	Chapter:	Section:	Subject:
	7	1	1

CHAPTER: HIPAA		
SECTION: HIPAA Privacy and Security		
SUBJECT: General Policy		
Administrative Approval:	Date of Governing Board Action: April 19, 2005	Page 1 of 5

I. PURPOSE: To provide for plans and procedures to comply with the HIPAA Privacy Rule to protect the privacy and security of personal health information; and, the HIPAA Security Rule to ensure the appropriate administrative, physical and technical safeguards of the system components that such data resides in.

II. APPLICATION: All personnel of WMCMH.

III. REQUIRED BY: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services privacy and security regulations implementing HIPAA, other federal and state laws protecting confidentiality of personal health information, professional ethics and accreditation requirements.

IV. DEFINITIONS:

HIPAA – Health Insurance Portability and Accountability Act of 1996

DHHS – Department of Health and Human Services

Security Officer – The WMCMH Security Officer is the Information Services Manager

Privacy Officer—The WMCMH Privacy Officer is the Rights and Regulations Officer

V. POLICY: It is the policy of West Michigan Community Mental Health to provide for the protection of individually identifiable health information. West Michigan CMH has implemented and revised policies, procedures and plans to safeguard individually identifiable health information. The accompanying procedures detail these mechanisms.

If any standards specified in the accompanying procedures are violated, immediate sanctions according to the Sanction Procedures will occur.

VI. PROCEDURES:
The HIPAA Security Rule Policy is a result of a thorough Risk Analysis (copy of Risk Analysis will be held by the Security Officer). A Risk Analysis will be conducted as new assets are acquired that may pose additional risk.

The Corporate Compliance Committee will review any Risk Analysis completed on new assets, to ensure HIPAA Security Rule compliance.

Specific procedures addressing all necessary elements of the HIPAA Security Rule are listed below.

Code of Ethics See: o Policy 4.2.1 (Code of Ethics)
Sanction Procedure – **Appendix 7.1.1.1**
Workstation Use Procedure – **Appendix 7.1.1.2**
Termination Procedure – **Appendix 7.1.1.3**
Access Authorization, Access Establishment, and Access Modification Procedure See: o Policy 2.2.1 (Care Planning, Documentation, and Coordination) o Policy 5.2.1.1 (Security of Protected Health Information (PHI) and Safeguarding Customer Clinical Records)
Training Procedure – **Appendix 7.1.1.4** See also: o Policy 4.6.2 (Orientation to Employment) o Policy 4.6.4 (Training and Development) o Personnel Security Procedures (HIPAA Appendix 7.1.1.10)
Report Procedure See: o Policy 6.1.3 (Open Lines of Communication) o Policy 6.1.7 (Compliance Enforcement and Discipline)
Response Procedure See: o Policy 6.1.3 (Open Lines of Communication) o Policy 6.1.4 (Handling Allegations of Non-Compliance) o Policy 6.1.7 (Duty to Report; Discipline)

Data Backup Procedure See: o Policy 3.8.2 (Network Backup)
Disaster Procedure – **Appendix 7.1.1.5**
Emergency Mode Operation Procedure – **Appendix 7.1.1.6**
Internal Audit Procedure See: o Policy 2.2.1 (Care Planning, Documentation, and Coordination) o Policy 2.2.2 (Clinical Records Elements and Organization) o Policy 2.2.5 (Security of Electronically Stored Clinical Information) o Policy 3.8.4 (Protection from Unauthorized External Access) o Policy 3.8.5 (Protection from Unauthorized Internal Access) o Policy 5.2.1.1 (Security of Protected Health Information (PHI) and Safeguarding Customer Clinical Records) o Policy 5.2.1.2 (Release of Information)
Combined Security and Privacy Business Associate Agreement See: o Policy 6.1.8 (Business Associate Agreement)
Security Management Component/Emergency Preparedness Plan – **Appendix 7.1.1.7**
Device and Media Controls Procedure – **Appendix 7.1.1.8**
Destruction Procedure – **Appendix 7.1.1.9**
Emergency Access Procedure See: o Policy 2.2.1 (Care Planning, Documentation, and Coordination) o Policy 5.2.1.1 (Safeguarding Client Records)
E-mail Procedure See: o Policy 3.8.3 (Electronic Communications)

Personnel Security Procedure – **Appendix 7.1.1.10** See also: o Policy 4.4.1 (Employee Personnel Record) o Policy 4.6.1 (Background Checks) o Policy 4.6.2 (Orientation to Employment) o Policy 4.6.3 (Performance and Competency Assessment) o Policy 4.6.4 (Training and Development)
Videoconferencing Procedure– **Appendix 7.1.1.11** See also: o Policy 2.2.1 (Care Planning, Documentation, and Coordination) o Policy 2.2.4 (Documentation Methods) o Policy 3.8.3 (Electronic Communications)
Cell Phone Procedure See: o Policy 3.8.3 (Electronic Communications)
Audiovisual Recording Procedure – **Appendix 7.1.1.12**
Access Establishment Modification Procedure – **Appendix 7.1.1.13**
Procedures for Selecting Health Record Review Information for Reviewers – **Appendix 7.1.1.14**

VII. <u>SUPPORTING DOCUMENTS</u>: See above.

Updated 7.1.1.14 8/07; Updated Jan2015 tinab; 2/16/16 tinab; 5/19/17 tina; May 2019 karenh

Sanction Procedure

Procedure

Duty to Report: Any officer, employee, or agent of WMCMH who believes another officer, employee, or agent of WMCMH has breached the HIPAA Privacy and Security Policy or the procedures and standards adopted to carry out the objectives of the HIPAA Privacy and Security Policy, or who otherwise breached the integrity or confidentiality of consumer or other sensitive information must immediately report such breach to the Regulations Officer of WMCMH or may report anonymously using the 24-Hour Compliance Hotline by calling 1-800-624-6689. WMCMH will not retaliate against or permit reprisals against a complainant. Allegations not made in good faith, however, may result in discipline or other penalty.

Duty to Investigate: The Regulations Officer will coordinate a thorough and confidential investigation into the allegations. The Regulations Officer will facilitate a report for the WMCMH Executive Director and applicable Team Leader/Supervisor that includes a recommendation for remedial action, if necessary. The Team Leader/Supervisor and Human Resources Coordinator will review the report made available by the Regulations Officer and, if the breach has been substantiated, will determine the appropriate sanction. The Team Leader/Supervisor will consult with the Human Resources Coordinator prior to making a recommendation for corrective or disciplinary action.

Communication of Investigation Outcome to Complainant: The Regulations Officer will inform the complainant of the results of the investigation and any corrective action that will be taken; however, the details of any disciplinary action taken will not be shared with the complainant.

