DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT: **SAFEGUARDS FOR PROTECTED HEALTH INFORMATION**	POLICY NO. **500.21**	EFFECTIVE DATE **04/14/03**	PAGE **1 of 6**
APPROVED BY:  Director	SUPERSEDES	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) **1**

PURPOSE

1.1 To establish safeguards that must be implemented by the Department of Mental Health (DMH) in order to protect the confidentiality of Protected Health Information (PHI).

POLICY

2.1 Set forth below are policies establishing minimum administrative and physical standards regarding the safeguarding of PHI that must be enforced by DMH. The Department may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the safeguarding of PHI in support of their specific circumstances and requirements. The development and implementation of policies and procedures in addition to those stated herein must be approved by the Chief Information Privacy Officer.

2.2 DMH will implement appropriate administrative, technical and physical safeguards which will protect PHI from any intentional, unintentional or incidental use or disclosure that is in violation of the Department's Privacy Policies or the HIPAA Privacy Rule. This requirement applies to all types of PHI in any form, i.e., oral, paper or electronic.

2.3 The Department workforce must reasonably safeguard PHI to limit incidental use or disclosure made pursuant to an otherwise permitted or required use or disclosure.

DEFINITIONS

3.1 **"Protected Health Information"** means information that is (i) created or received by a health care provider, health plan, employer or health care clearinghouse; (ii) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, of the past, present or future payment for the provision of health care to an individual; and (iii) identifies the individual or for which there is a reasonable basis for believing that the information can be used to identify the individual.

3.2 **"Particularly Sensitive Health Information"** means PHI that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse and communicable disease information.

3.3 **"Workforce"** means employees, volunteers, trainees and other persons whose conduct in their work is under the direct control of DMH, whether or not they are paid by the County.

PROCEDURES

4.1 Administrative Safeguards

4.1.1 Incidental/Oral Communications The Department's workforce must exercise due care to avoid unnecessary disclosure of PHI through oral communications. Conversations in public areas should be avoided, unless necessary to further client care, research or teaching purposes. Voices should be modulated and attention paid to unauthorized listeners in order to avoid unnecessary disclosure of PHI. Client identifying information should be disclosed during oral conversation only when necessary to further treatment, payment, teaching, research or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones should be used only in private areas. Computer monitors, printers, fax machines, whiteboards and any other equipment that displays PHI should be place where passers-by cannot see them. The type of PHI on a sign-in sheet or when paging a client should be limited to the least amount necessary to accomplish the purpose.

4.1.2 Cellular Telephones The use of cellular telephones is not prohibited as a means of using or disclosing PHI. However, their use poses a higher risk of interception as compared to legacy landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI.

4.1.3 Telephone Messages Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the client has requested an alternative means of communication pursuant to DMH's Right to Request Confidential Communications Policy. However, each provider and/or clinic should limit the amount of PHI that is disclosed in a telephone message. The content of appointment reminders should not reveal Particularly Sensitive Health Information, directly or indirectly. Telephone messages regarding test results or that contain information that links a client's name to a particular medical condition should be avoided.

4.1.4 Faxes The following procedures must be followed when faxing PHI:

4.1.4.1 Only the PHI necessary to meet the requester's needs should be faxed.

4.1.4.2 Particularly Sensitive Health Information should not be transmitted by fax, except in emergency situations of if required by a government agency. If Particularly Sensitive Health Information must be faxed, the recipient should be notified immediately prior to the transmission and, if possible, the sender should immediately confirm that the transmission was completed.

4.1.4.3 DMH should designate employees who can fax, or approve the faxing of, PHI. Unauthorized employees students and volunteers should never fax PHI.

4.1.4.4 Unless otherwise permitted or required by law, a properly completed and sign authorization must be obtained before releasing PHI to third parties for purposes other than treatment, payment or health care operations as provided in the Department's Authorization Policy. PHI may be faxed to an individual if he/she requests access to their own PHI in accordance with the Department's Client's Right to Access to Protected Health Information Policy.

4.1.4.5 All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. Use the **DMH Fax Cover For Transmitting PHI** (Attachment I).

4.1.4.6 Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be pre-programmed into fax machines or computers to avoid misdialing errors. Pre-programmed numbers should be verified on a routing basis. The numbers of new recipients should be verified prior to transmission.

4.1.4.7 Fax machines must be located in secure areas not readily accessible to visitors and clients. Incoming faxes containing PHI should not be left on or near the machine.

4.1.4.8 Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.

4.1.4.9 All instances of misdirected faxes containing PHI should be investigated and mitigated pursuant the Department's Mitigation Policy.

4.1.5 Mail PHI should be mailed within the County's departments in sealed envelopes. PHI mailed outside the County's department should be sent via first class and should be concealed. Appointment reminders may be mailed to clients unless the client has requested an alternative means of communication pursuant to the Department's Right to Request Confidential Communications Policy.

