Edwin Fair Community Mental Health Center

Information Technology Plan

2014 - 2015

Edwin Fair CMHC, Inc. operates offices in six counties, Kay, Osage, Nobel, Grant, Garfield and Payne; three in Kay County, one in Osage County, one in Nobel County, one in Grant, one in Garfield, and two in Payne County. Covering service areas for a total of seven counties, the above mentioned and Pawnee. Pawnee service area is covered out of the Payne county offices.

Hardware

The agency has approximately 108 computers within the seven locations. Computers are replaced every five years from date of purchase. Computers are placed on a rotation so that there are manageable amounts replaced hardware each year. Information Technology Coordinator or assigned staff will maintain detailed lists of all hardware being owned and operated by Edwin Fair CMHC, Inc.

Management, Coordinators and other staff that travel from site to site are provided with a lap top; all others are issued desk top units. Within the next two years the agency will consider purchasing more laptops for clinical staff as we move toward the electronic records.

Software

All workstations run the Windows 7 Pro operation system and all computer that had the XP operating system have been retired. The programs loaded on all computers are Microsoft Office 2013, all are using the Office 365 product, and our in house electronic record software, ThinkHealth.

**Security and Confidentiality**

Each user is expected to make correct and sufficient use of the security and confidentiality tools provided for each computer system. All users will be trained on Computer and Data security and confidentiality at the new hire orientation with additional training at least once a year.

The ultimate responsibility for the security and confidentiality of programs, data, and other information rests with the users. Therefore, users must understand and use the security features of the computers.

Each user is expected to maintain security and confidentiality in appropriate ways such as:

* Keeping the password and other type of authorization source;
* Not sharing passwords or other authorization with any person or group;
* Selecting a password and changing it frequently;
* Not using commonly used names or numbers;
* Leaving your workstation for a long period of time without logging off.
* Understanding the level of protection each computer system automatically applies to data files and supplementing it, if necessary, for sensitive information.
* Be aware of computer virus and other destructive computer programs, and taking steps to avoid being a victim of unwitting carrier.

Each user is responsible for protecting their own systems from power surges, data overload, alterations, and, deletions or overwrites.

Unauthorized installations or alterations of software’s computer configurations are strictly prohibited. Requests for software other than the standard installed software should be made directly to the MIS Coordinator.

**NETWORK ACCESS:**

Network access and rights are assigned based on job duties or responsibilities.

Network security is maintained by assigning different work groups:

- Read Only

- Data Processing

- Support

- Supervisory

- Systems Administration

The purpose of use of the internet is to support research and education in mental health related fields as well as to support the administrative functions of the Center.

The internet resources may not be used to upload, download, or distribute unethical or inappropriate subjects.

The internet may not be used to download or upload software and programs in any of the center's computer systems.

Users must not remove, alter, or damage configurations or set-ups, software or hardware on the center's computers.

The internet is not to be used to develop personal web pages using the center's name.

Access to confidential information in any computer files will be consistent with the policies and procedures established in the Edwin Fair Policies & Procedures manual.

**INTERNET SECURITY:**

Staff will not give personal or the center's password to any other individuals. The center's password is not to be used outside the center.

Staff will not reveal company or personal addresses, phone numbers, or any personal identification numbers over the internet.

All users must know and learn the warning signs of the internet. Unfamiliar signs must be reported immediately, including missing files or changes in configuration. Inexperienced users need to submit or report any or all signs or warnings to the MIS Coordinator before resuming the use of the internet. Beginners must not use the internet without proper orientation from the MIS Coordinator.

Users must not participate in surveys, mail lists, or chain letters over the internet.

**INTERNET ETIQUETTE:**

All users must refrain from illegal or unethical use of the internet that is inappropriate to your business function and responsibility.

Users must respect intellectual property by only downloading information or computer files with proper permission and authorization from your MIS Coordinator.

Users must respect the privacy of others. All forms of information and communication, such as e-mail messages accessible via network should be assumed as private property.

Users must not misrepresent themselves, or gain unauthorized access either outside or inside the center.

Users must restrict use of chat lines, group discussions, or games from the internet.

