

Policy #: DHHS-05-14

Issue Date: 4/15/14

Revised Date:

I. SUBJECT

HIPAA, Security of Portable Devices

II. POLICY STATEMENT

The Department of Health and Human Services (the Department) takes seriously the risks to protected health information (PHI) and confidential information in any format. The Department recognizes the high risk to electronic, digital or non-paper based PHI (ePHI) or other confidential information that is used, disclosed, accessed, stored, maintained, transmitted or otherwise moved or moveable via a portable electronic device. It is the policy of the Department to make reasonable efforts to lessen the risk to such information located on portable devices, including computers or electronic information storage items, through the procedure set forth in this policy.

This policy applies regardless of (A) whether the Department owns or purchased the portable device and (B) whether on or off-site. Examples of portable devices may include computers, such as laptops, tablets, and hand-held devices (PDAs, pager/cell phones with storage and processing capability), CDs; discs, memory sticks, MP3 players; portable phones or "smart phones", storage devices, and "thumb/USB/flash drives." As technology continues to change and progress, this policy will apply to other devices that may be used to access, store, transmit, maintain or otherwise hold or move ePHI or other confidential information of the Department.

III. RATIONALE

Portable devices are at great risk of loss, theft and unauthorized access to the Department's ePHI and other electronically stored information. This policy is implemented to document the Department approved practices regarding portable devices in an effort to avert the risk to our patient, member, and client ePHI or other confidential information. A violation of this policy could result in a high profile breach requiring notifications, including to individuals, federal and state regulators, broadcast and print media, and consumer reporting entities, as well as extensive legal enforcement against the Department.

IV. PROCEDURE STATEMENT

Portable Device Procedure:

- A. Inventory** - Each office shall, as necessary, make available to staff appropriately encrypted portable devices (or other means) for storing or transferring ePHI or other confidential information. Each office shall assign a responsible individual to maintain a written inventory of all portable devices (including both organization-owned and personally owned) used to access and/or store the Department's ePHI and shall ensure that use of any new devices or any changes in use of existing devices are promptly reported to the responsible individual. The use of unencrypted portable devices to download, copy, carry, transmit, store or otherwise transfer ePHI or other confidential information of the Department is prohibited.
- B. Encryption** - To prevent a regulatory or legal violation and a costly, high profile breach notification process if the portable device were lost, appropriate encryption software must be installed on the portable device and used to protect any ePHI or other confidential information used by the Department. Encryption software meeting Department-required standards and government-endorsed algorithms shall be used to encrypt Department data on portable devices. Only storage devices that meet appropriate encryption standards may be used to maintain, hold, transport, access or transmit ePHI for DHHS purposes.
- C. Safeguarding/Locking** - Portable devices must be kept in a locked or secured location when not in use, whether working in the office or off-site (if off-site work with ePHI is permitted by DHHS policy and the office Director).
- D. Reporting** - Any loss, theft, or actual or suspected misuse of a portable device containing ePHI or confidential information of any office shall be reported immediately to the individual responsible for maintaining the office's inventory of portable devices, the office Director and the Director of Healthcare Privacy. Where possible, communication service to electronic devices such as smartphones and cell phones will be immediately terminated and remote wiping capability implemented.
- E. Compliance** - Our workforce members will comply with this and other privacy and security policies in support of our compliance efforts. Failure to comply with this or other privacy and security policies will result in application of our Privacy and Security Sanctions Policy.

V. DEFINITIONS

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

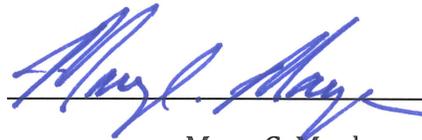
Electronic Protected Health Information (ePHI) is PHI that is stored, maintained, accessed, acquired, used, disclosed or transmitted via electronic or digital means.

VI. DISTRIBUTION

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

April 15, 2014

Date



Mary C. Mayhew
Commissioner