PURPOSE

To define a mechanism for safeguarding medical records and confidential information.

POLICY

The Agency will implement measures to safeguard medical records and confidential information against loss, destruction, tampering and unauthorized use.

PROCEDURE

I. Agency will:

A. Avoid placing medical records in unattended areas accessible to unauthorized individuals.

B. Assure medical records on desks or computers can't be read by unauthorized individuals.

C. Store medical records in a manner that minimizes the possibility of damage from fire and water.

D. Implement guidelines as to when release or removal of medical records is allowed (see policy on Medical Record Information on Release and Removal).

E. Implement guidelines regarding copying the medical record which include:

1. Consulting with the Privacy Officer before information is disclosed;

2. Which portions of the record may be copied and for what purposes the disclosure is made;

3. Documentation of the disclosure;

4. Staff accountability for protection of copies in their possession;

5. Control of the destruction of record copies.

F. Maintain confidentiality during and after normal business hours.

G. Educate staff, upon hire and annually thereafter, on steps to prevent unauthorized disclosure of medical record information.

H. Ensure retrievability of baseline data if the original medical records are destroyed.

I. Implement measures to maintain confidentiality when sending patient information by telecopier (fax) and email. Telecopier (fax) cover sheet will include a statement similar to the following and it shall appear in all email transmissions:

> "The information contained in this telefax/**email** message is legally privileged and confidential information intended only for the use of the individual or entity **to which it is addressed**. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copy of this telefax/**email** is strictly prohibited. If you have received this telefax/**email** in error, please immediately notify us by telephone and return the original message to us at the address **listed** via the United States Postal Service. Thank you."

J. Implement measures to maintain confidentiality and security when using an electronic record, Point of Care device, laptop, personal digital assistant (PDA), USB flash drive, memory card, or home computer, including but not limited to:

1. All employees using an electronic record, Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer will sign a confidentiality/security agreement form after being oriented to the electronic device. The form will include the employee's printed or typed name as well as a signature.

2. All persons using an electronic record, Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer will either be given a network and patient database username and password or they will password protect the program being used. These

passwords are not to be shared with any person. Passwords will be changed by the user at least annually or every 90 days if the Agency contracts with a Health and Human Services (HHS) agency, or following a breach of security.

3. Access to patient information on an electronic record, Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer will be limited to individuals with a legitimate "need to know" in order to effectively perform their specific job duties and responsibilities.

4. In the event an employee using electronic record, Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer is terminated, suspended or has an extended leave of more than 30 days, the user access will be inactivated or, if a laptop, data will be removed to an Agency file. The Agency will make every effort to remove confidential information from a personal Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer. Reactivation will only occur upon notification from the Administrator or supervising nurse.

5. In the event the electronic record, Point of Care device, laptop, PDA, USB flash drive, memory card, or home computer is not available, all entries will be made on the appropriate paper documents. Paper records should be carried in locked containers.

6. If using digital signatures, the above security measures must be taken and the signature must not be in an encrypted format.

7. Any concerns related to an electronic record, Point of Care device, laptop, PDA, USB flash drives, memory card, or home computer will be submitted as identified to the QAPI Committee and a report of findings will be submitted to the Board for review.

K. Security measures to be taken by authorized Agency staff using laptop and other portable media or devices may include but not be limited to:

1. Use of password management procedures (for changing and safeguarding passwords) for all portable or remote devices that store EPHI;

2. Installation of personal firewall software on all laptops that store or access EPHI or connect to networks on which EPHI is accessible;

3. Installation, use and regular update of virus-protection software on all portable or remote devices that may access EPHI;

4. Use of session termination (time-out), lock-down or other locking mechanisms for inactive or unattended laptops or other inactive portable or remote devices;

5. Prohibition of the placement of laptops or other portable media or devices in unattended areas accessible to unauthorized individuals (ex. Never leave in plain view in an unattended vehicle, hotel, public workstation, or Wireless Access Point);

6. Prohibition of transmission of EPHI (including email, Facebook, Twitter, text messaging, etc.) over open networks, such as the Internet, where appropriate, and

7. Prohibition of storage or creation of confidential information on free cloud services or social media sites.

L. If the Agency uses a Cloud Service Provider (CSP), the Agency must have a Professional Service Agreement with the CSP that will be creating, receiving, maintaining, or transmitting electronic protected health information (ePHI) on its behalf. The Professional Service Agreement must establish the permitted and required uses and disclosures of ePHI by the business associate performing activities or services for the Agency, based on the relationship between the parties and the activities or services being performed by the business associate. The Professional Service Agreement also contractually requires the business associate to appropriately safeguard the ePHI, including implementing the requirements of the Security Rule.

M. The preceding training/education and security measures will also be implemented to maintain confidentiality/security when using other kinds of devices and tools such as Smart Phones, Wireless Access Points (WAPs), Memory Cards; CDs, DVDs, backup media, Smart cards, and Remote Access Devices (including security hardware).

N. Contracted Services using electronic documentation, including electronic or digital signatures, will implement measures to maintain confidentiality/security of patient information and will provide the agency proof of such upon request.

O. If the Agency contracts with a Health and Human Services (HHS) agency, in addition to those requirements cited above, the Agency will meet the requirements for data security and privacy as outlined in the HHS Data Use Agreement (DUA), required when contracting and/or re-enrolling with an HHS agency.