Sanctions in Substantiated Breaches: In the discretion of management, WMCMH may terminate an employee for the first breach of the covered entity's HIPAA Privacy and Security Policy or individual procedures and standards if the seriousness of the offense warrants such action. An employee could expect to lose his or her job for a willful or grossly negligent breach of confidentiality, willful or grossly negligent destruction of computer equipment or data, or knowing or grossly negligent violation of HIPAA, its implementing regulations or any other federal or state law protecting the integrity and confidentiality of consumer information. For less serious breaches, management may impose a lesser sanction, such as a verbal or written warning, verbal or written reprimand, loss of access, suspension without pay, demotion, or other sanction. In addition, WMCMH will include such violations by contractors as a reason for termination of the contract and/or imposition of contract penalties.

Communication of Sanctions: The Executive Team will communicate the sanctions to be imposed to the Regulations Officer. The Regulations Officer will inform the individual's supervisor and Human Resources of the sanction decision.

Criminal Proceedings: Violation of the WMCMH HIPAA Privacy and Security Policy or its accompanying individual procedures and standards may constitute a criminal offense under HIPAA, other federal laws, such as the Federal Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, or state laws. Any employee or contractor who violates such a criminal law may expect that WMCMH will provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

Licensure / Accreditation Reporting and Investigations: Violations of the WMCMH HIPAA Security Policy or its accompanying individual procedures and standards may violate professional ethics and be grounds for professional discipline. Any individual subject to professional ethics guidelines and / or professional discipline should expect WMCMH to report such violations to appropriate licensure / accreditation agencies and to cooperate with any professional investigation or disciplinary proceedings.

No Employment Contract Implied: This Sanction Procedure is intended as a guide for the efficient and professional performance of West Michigan Community Mental Health's officers, employees, and agents' duties to protect the integrity and confidentiality of medical and other sensitive information. Nothing herein shall be construed to be a contract between the employer and the employee. Additionally, nothing in this Sanction Procedure is to be construed by any employee as containing binding terms and conditions of employment. Nothing in this Sanction Procedure should be construed as conferring any employment rights on employees. Management retains the right to change the contents of this Sanction Procedure, as it deems necessary with or without notice.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed: Jan2015 as & tinab; 2/1/16 as; 5/17/17ask; 5/31/19 ask

Appendix 7.1.1.2

Workstation Use Procedure

Assumptions:

- WMCMH computers are vulnerable to environmental threats, such as fire, water damage, power surge, etc.
- Computer workstations at WMCMH can access confidential consumer information if the user has the appropriate security permissions.
- Individuals who do not have access to confidential information may view that type of information on a computer.

Preventative Measures

- All computer users will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system.
- All computer users shall take appropriate measures to protect computers and data environmental threats.
- Personnel logging onto the computer system will ensure that no one observes the entry of his/her password.
- After five failed log on attempts, the users account will be locked and an event log will be generated.
- Personnel will not log onto the system using another's password nor permit another to log on with his/her password. Personnel will not enter data under another person's password.
- Each person using WMCMH's computers is responsible for the content of any data he/she inputs into the computer or any transmission of data. No person may hide his/her identity as the author of the entry or represent that someone else entered data or sent a message.
- All computer users shall familiarize themselves with e-mail usage.
- No employee may access any confidential consumer or other information that he/she does not have a need-to-know. No employee may disclose confidential consumer or other information unless properly authorized.
- Employees must not leave printers unattended when they are printing confidential consumer information. This rule is especially important when two or more computers share a common printer or when the printer is located in an area where unauthorized personnel have access to the printer.
- Computer users shall not enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or X-rated. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane or offensive language.
- Computer users shall not write down his/her password and locate it at or near the terminal, such as by putting their password on a yellow "stickie" on the screen or tape it under the keyboard.
- Computer users will have time out generated for idle usage. Supervisors may specify an appropriate period to protect confidentiality while keeping the computer available for use.

- Computer users shall lock the system if they leave for any length of time. User exceptions where clinically necessary must be approved in writing by his/her supervisor.
- Each user must follow the health records procedure on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the printouts, and how to maintain confidentiality of hard-copy printouts.
- No personnel may upload data from the WMCMH system without the express permission of his/her supervisor and with notice to the Information Systems Manager.
- No personnel may download any unauthorized software or data. The Information Systems Manager must approve any software or data that an employee wishes to download. This rule is necessary to protect against computer viruses from being transmitted into the covered entity's system.

Approved by the HIPAA Workgroup 04/06/05 cr; reviewed Jan2015 ck; 2/11/16 ck; 5/18/17ck,5/31/19 tf

Appendix 7.1.1.3

Termination Procedure

Responsibility to Notify: Supervisors, Contract Managers, and/or the Human Resources Coordinator are responsible for notifying the Information Services Coordinator and the Facilities Coordinator of employees and others, such as independent contractors, who will be leaving West Michigan Community Mental Health's employ or engagement (through reassignment, extended absence, contract termination, and so forth) and will no longer need access to individually identifiable health information and WMCMH data systems and facilities.

In instances in which the level of access to individually identifiable health information and WMCMH data systems and facilities changes for an employee or other agent of WMCMH, supervisors, contract managers, and/or the Human Resources Coordinator are responsible for notifying the Information Systems Manager so that their level of access can be adjusted.

Any other data user who becomes aware that a data user is leaving the covered entity either permanently or for an extended or unexplained absence should report the matter to the Human Resources Coordinator and/or the Information Systems Manager for a determination of whether to revoke or suspend that person's access.

Termination of Access Process:
Upon termination of an employee or other person with access to individually identifiable health information or WMCMH data systems, the following actions will immediately take place:

- Information Systems Manager or his/her designee will revoke access privileges, such as user-IDs and passwords, to system and data resources.
- The Facilities Specialist or his/her designee will retrieve sensitive materials, including access control items, such as passkeys and badges.
- The Information Systems Manager or his/her designee will retrieve all hardware, software, data, and documentation issued to or otherwise in the possession of the data user.
- The Human Resources Coordinator or his/her designee will arrange for an exit briefing to verify retrieval of all items, to discuss any security or confidentiality concerns with the data user, and to remind the data user of the continuing requirement to protect data security and consumer confidentiality.
- The Contract Manager or his/her designee will arrange for a contract termination briefing to verify retrieval of all items belonging to WMCMH, to discuss any security or confidentiality concerns with the data user, and to remind the data user of the continuing requirement to product data security and consumer confidentiality.
- The Contract Manager will notify the Finance Coordinator of completion of the termination procedures so that the contractor can receive any final monies due under the terms of the contract.
- The Information Systems Manager and the Facilities Specialist will notify the Human Resources Coordinator of completion of the termination procedure so that the data user can receive any final pay due.

Human Resources will keep records of the termination procedure for each employee in their personnel file, including the retrieval of security-related items, such as badges, passwords, and information system assets.

The Contract Manager will keep records of the termination procedure for each contracted entity in the contract file, including the retrieval of security-related items, such as badges, passwords, passkeys, and information system assets.

