

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

POLICY

It is the policy of the Mental Health and Recovery Services Board (MHRSB) of Lucas County to maintain the security of its offices and its property and to secure any and all information created, received and maintained in the offices.

ACCOUNTABILITY

Security Officer, Office Manager

PROCEDURE

A. FACILITY ACCESS CONTROLS

1) Security Measures

The Security Officer and Office Manager are responsible for assigning and changing all security measures undertaken at the MHRSB's offices. These security measures include codes/keys for exterior entrances to its offices, interior secured storage rooms and data center, and keys to employees' offices. If an employee believes that a code has been compromised or a key has been lost, the employee should report the compromise or loss immediately to the Security Officer and Office Manager. Non-employees of the MHRSB can be given codes/keys only with the approval of the Executive Director.

2) Security Codes

Security codes need to be administered in a secured format and should never be emailed. When an employee terminates employment with MHRSB, all security codes that the former employee had access to will be immediately changed.

3) Temporary employees

The Director of Operations & Information Technology should be notified immediately when a temporary employee begins an assignment with the MHRSB. The Director of Operations & Information Technology will initiate the procedure for securing the temporary employee a temporary password for computer access. The Information Technology Department will work in conjunction with the temporary employee's supervisor to determine the limit of computer access. Security codes, passwords and keys should not be available to temporary employees without approval from the Director

**MENTAL HEALTH & RECOVERY
SERVICES BOARD OF LUCAS COUNTY**

Facility Security

**Effective Date: 7/1/14
Supersedes Date: N/A**

of Operations & Information Technology and the temporary employee's supervisor. Such exceptions should be documented.

4) Badges/Keys

The Office Manager is responsible for requesting Access badges, New employee Badges, and issuing office keys to all new employees. All employees will be instructed not to share or loan their keys, badges or codes to other employees. A lost or stolen badge or key will be immediately reported to the Office Manager, who will coordinate with the appropriate County department to replace the lost or stolen badge or key.

5) Reception Area

The Office Manager will ensure that the front door by the reception area is secured when the receptionist is away from the desk. The Customer Service Representative will ensure that only expected visitors, who have signed in and are wearing an identification badge, are allowed to enter the MHR SB's offices, and are accompanied by an employee at all times.

B. DESKTOP, LAPTOP AND TABLET

1) Disposal of Electronic Equipment

The Information Technology employees will ensure that when electronic equipment is no longer serviceable that it is disposed of in a HIPAA approved manner.

2) Software Installations

All software installations must be executed by Information Technology (IT) personnel.

3) Software Applications

Requests for software applications other than standard Microsoft Office or standard computer hardware must be submitted via email to the Director of Operations & Information Technology. The email request must include justification for the new software or hardware and copy the individual's supervisor. Any exceptions to standard software or hardware will be reviewed and either approved or disapproved by the Director of Operations and Information Technology.

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

4) Uses of Desktops, Laptops and Tablets

- a. Personal Use: It is the policy of the MHR SB to provide employees with access to the Internet and use of other electronic communication services for performance of their job function. Occasional and reasonable use of the tools is permissible for non-business activities provided that use does not violate any federal, state, or local laws or established MHR SB Policy.
- b. Personal use of the Internet and other electronic communication services may not interfere with assigned work tasks or work performance, and such use must be consistent with professional conduct.
- c. Streaming Music, Videos or On-Line Gambling: The use of streaming music, video or gambling websites on computers is prohibited except for reasonable business or research use, with the goal of maintaining the integrity of the system.
- d. Employees shall be trained in the use of applicable computer systems and shall exercise integrity with all computers and networks.
- e. Users should have no expectation of privacy while using MHR SB owned or leased equipment. Information passing through or stored on MHR SB equipment can and will be monitored.
- f. Accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language is a violation of this policy.
- g. Employees shall adhere to copyright guidelines in the use of software, information, the attribution of authorship, and in the transmission or copying of a text or files on the Internet or from other sources. This section does not affect making backup copies of MHR SB files and software.
- h. Employees shall not install personally owned/licensed software on any MHR SB owned equipment.
- i. Infringements of this policy will be investigated on a case-by-case basis. Violation of the policy may result in disciplinary action up to and including termination of employment.

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

- j. Each employee will receive a copy of this policy during orientation and will be requested to sign a document acknowledging receipt of the policy
- k. Each employee will notify their immediate supervisor of any threatening or unwelcome communications received.

