longer than 30 days from the date of the statement, unless a


	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<b>Policy: <i>Unauthorized Disclosure of Protected Health Information</i></b>		
	<b>Originator: <i>Information Technology</i></b>		
	Policy Number	Effective Date	Revision Date
	137.02	October 3, 2011	July 1, 2013

written statement described above is provided to MIEMSS within that 30-day time period, stating a specific time for delay.

- b. Content of the Notice – Regardless of the method by which notice is provided to patients under this policy, the required notice shall be in plain language and, to the extent possible, shall contain the following information:
- i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
  - ii. A description of the types of unsecured PHI that were involved in the breach, such as whether full name, Social Security Number, date of birth, home address, account number, medical condition, or other types of information were involved. Only the generic type of PHI should be included in the notice, i.e., not the patient’s actual SSN or birth date.
  - iii. The steps the patient should take to protect themselves from potential harm resulting from the breach.
  - iv. A brief description of what MIEMSS is doing to investigate the breach, to mitigate harm to patients, and to protect against further breaches.
  - v. Contact procedures for patients to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

4. Documentation

- a. MIEMSS shall maintain documentation related to all breach investigations and notices, including the risk assessment conducted to determine whether a breach notification was required, and shall maintain such documentation for six (6) years after the discovery of the breach.
- b. The documentation maintained for each breach investigation shall include:
  - i. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patient affected, if known.
  - ii. A description of the types of PHI that were involved in the breach.
  - iii. A description of the facts upon which a determination was made that notice of the disclosure or breach was not required.
  - iv. A description of the action taken by MIEMSS with regard to notification of Covered Entities.
  - v. A description of the evidence demonstrating the necessity of any delay in providing notification.
  - vi. A description of the measures taken by MIEMSS to mitigate the breach.
  - vii. A description of the steps taken by MIEMSS to prevent future occurrences of that type of breach.

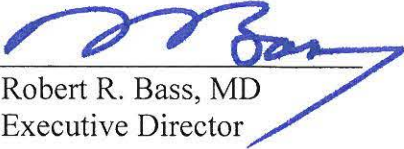
	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<b><i>Policy: Unauthorized Disclosure of Protected Health Information</i></b>		
	<b><i>Originator: Information Technology</i></b>		
	Policy Number	Effective Date	Revision Date
	137.02	October 3, 2011	July 1, 2013

5. Workforce Training – MIEMSS shall train all members of our workforce regarding this policy, including how to notify the agency security officer or the Attorney General of a possible breach.

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

Policy approved by MIEMSS:

Date: 6/19/13

Signature:   
 Robert R. Bass, MD  
 Executive Director

Revision History:

October 3, 2011 – Original  
 July 18, 2013 – Updated