When necessary, the Human Resources Coordinator will arrange for security escort of terminated personnel or contractors from WMCMH property and for an immediate audit of their accounts to detect any security or confidentiality threats or breaches. Employees and others who are terminated may expect to have their data access immediately terminated and not to receive any final pay due until the termination of access procedure is properly completed.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed: Jan2015 as; 2/1/16 as; 5/17/17ask; 5/31/19 ask

Appendix 7.1.1.4

Training Procedure

Assumptions

This Training Procedure is based on the following assumptions:

- In any organization, people are the greatest asset in maintaining an effective level of security.
- Likewise, poor personnel security can result in serious breaches of data integrity and confidentiality.
- Physical and technical security cannot adequately compensate for poor personnel security.
- Poorly trained, poorly supervised, or dishonest employees can often defeat physical and technical security mechanisms.
- An honest employee is still a security risk if he or she does not know what is expected with regard to security and confidentiality.
- No security program can be effective without maintaining employee awareness and motivation.
- Initial training is not enough. It must be supplemented with periodic refresher training.
- West Michigan Community Mental Health trained all personnel on the Privacy Rule on or before April 14, 2003. Thereafter, new personnel must be trained as soon as possible after beginning employment.
- All personnel will be trained on the Security Rule on or before April 22, 2005 with new personnel being trained as soon as possible after beginning employment. See the Access Establishment Policy.

Procedure

HIPAA and the DHHS security and privacy regulations require training all personnel with access to individually identifiable health information. The Information Systems Manager is responsible for developing, presenting, and documenting training in the following subjects:

- Principles of and need for privacy and security.
- Training required by § 164.308(a)(5)(i): Security reminders, protection from malicious software, log-in monitoring, and password management.
- Requirements of HIPAA and the DHHS regulations.
- Requirements of other federal and state laws regulating health information.
- West Michigan Community Mental Health's policies and procedures regarding health information.
- Practical guidance for protecting data integrity and confidentiality, such as the importance of proper password procedure, how to guard against computer viruses, and the like.
- Procedures for reporting breaches of security and confidentiality.
- West Michigan Community Mental Health will provide periodic refresher training in the above subjects. Such training will include "lessons learned" from security and confidentiality breaches, as well as any changes in the West Michigan Community Mental Health's policies and procedures.

- Data users will sign a statement certifying that West Michigan Community Mental Health has trained them, that they understand the training, particularly West Michigan Community Mental Health's policies and procedures, that they will adhere to the requirements of relevant laws and West Michigan Community Mental Health's policies and procedures, and that they understand that they face disciplinary action if they do not. See Appendix A
- The use of videotapes, e-learning, and other methods that do not take large numbers of data users away from their jobs for extended periods is encouraged when appropriate.

Human Resources will retain data users' statements of understanding and compliance for not less than six years from the date of training.

Supervisors must supplement the required training with any additional training necessary for the particular needs of their subordinate's duties. Supervisors will submit outlines of additional training to the Human Resource Department. These records of such supplemental training will be kept for not less than six years from the date of training.

Note:

Appendix A, certification statement
Training and Development Policy & Procedures 4.6.4

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed: Jan2015 as; 2/1/16 as; 5/17/17ask; 5/31/19 ask

Appendix 7.1.1.5

Health Information Disaster Procedure

Assumptions:

- A disaster may occur at any time, not necessarily during work hours.
- WMCMH must remain operational with as little disruption of consumer care as possible.
- Continuity of consumer care requires uninterrupted access to consumer information.
- In an evacuation, evacuating personnel has priority over preserving information assets.
- The following conditions can destroy or disrupt WMCMH information systems:
    - Power interruption
    - Fire
    - Water
    - Weather and other natural phenomena, such as earthquakes
    - Sabotage and vandalism
    - Terrorism

Preventive Measures:

The Information Systems Manager must ensure that all personnel must take the following preventive measures:

- Use the data backup plan to protect computerized files.
- Test integrity of backup system according to the data backup plan.
- Protect servers and other critical equipment by using uninterruptible power supplies.
- In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent. Use methods to protect information and equipment from fire or from water as appropriate.
- Must know responsibilities in the event of a disaster.
- Ensure that major hardware is covered under WMCMH property and casualty insurance policy.
- Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.
- Ensure complete system backup for disaster recovery in Hart is operational

High-Priority Tasks during Emergency Containment Measures:

Personnel should:

- If computers have not automatically powered down, initiate procedures to orderly shutdown systems, when possible.
- If a fire or flood occurs, disconnect power if possible.
- Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
- Respond to requests for records via portable phone rather than computer.
- Continue to provide consumer charts as they are requested.

High-Priority Disaster Recovery Tasks:

Personnel should:

- Determine how long it will be before service can be restored and notify supervisors.
- Replace hardware as appropriate in order to restore service.

- Work with vendors as necessary to ensure that support is given to restore service.
- Notify insurance carriers.
- Retrieve and upload backup files if necessary to restore service.
- Reconstruct or re-acquire documents from the following:
    - Computer system.
    - Holders of document copies.
- Move records and equipment back to home location.
- Document data that cannot be recovered in consumer records.
- Meet with staff to identify opportunities for improvement.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed Jan2015 ck; 2/11/16 ck; 5/18/17ck; 5/31/19tf

Appendix 7.1.1.6

Emergency Mode Operation Procedure

Assumptions

This Emergency Mode Operation Procedure is based on the following assumptions:

- Data, media, and computer assets are the physical property of WMCMH, wherever located, although clients and others may have rights of access to the data.
- Individually identifiable health information is sensitive and confidential. Such information is protected from improper use and disclosure by HIPAA, its implementing regulations, other state and federal laws, professional ethics, and accreditation requirements.
- HIPAA, its implementing regulations, other state and federal laws, professional ethics, and accreditation requirements specify that only those individuals with a need to access and use individually identifiable health information should have access to such information.
- Limiting access to those with a need to know and giving them no more access than necessary for performance of their duties will help WMCMH comply with the privacy regulations' "minimum necessary" rule.
- Those authorized access should have no more access than needed for the performance of their responsibilities.
- In an emergency, other individuals may need immediate access to data and equipment to carry out medical and business operations.
- An emergency override may be necessary for some data users, such as physicians and nurses, to respond to emergencies.
- Not all systems are considered critical and thus may not require invoking this procedure. Appendix D should be reviewed by the emergency mode operations team.

Emergency Procedures

In the case of an emergency, the individual detecting the emergency will immediately report the emergency to the Information Services Manager and/or the Security Officer who will immediately notify the members of the emergency mode operations team. The team leader will assign members to specific tasks as appropriate to operate during the emergency. Unless other instructions accompany the notification, team members will meet in the Ludington Training Room.