Users must not use inappropriate or abusive languages in any of the center's e-mail accounts.

Users must not download inappropriate graphics, pictures, or images from the internet.

Users must not participate in any vandalism, such as downloading of unauthorized software, e-mail messages from unknown sources, or viruses from the internet.

Users must not send advertising or messages to multiple recipients using the company name or account without prior authorization.

The internet resources may not be used to infringe on copyrights or to plagiarize materials, violate licensing agreements using the center's name or access code.

Internet resources or materials are not to be used as guidelines in dealing with consumers or achieving or change the center's objectives.

**ELECTRONIC RECORDS AND CONSUMER DATA**

To prescribe practices which secure electronic consumer protected health information in compliance with federal law and best information management practices and in according with 45 CFR 164.530 (c) (1) and (2), and 45 CFR Part 2.

Applies to Edwin Fair CMHC, Inc., its facilities and workforce.

(1) Contents

(A) Definitions

(B) Data Security

(C) Sanctions

(D) Review Process

(2) Definitions

(A) Computer Systems - Computers connected to local communication networks, database storage or electronic records systems, Internet or email.

(B) Edwin Fair CMHC, Inc. Network - Electronic network allowing access to the EFC's personal computers, facility-based systems, and centrally-based systems (e.g. Windows Servers, Citrix, etc.) and electronic data.

(C) Local Area Network - Electronic network access allowing access to an individual facility's electronic data and computers.

(D) Network attached computer - Any computer with access to a local area network and/or the EFC network.

(E) EFC Workforce - Includes employees, volunteers, contract workers, trainees and other persons who are in an EFC facility on a regular course of business. This shall include client workers employed by the EFC or any of its facilities.

(F) Client/Consumer - Consumer, any individual who has received or is receiving services from a Department of Mental Health state operated facility.

(G) Restricted access - Computer systems with access limited to specific systems, activities, or files.

(H) Chief Security Officer (Chief Security Officer) - Individual designated by the EFC to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other EFC data in compliance with federal and state laws and regulations.

(I) Local Security Officer (LSO) Individual designated by the Director to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(J) Media - Backup media, hard drives, floppy diskettes, CDs, zip drive cartridges, optical and paper hard copies.

(K) Protected Health Information (PHI) - Individually identifiable health information.

(L) CIMOR - Consumer Information Management Outcomes and Reporting systems.

(3) Data Security

(A) Users shall shut down their computer when exiting their room/area.

(B) The Chief Security Officer shall review all reported violations of accesses and changes to client data on a monthly basis and report violations to employee supervisors and EFC Management Team.

(C) Access to EFC networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of the designated EFC IT Department.

(D) IT Department shall review Datto back up on a regular basis. This is also monitored by the Interworks, Inc. though processes on the Internet

All other locations have backups performed nightly to backup media. Client information and all other data shall be differential backed up nightly and fully every 4th Monday.IT Department will daily check to see that backup were made and media has been rotated.

(E) IT Department shall ensure that all media has been thoroughly cleansed of any client data before the media is disposed of,

(F) Access to media containing client data shall be controlled by the IT Department through the following but not limited to:

1. Access control list to network media.

2. Physical access to EFC hardware.

3. Purging EFC data on any type of media before it is discarded.

4. Storage of data on media that is backed up shall be kept offsite.

(G) IT Department shall review the Policy & Procedure manual annually for appropriate procedures and practices for data security purposes.

(H) Virus protection / Spyware for the EFC network shall be maintained by IT Department pursuant to the EFC virus protection / Spyware procedures listed below.

1. E-mail’s - All EFC email shall be protected using the anti-virus / Spyware software…

2. Network and Member Servers. All network and member servers shall be protected using the anti-virus / Spyware software.

3. Workstations, laptops, PDAs

a. All workstations, laptops, PDAs or any other device that connects to the EFC network shall be protected using the anti-virus / Spyware software.

b. Equipment that has not been purchased by EFC shall not be allowed to connect to the EFC network without prior approval from the IT Department.

