Purpose: Encryption of data provides best practice protection for protected health information.

1. Protected health information stored on any mobile device in the possession or control of a MIEMSS employee including laptops, PCs, PDAs (such as iPads, iPhones, Palm Pilots, Blackberrys, Treos, or smart phones), USB flash drives (memory stick), CDs and all similar devices shall be encrypted at least to the level of AES 256 bit encryption.

2. Protected Health Information is any information that can be used to identify a patient – whether living or deceased and which relates to the patient's past, present, or future physical or mental health or condition, including health care services provided and the payment for those services.

3. Data which identify a patient include:

   a. Names;

   b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

      (1) The geographic unit formed by combining all zip codes with the same three

      (2) initial digits contains more than 20,000 people; and

      (3) The initial three digits of a zip code for all such geographic units containing

      (4) 20,000 or fewer people is changed to 000.

   c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

   d. Telephone numbers;

   e. Fax numbers;

   f. Electronic mail addresses;

   g. Social security numbers;

   h. Medical record numbers;

   i. Health plan beneficiary numbers;

   j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; or

r. Any other unique identifying number, characteristic, or code.

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