The Deputy Director of Administrative Services or emergency mode operations team leader will take the following steps:

- Determine the extent and seriousness of the disaster and notify WMCMH Executive Team thereof.
- Invoke this Procedure and the Disaster Recovery Procedure upon approval of WMCMH Executive Team.
- Determine whether additional equipment and supplies are needed.
- Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.

- If necessary, check with other vendors to see whether they can provide faster delivery.
- Rush order any supplies and equipment necessary.
- Notify the personnel listed at Appendix B that an alternate site will be necessary and where it is located.
- Coordinate moving equipment and support personnel to the alternate site.
- Bring recovery materials from offsite storage to the alternate site.
- As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine priorities of software that must be available and load those packages in order. These priorities are specified in Appendix C to this policy.
- Prepare backup materials and return them to the offsite storage area.
- Set up operations at the alternate site.
- Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- Ensure that periodic backup procedures are followed.
- Procedure to phase in all critical support.
- Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- Implement relevant portions of the WMCMH Disaster Procedure.
- Coordinate with administration and others for continuing support and ultimate restoration of normal operations.

The Information Services Manager is responsible for the following tasks:

- Select and maintain an alternate site to perform the WMCMH's data processing functions if a disaster seriously disrupts such functions. Currently Hart maintains the full disaster recovery system if available.
- Ensure compatibility between hardware and software of the primary and backup sites.
- Provide backup power and communications in the event of an emergency.
- Appoint personnel to the emergency mode operations team.
- Train all personnel in the Emergency Mode Operation Procedure.
- Test the Emergency Mode Operation Procedure and make revisions as necessary.

The Supports/Site Services Coordinator is responsible for the following tasks:

- Nominate personnel to the emergency mode operations team.
- Coordinate with Deputy Director of Clinical Services to ensure adequate medical record keeping during emergencies.
- Provide medical departments the necessary tools to record medical data on paper during computer outages.
- Ensure that documentation on paper is entered into the system after it has been restored to operations.
- Train personnel on emergency mode operations.
- With the Information Services Manager, test and revise health information management department emergency mode operations procedures.

Coordinators and Team Leads are responsible for the following tasks:

- Provide the Information Services Manager and/or the Deputy Director of Administrative Support Services priorities as to critical tasks within their departments involving health information.
- Train all department personnel on emergency mode operations.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed Jan2015 ck; 2/11/16 ck; 5/18/17ck; 5/31/19tf

Appendix 7.1.1.7

WEST MICHIGAN COMMUNITY MENTAL HEALTH

SECURITY MANAGEMENT COMPONENT
EMERGENCY PREPAREDNESS PLAN

PURPOSE:

The security program at West Michigan Community Mental Health is designed to ensure the personal safety of West Michigan Community Mental Health staff, consumers, visitors, as well as the protection of assets and confidential health records.

PROCEDURES:

The following program, policies and procedures have been established for implementation at West Michigan Community Mental Health board operated facilities.

1. ***Civil Disturbance****:* following are the procedures that CMH staff members shall implement in the event a person, either on the grounds or in a CMH center, who is unduly agitated, making verbal or physical threats, appears to be under the influence of intoxicating substance, destroying property, etc.

1.1. The staff member who is first aware of the situation may choose to do one or more of the following depending on the circumstances:

- Contact 911
- If necessary, contact the appropriate staff related to the consumer or situation
- Ask for assistance from the nearest available staff members

1.2. Team Leaders/supervisors shall alert other staff members in the building to the situation, if necessary.

1.3. Attempts should be made to isolate the disturbance from other areas/people in the building. Removing the uninvolved consumers to a safe area may be necessary.

1.4. If the disturbance is outside of the building, consumers, visitors and staff members shall stay away from the window.

1.5. Uninvolved staff members shall continue normal operations if feasible.

1.6. The staff member who is first aware of the situation shall complete an Critical Incident Report within 24 hours and submit it to the safety officer for review.

1.7. If the Disturbance is of such a nature that staff members, consumers and visitors need to evacuate the building, the Facilities Specialist shall be informed or the Deputy Director of Administrative Services or his/her designee in the absence of the Facilities Specialist.

1.8. The Facilities Specialist or Deputy Director of Administrative Services shall inform the Executive Director or his/her designee of the situation.

1.9. In the event of a building evacuation, the previously appointed building sweepers shall assure that the occupants of the section/building are evacuated to a safe area outside the building.

1.10 No staff member or consumer shall re-enter the building until the Facilities Specialist or Deputy Director of Administrative Services has given an "all clear" signal.

1.11 After the "all clear" signal has been given, the Deputy Director of Administrative Services and Facilities Specialist shall decide whether or not to resume normal operations. If the Deputy Director of Administrative Services decides to cancel operations, he/she shall contact the Executive Director and Team Leaders/supervisors to inform them of the decision. In addition, the following procedures shall be implemented:

- Arrangements shall be made for consumers to be picked up and taken home.
- Team Leader or their designee shall be responsible for ensuring all consumers have adequate transportation home and those consumers who reside in AFC or staffed group homes that the care providers are home.
- Team Leader or their designee shall remain at their program site until all consumers and program staff has safety evacuated.

2. ***Reception Alarm:*** There are alarms located at all receptionist desks at 920 Diana, 105 Lincoln and 1090 N. Michigan.

Following are the procedures that CMH staff members shall implement in the event that the receptionist alarm is activated due to circumstances involving, but not limited to, a disruptive person(s) presenting him/her self at the WMCMH premises or a person becomes potentially dangerous to him/her self or others.

1. When alarm is activated (a door buzzer sound), **STAY CALM;**

   1.1 In Baldwin and Hart, alarm will sound in hallways. When alarm sounds, available staff members (2 or 3, at least one clinical person preferred) shall go to the reception area.

   1.2 In Ludington, alarm will sound in alternate receptionist office. Alerted receptionist will immediately notify staff members (2 or 3, at least one clinical person preferred) to go to the respective reception area.

2. Caution shall be used when approaching the reception area, do not startle the person. The state of mind of the agitated individual may be unknown.

3. If a weapon appears to be present, the responding staff persons should attempt to retreat and call 911 from the nearest phone. If retreat is not possible, do what the person asks, within reason, but never leave the premises with the person.

4. If the person offers you their weapon, ask them to set it down and step away from it. It is then safe for the staff person to approach the weapon and pick it up.

5. If no weapon appears to be present, the responding staff shall attempt to intervene and assist the staff member and the agitated individual. Depending on the circumstances, the following interventions may be appropriate:

   5.1 When staff assistance arrives, if appropriate, attempt to relocate the situation from the lobby.
   5.2 Obtain an available clinician (if one did not accompany the initial contact).
   5.3 Ask the agitated person to leave the building (contact 911 accordingly).
   5.4 Instruct persons in the lobby to exit the building and vacate the area (contact 911). In the event of a building evacuation, refer to the WMCMH emergency preparedness procedure for Civil Disturbance/Disruptive Behavior.