5) Desktop Screen Savers

Each desktop shall have a screen saver with a screen lock. Access to password protected systems shall be by password only after the keyboard and/or the mouse have been idle for a period of 20 minutes or more, or for five minutes or more if the user works with Protected Health Information (PHI).

C. FACILITY SAFEGUARDS

1) Secure Information Storage

Client charts, records, reports, images (scanned, electronic, film, etc.), and other documents or media containing PHI must be securely stored. The means for securing such information must be appropriate to the location and the risk of unauthorized access. Secured record storage includes, but is not limited to, the following:

- a. Files and charts containing client medical, billing or other records must not be readily accessible to the public in areas that are not regularly monitored. If client records must be kept in such areas, they should be secured in locked drawers or other steps should be taken to prevent public access (for example, removing the records from public view).
- b. In secure work areas, employees will maintain records containing PHI properly filed, particularly outside of regular work hours (e.g., evening, and weekends). In unsecured work areas, employees will turn records left temporarily on a desk or work surface face down when not in use and file or promptly dispose of the records when no longer needed. Employees will not leave client records on desks or other work surfaces in unsecured work areas when the desk is not in use by the employee authorized to view the records.
- c. Employees are generally prohibited from removing from the MHRSB's facilities any charts, files, daily work assignments, other printed documents, equipment, computer disks tapes or other records or media containing PHI. Exceptions are allowed for: (1) Individuals who have the approval of their supervisor to remove

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

PHI from the work site for specific work related purposes, such as to disaster recovery operations or to transport the information; or (2) Management personnel who take PHI off site for work-related purposes. The above standards for secure storage of PHI apply to such information even when it is not within the MHRSB's facility. PHI that is removed from the MHRSB's work site remains the property of the MHRSB and must be returned to the MHRSB when it is no longer required off site for approved, work-related purposes.

2) Secure Information Transfer

Physical transfer of PHI within the MHRSB's office is conducted in such a way that the security of the records is maintained during transfer. Employees who physically deliver records within the MHRSB's facilities are responsible for ensuring that the information is not left at the destination unsecured. Managers of work areas that regularly receive PHI from elsewhere within the facility must implement appropriate controls to safeguard records received. This may include, for example, establishing a schedule for an assigned individual to check for and process incoming records (e.g., in-boxes, etc.).

When it is necessary to physically transfer PHI from the MHRSB's site to a non-covered entity's site, adequate precautions must be taken to ensure the information is protected during the transfer. Records transferred via non-covered entity's courier service generally should be enclosed in sealed envelopes and marked with "Confidential" or other similar designation and should clearly indicate the name and location of the intended recipient. When using non-covered entity's courier services for transfer of PHI, only reputable courier services that have been established systems for tracking documents should be used.

3) Secure Information Disposal

Secure methods must be used for disposal of PHI. This requirement applies for PHI in all forms, including paper, electronic, address-o-graph cards, labels, video tapes, labeled bags, and other materials containing or printed with PHI. PHI must **not** be disposed of in ordinary trash or by other insecure methods.

Secure methods for disposing of paper and most other media include shredding, burning, pulping, pulverizing, confidential recycling through a reputable confidential recycling vendor, or other similar methods. If accessible to the public, receptacles for confidential disposal of records must be covered and locked or otherwise secured to prevent public access. Computerized data should be destroyed through magnetic degaussing or overwriting. The following procedures will be followed in relation to Secure Information Disposal:

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

- a. Employees receive training on proper disposal methods of PHI including instruction to never dispose of information containing PHI in ordinary trash or by other insecure methods.
- b. Secure locked disposal bins from reputable vendor with an executed BAA with the MHRSB are located on site for disposal of PHI.
- c. Employees shall notify Office Manager if additional secure disposal bins are needed for special projects.
- d. Employees shall notify Security Officer to arrange disposal of computerized data to assure proper disposal through magnetic degaussing or overwriting.

D. WORKSTATIONS SAFEGUARDS

1) Secure Workstation and Computer Equipment Locations

- a. Computer workstations and other equipment used to access PHI in areas accessible to the public must incorporate physical controls to address the risk of unauthorized access to PHI. These controls include the following:
 1. Workstations used to access PHI should be located in secured areas that are inaccessible to unauthorized persons wherever possible.
 2. Monitors used to access PHI should be positioned and/or shielded so that information on the screen is not easily viewed by unauthorized persons.
 3. Printers, copiers, and fax machines used for printing of PHI should be shielded from public view or located in secured areas or in areas that are regularly monitored to reduce the likelihood that an unauthorized person will remove printed information.