4.2 Physical Safeguards

4.2.1 Paper Records Paper records and clinical records must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

4.2.1.1 Paper records and clinical records on desks, counters or nurses stations must be placed face down or concealed to avoid access by unauthorized persons.

4.2.1.2 Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

4.2.1.3 Original paper records and clinical records should not be removed from the premises unless necessary to provide care or treatment to a client or required by law.

4.2.1.3.1 DMH workforce members should not remove paper records or clinical records for their own convenience.

4.2.1.3.2 Any paper records and clinical records removed from DMH premises should be checked out according the Department policies and procedures and should be returned as quickly as possible.

4.2.1.3.3 The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out.

4.2.1.3.4 Paper records and clinical records that are removed from DMH premises must not be left unattended in places where unauthorized persons can gain access.

4.2.1.3.5 Paper records and clinical records must not be left in unlocked automobiles or in view of passers-by.

4.2.1.3.6 The theft or loss of any paper record or clinical record should be reported to the designated Privacy Officer so that mitigation options can be considered.

4.2.2 Destruction Standards PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI should be destroyed or shredded. Magnetic media and diskettes containing PHI should be overwritten or reformatted.

4.2.2.1 PHI files and documents awaiting disposal must be stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

4.2.2.2 Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.

4.2.2.3 Centralized bins or containers used for disposed confidential information must be sealed, clearly labeled “confidential”, “PHI” or some other suitable term and placed in a locked storage room.

4.2.2.4 Facilities or sites that do not have protected storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

4.2.3 Physical Access

4.2.3.1 Persons authorized to enter areas where PHI is stored or viewed must wear identifiable DMH employee badges or be escorted by an authorized County employee.

4.2.3.2 Persons attempting to enter an area where PHI is processed must have prior authorizations by DMH management.

4.2.3.3 Employees must not allow others to use or share their badges and must verify access authorization for unknown people entering an area where PHI is stored or processed.

4.2.3.4 Terminated or transferred personnel must be escorted in areas where PHI is stored or processed.

4.2.4 Escorting Visitors or Clients Visitors and clients must be appropriately monitored when on Department premises where PHI is located to ensure they do not access PHI about other clients without permission. This means that persons who are not part of the DMH workforce should not be in areas in which clients are being seen or treated or where PHI is stored without appropriate supervision.

4.2.5 Computer/Work Stations Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. Suggested means for ensuring this protection include:

4.2.5.1 Use of polarized screens or other computer screen overlay devices that shield information on the screen;

4.2.5.2 Placement of computers out of the visual range of persons other than the authorized user;

4.2.5.3 Clearing information from the screen when not actually being used;

4.2.5.4 Using password protected screen savers when computer workstations are not in use.

4.3 Technical Safeguards

4.3.1 Technical safeguards regarding the protection of PHI maintained in electronic form will be developed as part of the efforts to implement security best practices and the HIPAA Security Regulations and will be incorporated into this policy by reference.

4.3.2 Until appropriate securing mechanisms are implemented and supporting policies are published, DMH workforce members will not be permitted to use the following electronic systems for the distribution, processing or storage of PHI:

4.3.2.1 Electronic mail or e-mail;

4.3.2.2 Personal Digital Assistance (PDA), such as Palm Pilot, iPAQ, Blackberry or other similar devices.

4.3.2.3 Wireless networks

DOCUMENT RETENTION

5.1 This policy will be retained for a period of at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

AUTHORITY

HIPAA, 45 CFR, Section 164.530 (c)(1)

ATTACHMENTS

Attachment I DMH Fax Cover For Transmitting PHI

DEPARTMENT OF MENTAL HEALTH

DMH FAX COVER FOR TRANSMITTING PHI

FAX DETAILS

Date Transmitted: _____ Time Transmitted: _____

Number of Pages (including cover sheet): _____

Intended Recipient: _____

TO	FROM
Name: _____	Name: _____
Facility: _____	Facility: _____
Address: _____	Address: _____
Telephone #: _____	Telephone #: _____
Fax #: _____	Fax #: _____

Documents being faxed:

- ☐ Clinical Records
- ☐ Other: _____

CONFIDENTIALITY STATEMENT

This facsimile transmission may contain information that is privileged and confidential and is intended only for the use of the person or entity named above. If you are neither the intended recipient nor the employee or agent of the intended recipient responsible for the delivery of this information, you are hereby notified that the disclosure, copying, use or distribution of this information is strictly prohibited. In addition, there are federal civil and criminal penalties for the misuse or inappropriate disclosure of confidential patient information. If you have received the transmission in error, please notify contact person immediately by telephone to arrange for the return of the transmitted documents to us or to verify their destruction.

VERIFICATION OF TRANSMISSION OF PHI

Please contact _____ at _____ to verify receipt of this Fax or to report problems with the transmission.

I verify the receiver of this Fax has confirmed its transmission:

Name: _____ Date: _____ Time: _____

DMH Treatment Team Representative