Policy: The Division will implement policies and procedures to prevent, detect, contain, and correct security violations and security incidents, and to ensure all employees have appropriate access to Protected Health Information (PHI) as necessary to perform the duties and responsibilities associated with their position within the Division.

Purpose: The Division must ensure the confidentiality, integrity, and availability of all PHI it creates, receives, maintains, or transmits. In order to do so, the Division must protect against any reasonably anticipated hazards to the security and integrity of PHI, reasonably anticipate, and negate any risk of incidental or unauthorized use, disclosure or transmission of PHI. Controls that limit unauthorized access and minimize incidental disclosure of PHI while conducting business must be implemented.

SCOPE: Division Wide

REFERENCES: 45 CFR, NRS 433A.360, AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA), HITECH ACT (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL ACT DHHS Computer Acceptable Use Policy

Procedures:

I. Communication:

Any means of communicating PHI poses a risk of incidental or unauthorized disclosure. Whenever communicating PHI, observe the minimum necessary standard when determining what information to communicate. The following guidelines address most situations in which PHI is shared;

A. Telephone Conversations with individuals or authorized individuals that include PHI:

1. Requests for PHI made via the telephone must be handled cautiously. No information will disclosed without appropriate verification of identity and authority in accordance with the provisions of federal privacy and security rules. This includes, but not limited to, voice recognition with familiar individuals, confirming their social security number or date of birth, or through written authorization in the medical record.

2. Staff shall ensure that the phone they are using to convey PHI shall be is in a secure enough area to be reasonably sure that others who do not have authorization cannot overhear the conversation.

3. If the individual on the telephone is not reasonably identifiable as the client or designated representative, request the individual to appear in person at the Agency with a means of identification.

4. Under no circumstance will PHI be left on any type of an answering machine, voice mail, or any other type of device that records messages.

5. When leaving a message staff shall state their name and give a telephone number to return the call.

9. If frequently used numbers are programmed into a fax machine, the accuracy of the numbers must be tested periodically.
10. Passwords for computer access and/or electronic transmissions will not be saved, shared, written down, or stored where others might find them.

B. Electronic Transmission

1. Highly sensitive information must not be communicated via email or Fax.

   a. Electronic transmission, including email and Fax should be reserved for situations when physical separation and the need for rapid response make it impractical to use a more secure means of communication. Transmissions must be prepared and conveyed with attention to detail to ensure that PHI is disclosed only to the intended recipient;

   b. When PHI must be shared outside the Division, an alternate method of communication (i.e., standard mail) should be used whenever feasible.

   c. If an email or fax containing PHI is received in error, the sender must be informed that the message was misdirected and the misdirected email/fax must be destroyed.

   d. Passwords for computer access and/or electronic transmissions will not be saved, shared, written down, or stored where others might find them.

2. Emails:

   a. PHI must include the following privacy notice/warning:

   This message and accompanying documents are covered by the electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, and may contain confidential information intended for the specified individual(s) only. If you are not the intended recipient or an agent responsible for delivering it to the intended recipient, you are

hereby notified that you have received this document in error and that any review, dissemination, copying, or the taking of any action based on the contents of this information is strictly prohibited. If you have received this communication in error, please notify us immediately by E-mail, and delete the original message.

b. PHI must never be forwarded to a personal email account (e.g. AOL, MSN, etc) and attachments containing PHI should not be downloaded to a non-state computer.

c. When sending PHI via email, identifiable information shall not be placed in the subject line. When sending emails with attachments containing PHI, staff shall include Secure e-mail in the subject line to ensure encryption.

3. Fax transmission

a. Every fax transmission containing PHI must be accompanied by a confidential cover sheet that includes the following privacy notice/warning:

This message contains protected health information that is intended for disclosure only to the authorized recipient. Unauthorized interception and/or disclosure are violations of both the Electronic Communications Privacy Act and the Health Insurance Portability and Accountability Act. Violations may result in administrative, civil, or criminal penalties. If this document is received in error, please notify the sender immediately and destroy the document and any copies made.

b. If frequently used numbers are programmed into a fax machine, the accuracy of the numbers must be tested periodically.

c. No PHI may be included on the fax cover sheet.

C. Placement of fax machines that are used to send and receive PHI:

1. Fax machines used to send or receive PHI must be placed in an area that only the intended recipient will receive the transmission when possible.

2. All levels of supervisory staff are responsible for surveying their program area to secure and ensure fax machines are strategically placed in areas where unintended recipients are not likely to have access to fax transmissions, including PHI.

3. All staff are responsible for reporting suspected violations of this policy to heir supervisor or Agency HIPAA Compliance Officer.

D. Standard Mail:

1. Individuals responsible for opening mail or preparing outgoing mail containing PHI must be trained in the proper handling of PHI.

2. Incoming mail containing PHI must be delivered directly to the intended receiver or placed in a staff mailbox located in a non-public area, face down.

3. Subpoenas for release of PHI must be forwarded immediately to the Agency Director to ensure prompt and appropriate response.

E. Texting and Social Media

1. To ensure the confidentially, integrity and availability of the information, to protect against any reasonably anticipated threats or risks to the security or integrity of the information, and to protect against unauthorized uses or disclosures of the information, MHDS prohibits texting of PHI.

2. Use of Internet that has no bearing on the Division/Department's mission to include Social Networking, blogging, chat rooms, instant messaging is prohibited.

3. Storing unencrypted PHI on mobile devices is prohibited.

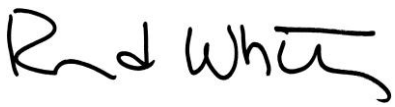
II. Monitoring MHDS Agency Office Privacy and Security Controls

A. Managers and supervisors of MHDS agencies and/or facilities or the Division or Agency HIPAA Privacy Officer will conduct a review at least one time a year utilizing the "MHDS HIPAA Privacy/Security Safeguards Checklist" which is attached to this policy. The completed reviews will be forwarded to the Division HIPAA Privacy Officer.

B. Managers and supervisors of MHDS agencies and/or facilities or the Division or Agency HIPAA Privacy Officer will conduct a review at least one time a year utilizing the Addendum MHDS HIPAA Privacy/Security Safeguards Checklist .

C. The completed reviews will be forwarded to the Division HIPAA Privacy Officer.

Each Division agency shall develop specific written procedures to implement the provisions of this policy or shall incorporate this policy into their agency policies.



ADMINISTRATOR

EFFECTIVE DATE: 4/15/03
REVIEWED / REVISED DATE: 4/15/03; 8/16/07, 9/21/12
SUPERSEDES: #6.020 – HIPAA Compliant Communications
APPROVED BY MHDS ADMINISTRATOR: 9/21/12
APPROVED BY MHDS COMMISSION: 9/21/12