

**COMMUNITY MENTAL HEALTH CENTER
OF EAST CENTRAL GEORGIA
POLICY**

SUBJECT: Security of Clinical Information
POLICY NUMBER: PIM 3.02
EFFECTIVE DATE: 04/01/2003
RESCISSION DATE:

SUPERSEDES:	REVIEWED DATE:	04/01/2003
Policy # IM-4	LAST REVISION DATE:	04/01/2003

POLICY:

It is the policy of the Community Mental Health Center of East Central Georgia to secure clinical records, computerized clinical information and clinical information transmitted/received via facsimile (fax) machines.

PROCEDURES:

I. Clinical Records:

A. Outpatient and Day Services:

1. All records are stored in a secure area, i.e., a room designated for clinical records or a locking file cabinet.
2. All records are signed out and checked in using the CMHC's "outguide" procedure. The staff person signing the record out is accountable for the record until it is checked into the record storage area.
3. All clinical records will be returned to the record storage area by the end of the business day.

B. Residential Services:

1. As clinical records are in continuous use the responsibility for clinical record security is assigned to program services supervisors and staff.
2. Program managers are accountable for designing and maintaining methods to assure the security of clinical records.

II. Data Security:

- A. Users shall be automatically logged off their workstations after a maximum period of 15 minutes of inactivity.
- B. The Security Officer shall review an audit trail, produced by Unicare or existing legacy systems, of all accesses and changes to client data on a monthly basis and report violations to employee supervisors and other appropriate staff.
- C. Access to CMHC networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of designated MIS staff.
- D. Designated MIS staff shall back up data to backup tapes and backup

Subject: Security of Clinical Information

Policy PIM 3.02

Page 2

- CMHC databases in their entirety nightly. Client and other data shall be backed up incrementally nightly and fully on Saturdays.
- E. Designated MIS staff shall ensure that all media has been thoroughly cleansed of any client data before the media is surplus or disposed of.
 - F. Access to media containing client data shall be controlled, by designated MIS staff through:
 - 1. Access control lists to network media
 - 2. Physical access control to hardware
 - 3. Purging data on any type of media before it is surplus or discarded.
 - 4. Storage of data on media that is backed up
 - G. Designated staff in the MIS office shall maintain an up to date Standards List, which prescribes appropriate procedures and practices for data security purposes.
 - H. Virus protection for the network shall be maintained by designated MIS staff, pursuant to the virus protections procedures listed below.
 - 1. Email Servers. All email servers shall be protected using the email-specific anti-virus software.
 - 2. Network and Member Servers. All network and member servers shall be protected using anti-virus software.
 - 3. Workstations, laptops, PDA's.
 - a. All workstations, laptops, PDA's or any other device that connects to the Network shall be protected using the anti-virus software for that device installed by designated MIS staff.
 - b. Equipment that has not been purchased by CMHC shall not be allowed to connect to the CMHC network.
 - 4. Virus signature updates:
 - a. Anti-virus server software shall be configured by designated MIS staff to check for virus signature updates daily.
 - b. Anti-virus PC's, laptops, PDA's software will check for virus signature updates hourly from the master console of the anti-virus program, as a result of MIS staff actions.
 - c. Special virus signature updates created in the event of a known virus, will be manually pushed by designated MIS staff to all servers, PCs, laptops, and PDAs within 24 hours of the time the receipt of the update has been received at the master console.
 - 5. Software Updates. Anti-virus software shall be kept by designated MIS staff at the current release or no more than one release below the most current release version.
- III. Facsimile (Fax) Machines.
- A. Fax machines are located in secure areas.
 - 1. Entrances to areas where fax machines are located have "Authorized Staff Only" signs posted.
 - 2. A person is assigned to periodically check for and distribute incoming documents.
 - B. When faxing PHI the individual must:
 - 1. Insure that documents are handled securely/confidentially.

Subject: Security of Clinical Information

Policy PIM 3.02

Page 3

2. Insure that the document is delivered to the addressee.
 3. Verify the destination when sending number for the first time.
 4. The individual will call the sender to determine the disposition of a misdirected fax transmission and assist the sender in accordance with their request.
- C. CMHC includes a confidentiality notice with clinical information transmitted via fax machine (see attachment I).
 - D. All machines must be stocked with fax coversheets that are within arms reach of the user.
 - E. Any incoming faxes that do not contain a coversheet must be covered before they are placed in a storage tray.
 - F. No PHI can be placed on the coversheet.
- IV. The CMHC workforce shall not load software, from any source, onto their assigned workstation or any other CMHC equipment. This software includes but is not limited to software from the Internet, a CD, or a floppy diskette. Software shall be loaded on workstations only by designated MIS employees.
- V. CMHC workstations shall be situated by respective designated MIS staff to prevent more than incidental observation of work product.
- VI. Failure of workforce members to comply or assure compliance with this policy may result in disciplinary action, including dismissal.
- VII. The Security Officer shall collect information for the purpose of providing feedback to the Executive Director and to the Leadership Team regarding trends and issues associated with compliance with this regulation.

ATTACHMENT:

- I. [Facsimile Transmittal Sheet \(SBHS Form #403 9/05\)](#)

REFERENCES:

- I. Public Law 104-191: 104th Congress

Acting Executive Director

Date

CSB Chair

Date