4. Virus signature updates

a. Anti-virus / Spyware server software shall be configured by IT Department to check for virus signature updates daily.

b. Anti-virus / Spyware for PC, laptops, PDAs software will check for virus signature updates daily from the master console of its anti-virus program.

c. Special virus signature updates created in the event of a known virus will be manually pushed by the IT Department 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 / Spyware software shall be kept by the IT Department at the current release or no more than one release below the most current release version.

6. Software Support. The IT Department shall maintain a support contract with the anti-virus / Spyware software vendor(s) to ensure uninterrupted support.

7. Attachments. To avoid potentially virus-carrying attachments, all EFC staff will be warned that attachments are capable of malicious software. Not to open any attachments from some they don’t know or have received unexpectedly.

(I) The EFC workforce shall not load software from any source onto their assigned workstation or any other EFC equipment. This software includes but is not limited to software from the Internet, a CD, a Thumb drive, or a floppy diskette. Software shall be loaded on workstations only by the IT Department designated staff.

(J) EFC workstations shall be situated by the IT Department or designated EFC staff to prevent more than incidental observations of work product.

(4) Sanctions. Failure of work force members to comply or assure compliance with the policy and procedures outlined in this document may result in disciplinary action, including dismissal.

(5) Review Process. The Chief Security Officer shall collect information from the LSO's during the month of April each year beginning in 2004 for the purpose of providing feedback to the Director, IT Department and to the Executive Team regarding trends and issues associated with compliance with this regulation.

**USER ACCESS TO ELECTRONIC DATA**

It is the policy of the Edwin Fair CMHC, Inc to secure our consumer's protected health information (PHI) in compliance with federal law and federal regulations at 45 CFR 164(c)(l) and (2), and 42 CFR Part 2. To assist in assuring that protection, it is the practice of Edwin Fair CMHC, Inc. to assure that its workforce recognizes the importance of such security provisions, and affirmatively acknowledge those guidelines.

**Procedure:**

Applies to Edwin Fair CMHC, Inc., its facilities and workforce

(1) Contents

(A) Definitions

(B) General

(C) User Access to EFC Data

(D) Training on Access

(E) Required Confidentiality Agreement

(F) Password Management

(G) Sanctions

(H) Review Process

(2) Definitions

(A) Computer Systems - Computers connected to local communication networks, database storage or electronic records systems, Internet or email.

(B) Edwin Fair CMHC, Inc. Network - Electronic network allowing access to the EFC's personal computers, facility-based systems, and centrally-based systems (e.g. Windows Servers, Citrix, etc.) and electronic data.

(C) Local Area Network - Electronic network access allowing access to an individual facility's electronic data and computers.

(D) Network attached computer - Any computer with access to a local area network and/or the EFC network.

(E) EFC Workforce - Includes employees, volunteers, contract workers, trainees and other persons who are in an EFC facility on a regular course of business. This shall include client workers employed by the EFC or any of its facilities.

(F) Client/Consumer - Any individual who has received or is receiving services from Edwin Fair CMHC.

(G) Restricted Access - Computer systems with access limited to specific systems, activities, or files.

(H) Chief Security Officer (CSO) - Individual designated by the EFC Executive Director to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other EFC data in compliance with federal and state laws and regulations.

(I) Local Security Officer (LSO) Individual designated by the Executive Director to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(J) Media - Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, optical, and paper hard copies.

(K) Protected Health Information (PHI) - Individually identifiable health information.

(L) Client Work Program - any number of DMH programs which employ consumers of the Department.

(M) Confidentiality Agreement – Agreement between any business partner with which EFC shares client data which sets forth confidentiality requirements and limitations necessary for working with client, facility, and the EFC’s information

(3) General:

(A) Management's Right to Access Information

1. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), the members of the Administrative staff, the CSO, and the LSO's shall have complete access to all email and Internet activities. No electronic communications sent or received are considered private to the employee. The members of the Administrative staff, the CSO, and the LSO's shall have the right to monitor messages and Internet use as necessary to assure efficient and appropriate use of the technology.