6. After the incident is over, the staff person who activated the receptionist alarm shall complete a Critical Incident Report form within 24 hours and submit the report their supervisor.

3. ***Confidential Health Records:*** following are the procedures for access to confidential health information regarding the consumers who receive services.

3.1. All information regarding a consumer shall be compiled in one primary electronic clinical file. Information in the record of a consumer and other information acquired in the course of providing mental health services to a consumer shall be confidential. The fact that person is receiving services is confidential.

3.2. Only authorized staff members may access health records on a need to know basis.

- Clerical functions, e.g. typing, filing, fee determination, processing for release or request for information, etc.
- Program staff members assigned a case and working either with the consumer or on the case record itself.
- Consultants working either with consumers or on the case record.
- Clinical Team Review, Peer and Utilization Review Committee members and Clinical Oversight Committee Executive Committee
- Supervisory and administrative personnel.

3.3. The Support Services Coordinator along with Information Systems Manager shall be responsible for establishing and implementing specific procedures for the control of health records.

3.4. Security of electronically stored confidential, clinical information is addressed by the West Michigan Community Mental Health Administrative Manual, Chapter 2, Section 2, and Subject 5.

4. ***Facility Keys:***

4.1. Upon hire, each employee shall be issued a KeyScan card for all locations. The Human Resource Specialist is responsible for issuing the KeyScan cards. Senior Leadership members, and the Facilities Specialist will receive hard keys to each of the board-operated facilities. The Facilities Specialist is responsible for issuing hard keys.

4.2. Each card will be numbered. The number and name of the employee receiving the card shall be recorded in the KeyScan software.

4.3. At termination of employment, the employee shall return the KeyScan card, it will be deactivated by the Human Resource Specialist and hard key returned to the Facilities Specialist via Human Resources.

4.4. The employee shall not loan or otherwise give his/her key to another person.

4.5. If a key or KeyScan card is lost or stolen, it will be reported to the Human Resource Specialist immediately. A new KeyScan card will be issued and the lost card deactivated.

5. *Employee Identification:*

West Michigan Community Mental Health provides identification badges to all employees upon hire. The identification badge is returned to the agency when the employee terminates employment. Chapter 4, Section 6, Subject 1 of the Administrative Manual addresses this issue.

6. *Building Access:*

In an attempt to address security by limiting the access to West Michigan Community Mental Health board operated facility entrances, the following procedures have been implemented:

6.1. **920 Diana Street, Ludington:** All entrances except the main north entrance will remain locked at all times. The main entrance is unlocked for consumer and visitor entrance during regular business hours. This assists with limiting consumer and visitor access to sensitive and employee only areas. There is adequate signage on the exterior of the building to direct consumers and visitors to the main entrance.

6.2. **105 Lincoln Street, Hart:** The main entrance is unlocked during regular business hours. All other entrances are locked. The receptionist at the main entrance greets consumers and visitors. Access to sensitive and employee only areas is limited by a closed door, which leads to employee offices. There is adequate signage on the exterior of the building to direct consumers and visitors to the main entrance.

6.3. **1090 North Michigan, Baldwin:** The main entrance is unlocked during regular business hours. All other entrances are kept locked at all times. Consumers and visitors enter into the main reception area and are greeted by the receptionist. Access to sensitive and employee only areas is limited due to a closed door that leads directly to employee offices. There is adequate signage on the exterior of the building to direct consumers and visitors to the main entrance.

7. *Staff Training and Orientation:*

7.1. All staff receive orientation and training at hire in the following areas related to security:

- Reception Alarm procedures
- Civil disturbance procedures

- Proactive Response Options Training
- Use of building keys
- Use of employee identification
- Building security issues, i.e., locked doors, after hour's admittance, parking lot safety
- Access to and confidentiality of health records

7.2. For personal safety and consumer service, front line support staff (receptionists and clerical) and staff who work with potentially dangerous consumers; shall be trained in de-escalation techniques. Other training shall be made available as deemed appropriate by the position.

7.3. Ongoing training and inservicing shall occur regarding issues of, but not necessarily limited to violence in the work place and personnel security.

8. Procedures for Unscheduled Clinical Staff Absence:

Clinician's will:

A) Contact supervisor or designee at home phone no later than 7:00 A.M. If direct contact is not made with supervisor/designee at their home, leave a WMCMH text message with supervisor and all team members no later than 8:00A.M., indicating high-risk appointments when feasible.

B) Change voicemail greeting indicating your absence for the day(s).

Supervisor or designee will immediately:

A) Review clinician's scheduler and evaluate appointments for high-risk.

B) Contact an alternative team member(s) to redirect high-risk consumer(s) and schedule accordingly.

C) Contact clinician's "home-base" front-desk secretary to report absence and identify redirection of high-risk consumer(s).

Secretary's will immediately:

A) Post absence in clinician's scheduler keying in all necessary data/codes for "therapist cancelled."

B) As instructed, enter high-risk consumer in the alternative team member's scheduler.

C) Contact non-risk consumers and reschedule a mutually convenient appointment.

FROM CELL PHONE

Text your Supervisor and Team Members.

Special tips: Keep a copy of the WMCMH employee extension list at your home.

RECORDING WMCMH EXTERNAL GREETING FROM HOME OR REMOTE PHONE

1. From a touch-tone phone call a WMCMH back-door number (e.g., (231) 843-5493; 873-6499; 745-8020) (if rotary phone move switch from pulse to tone).

2. You will hear the WMCMH automated greeting. During or after automated greeting it will prompt you to what is needed or do the following:

    - Press 7; then
    - Log into your mailbox by entering your extension number & #; enter your password number & #, then
    - Press 7
    - Press 1 for external greeting
    - Follow phone menu to record new greeting

9. Safety/Security Procedures with Customers for Protecting Consumer Confidentiality:

A Confidentiality Notice will be posted in WMCMH facility lobbies expressing WMCMH values to maintain consumer confidentiality.

EXTERNAL WORKER'S CONFIDENTIALITY STATEMENT:

Contracts for external operations providers (such as furnace repair, lawn maintenance, copier repair, etc.) will contain information about WMCMH confidentiality expectations. The contract will specifically indicate that it is the contractor's responsibility to ensure all of his/her staff are aware of and abide by WMCMH confidentiality/expectations. The contractor will be required to sign a document attesting to understanding and abiding by these expectations.

CONFIDENTIALITY NOTICE

Consumers receiving mental health services have rights that are safeguarded and protected by the Michigan Mental Health Code in addition to other laws. West Michigan Community Mental Health (WMCMH) promotes and endorses the rights of our consumers and we request external workers and visitors to join us in the responsibility to protect the rights, including confidentiality, of WMCMH consumers that may be observed during your visits here.

10. FACILITY ACCESS CONTROL (Key-less Entry) SYSTEM PROCEDURES:

Software & Enrollment Reader:

Software and Enrollment Reader is at 920 Diana, Ludington, this allows prox card/key enrollment for all 5 WMCMH locations on demand for immediate use.

