

## **MANAGEMENT INFORMATION SYSTEM**

### **Policy**

Mid-Ohio Psychological Services will develop and maintain a Management Information System (MIS) to track client involvement in services, billing records, clinical information, and client demographic information. This MIS system will interface with ODMH/ODADAS MIS systems in accordance with guidelines established through the MACSIS information system. The MIS system will maintain the same level of confidentiality and completeness as the hard copy client record system and comply with HIPAA rules.

The MIS Coordinator, Executive Director and the Administrative Coordinator will develop the procedures. The MIS Coordinator will be responsible for implementing them.

### **Procedure**

The MIS system has considered the following areas in designing and maintaining the agencies system:

Authentication – providing assurance regarding the identity of a user and corroboration that the source of the data is as claimed; Users at Mid-Ohio are required to log on to the computer system with assigned usernames and passwords to insure that rogue users are not given access to system resources.

Authorization – the granting rights allow each user to access only the functions, information, and privileges required by his/her duties; Users at Mid-Ohio are assigned levels of security, limiting the areas of the MIS system that the user can access. These levels of “user rights” are determined based on the staff work duties by the MIS coordinator and the Executive Director.

Integrity – ensuring that information is changed only in a specific and authorized manner. Data, program, system and network integrity are all relevant to consideration of computer and system security; Depending on the level of assigned security, users are restricted to what files they are allowed to modify and install on the MOPS computer system. These limitations are based on the design of the system and determined by the MIS coordinator and the Executive Director.

Audit trails – creating immediately and concurrently with users actions a chronological record of activities occurring in the system; A security auditing system is currently being developed to track the log on and log off attempts of each computer. Access to word processing files can be identified as to who saved them last. Within the Clinical Information System, any access of records by

persons who are not clinically attached to the case require a “reason for access” to be recorded in the system.

Disaster Recovery – the process for restoring any loss of data in the event of fire, vandalism, disaster, or system failure; Daily backups are performed to insure that files can be recovered in the event of a disaster. Procedures are in place to insure that at least one copy of the MIS data is stored in a separate building (in the in the Accounts Payable Office) from the servers. This data is kept in a fire resistant safe and updated at least weekly. A backup of the core MIS system (XaktClaim Database, CIS Database, and Financial Records) will be made at least daily and all MIS data will be backed up weekly (Notes, ancillary databases, etc.).

Data storage and transmission – physically locating, maintaining and exchanging data; the computer system is in an area that is locked to restrict access to only supervisory staff. There are redundant drives and power systems to insure that data is maintained intact. Data is encrypted when sent outside of the physical MOPS site to ensure that data is not intercepted or tampered with.

Electronic signatures – a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual’s electronic signature; a computer-generated signature code created for an individual; or an electronic image of an individual’s handwritten signature created by using a pen computer. Client record systems utilizing electronic signatures shall comply with section 3701.75 of the Revised Code. Mandatory passwords are utilized for everyone who accesses the computer system to insure that only authorized personnel are allowed access.

## **MIS Risk Management**

Mid-Ohio has evaluated the risks posed to the agency’s MIS system in many ways and risks will continue to be analyzed as the system evolves.

### Password Management

All persons accessing the computer system must utilize their assigned user name and generated password. No person will be allowed to access the computer system without a user name and password. Staff shall not allow other persons to use any of the computer system using their user name/password. Staff are required to safeguard their password and change their password if they think someone else has obtained it. The agency uses passwords that are classified as “complicated”. These passwords require combinations of uppercase and lower case characters, numbers, and symbols with a minimum length of eight letters. Passwords must be changed every 90 days and are only reusable after 180 days. This authentication provides assurance regarding the identity of a user and corroboration that the source of the data is as claimed.

All staff must logoff or lock the desktop system when they are not at the station.

#### Data Access

Access to the various levels of the system is assigned based on the agency staff hierarchy and job duties. Individual directories are password protected and can only be accessed by staff whose job duties depend on access to the computer files in those directories.

#### Sanction Procedure

Staff who violate the agency's MIS policy are subject to disciplinary action as identified in the agency's personnel policy and acknowledged when signing the agency's confidentiality and security agreement. (Confidentiality and Security Agreement Form)

#### Information Systems Activity Review

The security auditing system includes a log in/log out record that is maintained on the server for approximately 30 days. These log in/log out records are tracked in Event Viewer (security) in Windows 2003. Internet logs are maintained for one year, they are tracked through email and the system log service.

#### Termination Procedures

All access to the agency's MIS system will be terminated when all necessary work has been completed by the employee leaving the agency. Access will be restructured in the event that employees' job duties are significantly changed.

#### Training

All staff are required to complete HIPPA and other security related training using the agency's on-line training program annually or more frequently if needed due to changes. Staff will also be updated via email of any concerns that arise related to the security, usage etc of the MIS system.

#### Security Reminders and Updates

Staff will be notified by email of updates to the security practices of the agency.

#### Protection from Malicious Software

Unauthorized software is removed from the system whenever discovered. Staff are not to download any software onto agency computers without the approval of the MIS Coordinator and the Executive Director.

### Log-in Monitoring

The agency will implement system procedures that require that if there are three failed attempts to log-in properly to the system, the log-in will be disabled for 30 minutes.

### Security Incident Procedures

Security incidents are to be reported immediately to the MIS Coordinator and Executive Director. Incidents will be documented using email and handwritten notes that will be maintained by the MIS Coordinator. The MIS Coordinator will review logs and any other documents regarding reported incidents to obtain information on the extent of the incident and to make changes to protect the system against any future incidents. The agency will notify clients, staff, or other applicable parties if it is deemed necessary by the nature of the incident.