2. Each of the electronic communications technologies may create electronic records that are easily saved, copied, forwarded, retrieved, monitored, reviewed, and used for litigation. All electronic records are the property of the EFC and can be accessed and used by management when:

a. A legitimate business need exists that cannot be satisfied by other means; or

b. The involved employee is unavailable and timing is critical to a business activity; or

c. There is reasonable cause to suspect criminal activity or policy violations, or

d. Law, regulation, or third-party agreement requires such monitoring

3. These disclosures of electronic records may be made without prior notice to the staff members who sent or received the communications. Staff members should not assume that any electronic communications are private.

(4) User Access to Electronic EFC Data

(A) To gain access to any EFC PHI, EFC workforce members are required to complete the EFC Staff Access Request Form as appropriate. Such access shall be limited to the minimum necessary amount of PHI to accomplish the purpose of any requested use or disclosure of PHI.

1. The appropriate supervisor or manager must approve the request(s) in writing.

2. The request form(s) must be submitted each time a user's access status changes.

3. Users will be assigned a unique user ID by the CSO.

4. User IDs will be password protected.

(B) All users shall be required to protect confidential data pursuant to DOR 8.040, Access to Consumer Protected Health Information. (EFC Staff, Volunteers or Students)

(C) All facilities shall maintain a Business Continuity/Disaster Recovery Plan, approved by the Chief Security Officer to assure continued operations in the event of an emergency.

(D) No EFC client/consumer or volunteer shall have access to or any other EFC client demographic system, or be allowed to input information to local systems that may be used to feed or modify those systems unless they are employed under the Client Work Program defined in this policy and have signed the confidentiality statement, or unless authorized by the consumer. Any proposed client/consumer access shall include documentation of the client/consumer reviewing and agreeing to a confidentiality statement. Documentation shall include: the types of systems and files accessed.

(E) Such client/consumer access shall be approved by the EFC Executive Director, or their designee.

(5) Access to Electronic Media - Internet and Email

(A) Users are required to abide by the guidelines of this Policy and Procedure and all other computer related Policies and Procedures in this manual when using the Internet or email.

(B) No client PHI can be sent without encryption. The use of chart numbers as an identifier is deemed appropriate.

(C) The Email Disclaimer Provision should be used on all email sent: "This electronic message contains information from Edwin Fair Community Mental Health Center, Inc., which may be confidential or privileged. This information is intended only for the individual/entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents of this information is prohibited. If you have received this transmission in error, please notify the Administrative Offices of Edwin Fair Mental Health Center, Inc. immediately by telephone (580-762-7561) or electronic e-mail (jim.henderson@edwinfair.com or efc.tech.support@edwinfair.com) Please permanently delete this message and any copies. Thank You."

(D) Opening Attachments - Do not open an attachment sent to you from anyone you do not recognize.

(6) Training on Access. All EFC employees, client/consumers and volunteers must receive the privacy training required by DOR 8.090.

(7) Required Confidentiality Agreement

(A) EFC workforce members that receive or maintain PHI shall be required to agree to the security of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement pursuant to DOR 8.040. A copy of the signed confidentiality statement shall be maintained in the personnel file of EFC staff.

(8) Password Management

(A) Passwords shall not be shared.

(B) Passwords shall be changed immediately if user is aware that someone else knows it.

(C) Users shall not change their passwords while others are present.

(D) Passwords should contain four to eight characters.

(E) Passwords should have no connection to the user. i.e. user name, children's name, etc.

(F) Passwords should contain a minimum of two alpha and one numeric characters.

(G) Passwords should contain both upper and lower case characters.

(9) Sanctions. Failure of workforce members to comply or assure compliance with the policy and procedures outlined in this document may result in disciplinary action, including dismissal.

(10) Review Process. The Chief Security Officer shall collect information from the LSO's during the month of April each year beginning in 2004 for the purpose of providing feedback to the Executive Director, MIS Coordinator and to the Management Team regarding trends and issues associated with compliance with this regulation.

(A) EFC workforce members that receive or maintain PHI shall be required to agree to the security of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement pursuant to DOR 8.040. A copy of the signed confidentiality statement shall be maintained in the personnel file of EFC staff.