System Administrator:

A select group of WMCMH employee's will have the responsibility of configuring, operating and printing the system data installed at 920 Diana, Ludington. Individual's identified:

- Zack Vander Wall, Facilities Specialist
- Lori Smith, Human Resources Generalist

Enrolling Proximity Cards into the System:

WMCMH employees will be assigned a prox card (key) allowing entry to all three (3) facilities.

KeyScan Keyless Entry Access Control System logs (tracking device of all prox cards enrolled as active or non-active) will be regularly monitored to determine usage of access to WMCMH facilities after routine business hours.

WMCMH housekeeping contract providers will be assigned prox cards accessible to their contracted site only. The WMCMH general maintenance contract provider will be assigned a prox card to access the three WMCMH outpatient facilities in Ludington, Hart and Baldwin.

Other contracted service providers (i.e. Carpet cleaners) may be provided a KeyScan key with an assigned time period.

External customers using WMCMH facilities after regular business hours and in need of a KeyScan card will be given access to a specific KeyScan door with an assigned user schedule (date & time schedule) to access door. At all times an employee of WMCMH sponsoring the group or activity will remain responsible for security.

Back-up Measures In Case of a Total Access System (prox card) Failure:

Hard keys will be identical to open all three (3) facilities. (Note: System includes a 7AH-battery back up lasting from 10 to 24 hours before releasing the KeyScan magnetic keyless lock system).

Proposed Schedule of Hard-Key Distribution:

- Each WMCMH Executive Team member and the Facilities Specialist will possess an identical hard key on site (capable of opening any Non-KeyScan keyless entry door at all WMCMH sites).
- Primary front-desk secretary (ies), as they are responsible to have facility consistently opened by 8:00 A.M.

11. INSTRUCTIONS TO ENTER/EXIT WMCMH FACILITIES BEGINNING 03/26/2001:

In a continuing effort to improve security, WMCMH installed "WMCMH Access Control Systems" (hereinafter referred to as KeyScan) at the following WMCMH employee door entrance/exit locations:

LUDINGTON:

Four (4) doors @ 920 Diana - East side middle door (employee entrance); South East side door (HST/Training Room entrance); South West side door (Service Entry); HST office, rooms #158 & #157.

HART:

Two (2) doors at 105 Lincoln: Northwest employee entrance and HST office, room #3

BALDWIN:

Two (2) doors at 1090 N. Michigan Avenue: North employee entrance and HST office, room 108B

PROGRESSIONS:

Hard key distribution only.

DIMENSIONS**:**

Hard key distribution only.

Staff members with offices at any of the five WMCMH facilities noted above will be issued a KeyScan Access Card. This card is the size and shape of a credit card, containing encoded data.

The KeyScan Card allows regular employees to enter all three WMCMH facilities at any KeyScan door identified above, 24-hours a day, and seven days a week. The KeyScan System monitors usage of all cards issued.

How to Use Your Card: Outside to the immediate left of the KeyScan door(s) there is a KeyScan card reader device (dark gray box). To enter the building present your KeyScan card by holding either side of your card in front of this device. The device automatically identifies your privileges to access the building and will disengage the magnetic lock for 10 seconds allowing your entry. It is recommended that you keep your KeyScan card on your key ring or in your wallet. Please, do **not** attach the KeyScan card with your employee identification badge (if your I.D. badge was to accidentally detach from you and become lost we do not want your key attached with it).

To Exit: All KeyScan doors have an automatic infrared sensor device that will sense your movement within a range of approximately 6 feet and will immediately release the magnetic lock for 10 seconds allowing your exit. In addition, a green Push to Exit button is near every KeyScan door. The Push to Exit button is a secondary emergency back-up device that releases the magnetic lock for exit.

Customer entrances at these five WMCMH locations will be unlocked during routine business hours. You may use any of the customer entrances to enter and/or exit the buildings. However, the locations of KeyScan doors are near preferred employee parking areas.

Please note in 2-12-9 of the WMCMH Administrative Manual for Safety and Therapeutic Environment for Control of Agency Keys (available to you via the Intranet). Item VI. 1.5. Specifies if a key/card is lost or stolen the employee losing the key/card shall complete a CIR and report the lost card immediately to HR staff and a new key/card will be issued and the previous card deactivated.

Additional information or clarification regarding the KeyScan Access System may be acquired from HR staff.

12. ACCESSING WMCMH FACILITIES DURING BUSINESS HOURS:

EMPLOYEES:

To improve safety/security measures within the West Michigan CMH employees shall be **encouraged to wear pictured identification badges at all times during agency business**. Good clinical judgement will be maintained; thereby, respecting a consumer's request that it not be worn during a public outing or other out-of-office setting.

CUSTOMERS:

Individuals in the WMCMH facilities without an employee identification badge will include; but not be limited to, consumers, visitors, board members, other professionals and service technicians. While occupying a WMCMH facility, consumers and visitors shall be escorted by an appropriate employee to and from lobbies and to coffee and other vending machines, as necessary. Employees shall introduce themselves and redirect any unescorted non-employee in a WMCMH facility area not applicable to them (this excludes areas such as; restrooms, lobbies and meeting rooms). Any unusual incidents shall be reported on a Critical Incident form EC001 within 24 hours.

SERVICE TECHNICIANS:

The WMCMH Facilities Specialist or designees shall coordinate work schedules with external service technicians notifying applicable staff when necessary.

13. *BUILDING SECURITY PROCEDURES WITH OUTSIDE CONTRACTORS AFTER BUSINESS HOURS:*

Building sites are to include; Ludington Sites at 920 Diana Street and 910 Conrad Industrial Drive; Hart Sites at 105 Lincoln and 101 Water St, and Baldwin Site at 1090 Michigan Avenue.

1. Scheduled Event:

    1.1 The site supervisor shall be notified of any "after hours" scheduled event.

        1.1.1 See the policies for use of agency buildings after hours for procedures in securing authority/approval for building use (i.e. outside meeting groups).
        1.1.2 The Facilities Specialist will notify the site supervisor when an outside contractor after business hours event will be occurring (carpet cleaning, painting, fire alarm testing, electrical, phone, computer, etc.). Event will

already have approval through signed contractual agreement or purchase order.

1.2 The site supervisor and/or the Facilities Specialist shall determine the responsible staff person in charge of such event.

1.3 The Facilities Specialist and/or site supervisor shall be responsible for building security and/or arrange building security for the event. The responsible staff person assigned shall be available to unlock the building prior to the event and ensure lock up after the event.

1.3.1 The Facilities Specialist or site supervisors will e-mail staff affected, reminding them to clear their desks of confidential material, log off computers and lock desks and file cabinets, as applicable.
1.3.2 The responsible staff person will check the area prior to event, securing confidential information they may find left out, lock applicable doors (see section 2.1 and 2.2), shut off computers left on, etc.
1.3.3 Upon completion of the event, the responsible staff person will examine the area as feasible taking notice of the quality of work completed; scan WMCMH assets and condition of the building/room after the event.