2) Faxing and Photocopying PHI

- a. Faxing Sensitive Information: Employees may not send by fax especially sensitive medical information, including, but not limited to, AIDS/HIV information, mental health and developmental disability information, alcohol and drug abuse information, sexual or other abuse information, and other sexually transmittable disease information, except as required in its operations, without

**MENTAL HEALTH & RECOVERY
SERVICES BOARD OF LUCAS COUNTY**

Facility Security

**Effective Date: 7/1/14
Supersedes Date: N/A**

separate specific written authorization by the Consumer or legally authorized representative.

- b. When Information May be Released without Consumer Authorization: Qualified employees may send PHI by fax without authorization when: (1) The original record or mail-delivered copies will not meet the immediate needs to treat the client and the recipient is a health care provider; (2) When PHI is urgently required by a third-party payer and failure to fax the records could result in the loss of reimbursement to the MHR SB; or (3) Facsimiles of records may be sent to parents or legally authorized representatives of Consumers.
- c. Limit Release: Employees shall limit information transmitted to the minimum amount reasonably necessary to meet the requester's needs or to accomplish the purpose for which the request is made. No fax request will be honored unless it is specific as to the purpose and the information required.
- d. Documentation of Release: All releases of PHI shall be documented in the Consumer and HIPAA files. Documentation shall include the following:
 - i. The date of the release.
 - ii. The information released.
 - iii. The date of the released information.
 - iv. To whom the information was released.
 - v. The purpose of the release.
 - vi. How the release was carried out (fax, photocopies mailed or hand delivered, verbal, etc.).
- e. Cover Page: The cover page accompanying the facsimile transmission also must include:
 - i. The sender's name and title, address, telephone number, and fax number.
 - ii. The recipient's name and title, address, and telephone number.
 - iii. The name of the facility.

**MENTAL HEALTH & RECOVERY
SERVICES BOARD OF LUCAS COUNTY**

Facility Security

**Effective Date: 7/1/14
Supersedes Date: N/A**

- iv. The fax number.
- v. Verification that the fax number is accurate.
- vi. Verification that the fax was received.
- vii. Number of pages transmitted.
- f. Verification of Destination: The MHR SB must make reasonable efforts to send the facsimile transmission to the correct destination. The MHR SB shall pre-program frequently used numbers into the fax machine to prevent misdialing errors. Pre-programmed numbers should be tested prior to being used to transmit PHI. When the pre-programming of fax numbers cannot be performed, strict number verification procedures prior to transmission of information shall be used to route information to the correct location. For a new recipient, the sender shall verify the fax number before sending the fax and verify the recipient's authority to receive confidential information.
- g. Location of Fax Machines: Fax machines must be located in secure areas which limits access to the machines.
- h. Handling of Received Faxes: All MHR SB employees are responsible for the proper handling of incoming faxes, and that assuring faxes are not left sitting on or near the machine, but rather shall be distributed to the proper recipient expeditiously while protecting confidentiality during distribution.

3) Email

- a. Any outgoing email that contains PHI **must** be encrypted.
- b. Any portable electronic device (cell phone, iPad, PDA, etc.) that may contain, transmit or receive PHI must be password protected.
 - i. Employees request technical assistance from IT Department, when needed, to ensure that outgoing email containing PHI is encrypted.
 - ii. PHI should not be included in the subject line of the email nor in the body of the email. PHI information should only be included in the secured attachment.

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

- iii. If other persons or organizations send PHI to the MHR SB by email employees must: (1) not forward the email or attachments externally or unnecessarily internally and (2) request persons transmitting the email not to forward client identifying information in the subject line or body of the email in future transmissions.
- iv. Any accidental disclosures of PHI should be reported to the Privacy Officer and/or Security Officer immediately upon discovering the disclosure.

4) Paper Documents/Written Information

- a. All incoming correspondence should be funneled through a distinct channel that involves the smallest number of viewers possible to generate the necessary business response. To achieve this goal, consider steps such as: (1) Pre-addressing mailing envelopes to employees or specific departments within the MHR SB; and (2) Having one highly responsible MHR SB employee acting as the conduit for all incoming correspondence, with the employee distributing all opened mail to the appropriate person.
- b. MHR SB employees should make the minimum necessary copies of documents that contain PHI. If documents must be printed, the documents should be retrieved immediately.
- c. During the workday, paper files and records with PHI should not be piled on desks or left unattended, but should be kept in drawers or files to reduce exposure.
- d. Employees should clear their desk of all paperwork and files prior to leaving every day. This will eliminate the possibility of janitorial employees or others who leave later or arrive earlier from viewing PHI they have no right to access.