## **Contingency Plan**

### Data Backup Plan

The major areas of the MIS system are backed up on a daily basis on a removable drive system.

### Disaster Recovery Plan

Daily backups are performed to insure that files can be recovered in the event of a disaster. This would result in only a few hours of data being lost. The MIS Coordinator insures that at least one copy of the MIS data is stored weekly the Accounts Payable Office in a fire resistant safe.

Servers are built from standard parts so they can be replaced quickly in the event of a disaster. Some redundant hardware is maintained on-site to be used for replacements when needed.

In the event of a disaster the following steps will be taken:

1. Verify that hardware is operational; replace parts as necessary.
2. If OS is missing or corrupt, retrieve offsite storage of Ghost Image for server.
3. Restore Ghost Image to server primary drive.
4. Restore data from latest valid on-site or off-site backup to data drives on server.
5. Documentation throughout this process will be maintained by the MIS Coordinator.

### Emergency Mode Operations Plan

As access to application and data are restored, the security of the agency's electronic protected health information will be maintained because log-in and password requirements will be in place.

### Testing and Revision Procedures

The agency has developed and used the disaster recovery plan due to hardware failure and the plan has worked and will continue to evolve with the agency.

### Applications and Data Critically Analysis

Applications and data will be restored in the following order if at all possible:

Xakt Claim – Contains client contact information, agency schedules, and billing information.

CIS – The agency's clinical information system that contains all client treatment information.

QuickBooks – Contains the agency's payroll, accounts payable and financial records.

Exchange Server – Enables the agency's email and Internet capabilities.

## **Facility Access Controls**

All employees have keys to the main entrances of the building and their individual workspace if applicable. Only the Executive Director, MIS Coordinator, Supervisors and Maintenance Staff have keys to the areas that contain the servers for the electronic protected health information.

### Contingency Operations

The MIS Coordinator has access to all areas that would need to be entered to restore lost data during an emergency.

### Facility Security Plan

The areas that contain the MIS system that contains the electronic protected health information are secured behind locked doors beyond the main entrances. In addition,

windows in the agency are covered by blinds and or curtains to prevent viewing from outside of the building.

#### Access Control and Validation Procedures

Access to “staff only” areas of the agency are restricted by doors. An employee accompanies any visitors to the agency that are allowed beyond the common areas.

#### Maintenance Records

A maintenance log will be maintained to document repairs and modifications to the physical components of the facility that are related to security including hardware, walls, doors, and locks. The Administrative Coordinator will maintain these logs.

### **Transmission Security**

Data is 128-bit encrypted and/or password protected when sent outside of the physical MOPS site to insure that data is not tampered with. If the data would be intercepted, it is unusable. The agency also uses Secure Socket Layer and 128-Bit encrypted VPN.

The agency cannot certify that information was received however, if it is intercepted it will reasonably unreadable.

### **Workstation Use**

All workstations will be located in employee work areas; access to these areas will be restricted to employees only. In areas that are open to client access, the employees are to lock workstations and use screen savers to block client access to electronic protected health information. No clients will be allowed to sit at or use workstations.

#### Device and Media Controls

All workstations within the agency have inventory tags so there location can be monitored within the agency. All equipment used in off site locations are also inventoried.

Protected Health Information (PHI) is not to be stored on the local machines in the agency. No PHI is to be copies to media including but not limited to jump drives, CD/DVD's, disks, or removable hard drives without the explicit consent of the MIS Coordinator and/or the Executive Director. If PHI is placed on removable media, it is to be encrypted with at least 128 bit encryption.

### Disposal

All computers and storage devices are dismantled and destroyed when they are no longer used by the agency. Media storage is either physically destroyed or electronically destroyed to prevent accidental release of PHI

### Media Re-use

Media reused within the agency include dictation tapes, and these are individually run through a tape eraser and then reused by clinical staff, floppy disks are reformatted, and optical media are destroyed or reformatted.

### Accountability

An inventory list is maintained for all agency property.

### Automatic Logoff

The agency workstations are set so that after a short period of inactivity that the screen saver locks the computer. Settings are in place to log users off during restricted hours.

### Encryption and Decryption

The agency's *Watchguard* firewalls use at least 128-bit encryption on VPN. Zip files are password protected and at least 128-bit encrypted.

## **Audit Controls**

Log in/Log Outs are recorded in logs. Files show the last user to save the document. The agency's Clinical Information System logs all access to files and will also record a reason the file is accessed for anyone who does not require clinical access to the file. The agency also utilizes an electronic check-in/check-out program for the client charts.

The MIS Coordinator is the primary person who can log on to the system as Administrator and can delete or modify key data. The Executive Director has these privileges as well to act as a back-up if the MIS Coordinator is unavailable to do so. No other staff will be granted Administrative privileges on the servers with out the consent of the Executive Director.

## **Use of Consultants**

From time to time, consultants may be used to aid in developing/maintaining the Management Information System. Whenever consultants are used, the credentials and reliability of the consultant will be reviewed prior to the consultant gaining access to the MIS system.

### Business Associate Contracts

Mid-Ohio Psychological Services, Inc utilizes a Business Associate Agreement with all outside agency that may have contact with protected health information. Business Associate Contracts will be terminated at the completion of the project for which they were signed. Contracts will be terminated if behaviors or incidents warrant such action to protect electronic health information.

### Access to System

Any consultant having access to the MIS system will be provided a user name/password based on the same criteria applied to agency staff, thus allowing control to only those areas that they require access to and a means for auditing their access.

Rev.01/23/06