1.4 When the event affects an entire wing or an entire building (i.e., carpet cleaning), the Facilities Specialist shall be responsible for notifying the affected staff persons.

2. Building Security Issues: The health team offices that contain medications will be locked with a KeyScan and will require a KeyScan card to enter the room when it is not attended by a health team member.

3. Offices:

3.1 Staff in the affected area (wing or building) will make sure that their desks are free of confidential material.

3.2 Staff shall lock their desks and filing cabinets containing confidential material.

3.3 Staff shall be informed via e-mail of the scheduled event and will be asked to remove personal items off the floor for carpet cleaning purposes.

4. Keys:

4.1 No keys will be retained by outside contractors with the exception of housekeeping and maintenance personnel.

4.2 All building keys remain under the control of the, Facilities Specialist and as applicable front-desk receptionists.

Appendix 7.1.1.8

Device and Media Controls Procedure

Assumptions:

- Data, media, and portable electronic devices are the physical property of West Michigan CMH, wherever located, although consumers and others may have the right to access data.
- Individually identifiable health information is sensitive and confidential. Such information is protected from improper use and disclosure by HIPAA, its implementing regulations, other state and federal laws, professional ethics, and accreditation requirements.
- Loss or breach of confidentiality of such data may cause severe harm to the subject of the information, to West Michigan CMH, and to its officers, agents, and employees.
- It is difficult to protect portable assets, such as laptop computers, USB devices and such, other than by maintaining good physical custody and control over the asset.
- Insurance alone cannot compensate for the loss of West Michigan CMH data and equipment.
- West Michigan CMH personnel who remove data or information assets from a facility must be responsible for safeguarding such assets.
- Use of personal equipment, to record, store, or retrieve information relating to West Michigan CMH, its consumers, or business activities subjects the user to the terms of this procedure.

Procedure:

Data, media, computers that are not normally used in day to day activities, and other information assets may not be removed from West Michigan CMH without the consent of the appropriate supervisor. Such consent may consist of a blanket approval for certain personnel, such as employed clinicians, to remove and use such assets offsite. Supervisors will notify the Security Officer or designee when on-going consents are established.

If an employee, agent, independent contractor, or other authorized individual wishes to use personal information assets, such as a personal computer, PDA, or other portable electronic device, he or she must obtain the permission of the appropriate supervisor. The supervisor will notify the Security Officer or designee. The request for and granting of such approval manifests the individual's consent to be governed by this and all other relevant information security policies, such as the workstation use procedure.

Conditions for offsite use of data, media, computer, or other information assets include the following:

- Data, media, supplies, or information assets of West Michigan CMH are not to be used for private business purposes or for unauthorized reasons, such as unapproved research.
- When such assets are not on the premises of West Michigan CMH, they must be under the care and control of the person approved to use the assets.
- Usage of WMCMH data should be thru VPN and only thru WMCMH equipment.
- User assigned equipment may be used offsite
- Removal of unassigned equipment must have approval by his/her supervisor.

- Users must immediately report all losses of or damage to such equipment to their supervisor and the Security Officer or designee. Breaches of confidentiality and other reportable incidents must be reported in accordance with the confidentiality procedures.
- Users will safeguard assets appropriately. Assets, such as computers, PDAs, or removable media must not be left unattended. Users must secure media in appropriate locations.
- Before re-using media containing PHI, the data user will consult with the Security Officer for guidance as to how to destroy the data in such a way as to preserve confidentiality.

Approved by the HIPAA Workgroup 04/06/05 cr; Revised CCC July2010 fg; Reviewed: Jan2015 ck; 2/11/16 ck; 5/18/17ck; 5/31/19tf

Destruction Procedure

Assumptions:

- Confidential individually identifiable health information may reside in numerous locations and on different media—on magnetic media in hardware, on disks, and on paper.
- West Michigan CMH must destroy such data in a method that preserves confidentiality.
- Destroying data improperly may harm West Michigan CMH, its officers, employees, and agents, its consumers, and others on whom West Michigan CMH maintains individually identifiable health information.

Procedure:

West Michigan CMH, its officers, employees, and agents must destroy data that is no longer necessary to retain in the regular course of business pursuant to West Michigan CMH Retention Schedule. West Michigan CMH, its officers, employees, and agents must not destroy data that is involved in audit, investigation, or litigation.

West Michigan CMH employees and agents must destroy data as follows:

- Paper records must be shredded. Supervisors are responsible for determining whether to shred in-house or to use a commercial destruction service. The Information Systems Manager must approve the method of destruction for electronic media.

- Clinical paper information that is scanned into the WMCMH electronic health record will be stored in a secured location for six (6) months from scan date; at which point it will be picked up by Dimensions Unlimited for shredding.

Electronic media that has been determined to be of no further use by the Information Systems Manager must be cleared (using software or hardware products to overwrite media with non-sensitive data) or by destroying the media (disintegration, pulverization, melting, incinerating, or shredding). The Information Systems Manager must approve the method of destruction.

- Computer hard drives must be shredded in a manner approved by the Information Systems Manager.

- Supervisors will keep destruction records for not less than six years.

- The Compliance Officer is responsible for ensuring that selected destruction services entities have signed business associate agreements before providing destruction services.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed and revised 1/22/15 T. Bonstell; 2/16/16 T. Bonstell; 5/19/17 T. Bonstell; 5/31/19tb/tf

Appendix 7.1.1.10

Personnel Security Procedure

Procedure:

Screening of Individuals with Access to Individually Identifiable Health Information: WMCMH has determined that Human Resources is responsible for screening all employees with access to individually identifiable health information. The WMCMH pre-employment screening process includes:

- Criminal record check.
- Medicaid / Medicare Fraud activity check.
- Primary source verification of educational background and professional licenses held.
- Verification of references.
- Verification of employment history.
- In-depth interview.
- Drug and alcohol testing.

In addition, WMCMH conducts regular, ongoing background checks of employees on an annual basis. For full details of the pre-employment and on-going background checks, please see Policy 4.6.1– Background Checks.

Human Resources will retain the most recent records of screening in the personnel files. Upon separation from employment, the final set of screening records will be retained based on the personnel file records retention procedure. These procedures for personnel file management and retention are fully described in Policy 4.4.1 - Employee Personnel Record - General Policy.

Contract managers will direct the contracted entity to effectively screen its employees who will be given access to WMCMH customers' individually identifiable health information or any of its system data by stipulating this requirement in a clause of the vendor contract. Contractors will also be required to sign a confidentiality statement with WMCMH.