5) Phone Calls

A primary concern for the MHR SB is the use and disclosure of PHI during oral communications, whether it is with the client, between providers, or in a business context.

The key to protecting oral communications is the same as for other information and forms of communication: Employ reasonable administrative, technical, and physical safeguards and comply with the minimum necessary standard. If the MHR SB's efforts to protect inappropriate disclosure or misuse of PHI meet the reasonable safeguards and minimum necessary standards, the MHR SB complies with the HIPAA Privacy and

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14
Supersedes Date: N/A

Security requirements. This also applies to incidental uses and disclosures of PHI that occur as a by-product of an otherwise permissible use.

- a. Protecting PHI during Conversations
 - i. Employees will be educated with regard to who may receive PHI and what constitutes appropriate and lawful exchanges when discussing PHI.
 - ii. Employees are to keep their voices low when discussing issues that may involve PHI.
 - iii. Make sure that Consumer information is not dictated into audio records within earshot of other employees.
- b. Protecting PHI during Telephone Conversations: Telephone calls requesting or disclosing PHI represent a liability, and it is important to educate employees on the basics of privacy disclosures – who may receive PHI, for what purpose, and how much PHI may be disclosed.
 - i. Use physical barriers of different types to help prevent conversations from being overheard. Among possibilities: cubicle walls or dividers.
 - ii. Employees should speak as quietly as possible while on the phone.
- c. PHI and Voice Mail/Answering Machines: While the HIPAA Privacy Rule does not prohibit leaving messages for individuals on their answering machines, Consumer privacy can be violated when PHI and Consumer names are left in voice mail messages or on phone answering machines. Employees should leave only their name and number and ask the Consumer to call back.

E. PASSWORD COMPOSITION

- 1) For secured access to systems and applications, such as electronic mail and LAN access, passwords shall have at least eight characters of any sort.
- 2) To the extent possible, passwords shall be composed of a variety of letters, numbers and symbol.

MENTAL HEALTH & RECOVERY SERVICES BOARD OF LUCAS COUNTY

Facility Security

Effective Date: 7/1/14

Supersedes Date: N/A

- 3) To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
- 4) Password management application features that allow users to maintain password lists and/or automate password inputs are prohibited.

1 Valid symbols are @, \$, +, -, #, ?, ., !, %, and _ . In RACF, the first character of a password must be a letter.

2 Other number/symbol for letter examples are 0 for o, \$ for S, 1 for i, and 1 for l, as in capta1n k1rk or mr5pock.

F. PASSWORD MANAGEMENT

- 1) Passwords shall not be revealed to anyone, including a supervisor, family consumers or co-workers.
- 2) Users shall enter passwords manually.
- 3) Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media.
- 4) Passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.

G. REMOTE ACCESS SECURITY STANDARD

1) Users

- a. Responsibility for Use: All users who require remote access privileges (LogMeIn account) are responsible for the activity performed with their user-IDs, whether or not these user-IDs are connecting via external network facilities. LogMeIn User-IDs shall never be shared with those not authorized to use the ID. User IDs may not be utilized by anyone but the individuals to whom they have been issued. Similarly, users are forbidden from performing any activity with LogMeIn user-IDs belonging to others.
- b. Revocation/Modification: Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon an employee's or contractor's termination from service.

**MENTAL HEALTH & RECOVERY
SERVICES BOARD OF LUCAS COUNTY**

Facility Security

**Effective Date: 7/1/14
Supersedes Date: N/A**

Remote access privileges shall be reviewed upon an employee's or contractor's change of assignments.

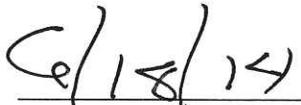
H. MISCELLANEOUS

- 1) Disclosure of Systems Information: The internal addresses, configurations, and related system design information for MHR SB computers and networks are confidential and shall not be released to third parties. Likewise, the security measures employed to protect MHR SB computers and networks are confidential and shall be similarly protected.

Approved:



Scott A. Sylak, Executive Director



Date