Training: HIPAA and the DHHS security and privacy regulations require training all personnel with access to individually identifiable health information. Training is an integral part of personnel security. As part of the mandatory training requirements of all new and continuing WMCMH personnel, training on the HIPAA Privacy and Security Policy and procedures adopted by the agency are included. In addition, all supervisors are responsible for training those who report to them about their specific responsibilities relative to the HIPAA Security Policy and procedures of the organization and how they apply within the department or program in which the employees work. These training requirements are detailed in Policy 4.6.2 – Orientation to Employment and Policy 4.6.4 – Training and Development.

Independent contractors granted access to individually identifiable health information of WMCMH customers or any of the WMCMH data systems are required by the terms of their contract with WMCMH to train their employees on the HIPAA Security regulations.

Supervision: Properly screening and training personnel with access to individually identifiable health information is not enough. Employees and others with access must be continually

reminded of their responsibilities concerning protection of health information. Therefore, supervisors must take the following steps:

- Detail security and confidentiality requirements in position descriptions and performance evaluations. Adherence to security and confidentiality procedures must be part of every data user's performance evaluation process. The competency and appraisal process used by WMCMH does this and is clearly detailed in Policy 4.6.3 – Performance and Competency Appraisal.
- Monitor the day-to-day performance of data users to detect problems with security and confidentiality before they become serious breaches.
- Audit compliance with security and confidentiality procedures in accordance with the WMCMH Information Audit Procedure.
- Report breaches of security or confidentiality in accordance with the WMCMH Report Procedure.
- Respond to breaches of security or confidentiality in accordance with the WMCMH Response Procedure.
- Take appropriate sanctions against data users who breach security/confidentiality in accordance with the WMCMH Sanction Procedure.

Contract managers must monitor the performance of independent contractors relative to the protection of individually identifiable health information to which they are given access. If a breach occurs, they must follow the WMCMH Report Procedure to report it. If the investigation of the breach substantiates it, the contract manager is responsible for holding the independent contractor accountable for the breach per the terms of the contract.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed Jan2015 as; 2/1/16 as; 5/17/19ask; 5/31/19 ask

Appendix 7.1.1.11

Videoconferencing Security Procedure

Assumptions

This Videoconferencing Security Procedures are based on the following assumptions:

- Videoconferencing can, in certain instances, provide better, more cost-effective health care than providing health services at one site alone.
- Use of videoconferencing can provide for better diagnosis and treatment than traditional referrals and consultations by allowing for remotely located physicians to interact live with the patient and his or her providers.
- Videoconferencing can provide additional contact between customers and caregivers, thereby improving their relationship and resulting in better care.
- Videoconferencing carries with it the risks inherent in any transmission of health information, such as loss of data integrity, availability, and confidentiality.
- Videoconferencing may result in the unauthorized practice of medicine in another state or other jurisdiction.
- Videoconferencing will be utilized by WMCMH employees or employees under contract with WMCMH and WMCMH customers

Procedure

West Michigan CMH will practice videoconferencing in appropriate cases only approved by the West Michigan CMH Executive Team or designee and in accordance with the law, medical ethics, and accreditation requirements. All personnel involved in video-conferencing must take the following actions:

- Safeguard the privacy and confidentiality of customers involved in videoconferencing.
- Videoconferencing will only occur for customers within the West Michigan CMH facilities and with the West Michigan CMH independent contract Internet healthcare service providers over a secured link (i.e., Telemedicine with 128 bit encryption or higher).
- Ensure the physical environment is secure at both ends for which videoconferencing is occurring, which includes confirmation of the identity of all involved parties.
- Ensure that one consumer does not appear in the background or otherwise when another customer's videoconferencing is occurring.
- Ensure that each customer's data is removed from the screen when the videoconferencing involving that customer is completed.
- Videotapes or other media involved will not be utilized during video conferencing.
- Report any violations of this Videoconferencing Security Procedure in accordance with West Michigan CMH Report Procedure.

Individuals in the following roles at WMCMH have the following responsibilities relative to videoconferencing for delivery of healthcare services:

Clinical Director:

- Ensure that Procedures for Clinical Oversite Committee detail the requirements for the practice of videoconferencing, including guidelines for routine and emergency use of videoconferencing.
- Ensure the attending staff person provides informed consent on the practice of videoconferencing. The information provided will enable the customer to evaluate knowledgeably the options available and the risks inherent in the practice of videoconferencing.

Information Systems Manager

- Establish video and image links to the correct location(s) and train staff.
- Perform necessary videoconferencing information asset maintenance.
- Audit videoconferencing for data integrity and for compliance and maintain documentation in accordance with West Michigan CMH policies and procedures.
- Test and revise videoconferencing procedures.
- Maintain documentation of videoconferencing security measures in accordance with West Michigan CMH Retention and Destruction Policies.
- Ensure that videoconferencing communications are secure and protected from breaches of confidentiality.

Approved by the HIPAA Workgroup 04/06/05 cr; Rev. Sep. 2008 tb; Reviewed & revised 1/22/15 T. Bonstell; 2/16/16 T. Bonstell; 5/19/17 T. Bonstell; 5/31/19tf

Appendix 7.1.1.12

Audiovisual Recording Security Procedure

Assumptions

These Audiovisual Recording Security Procedures are based on the following assumptions:

- Audiovisual Recording can, in certain instances, provide opportunities for direct supervision of consumer care and support enhancing quality of services delivered.
- Use of Audiovisual Recording can aid for better diagnosis and treatment than traditional referrals and consultations by enhancing ability of clinical supervisors to review entire sessions and provide feedback derived from direct observation.
- Audiovisual Recording carries with it the risks inherent in any collection, transmission, storage, and/or destruction of health information, such as loss of data integrity, availability, and confidentiality.
- Audiovisual Recording will be utilized by WMCMH employees and/or employees under contract with WMCMH and WMCMH customers.
- Audiovisual Recording will occur only in the context of a written consent from the consumer and with written supervisor authorization to use these devices for the purpose of enhancing care and/or providing supervision.

Procedure

West Michigan CMH will practice Audiovisual Recording in appropriate cases only in accordance with the law, medical ethics, and accreditation requirements. All personnel involved in Audiovisual Recording must take the following actions:

- Safeguard the privacy and confidentiality of customers involved in Audiovisual Recording
- Audiovisual Recording will only occur for customers within West Michigan CMH facilities
- Ensure the physical environment is secure when Audiovisual Recording is occurring and ensure that all participants have signed the WMCMH Consent for Videotaping, Audiovisual aid, and Photographing (Form CRO10).
- Audiovisual Recordings may be shared with other entities for the purpose of supervision and training only if a Business Associates Agreement is in place
- All sharing of Audiovisual recordings with a Business Associate must comply with existing WMCMH Device and Media Controls Procedures and the Security of Electronically Stored Clinical Information Policy
- Ensure that each customer's data is removed from the device when the Audiovisual Recording involving that customer is completed.
- All Audiovisual Recording materials will be disposed of in compliance with the WMCMH Destruction Procedure
- Videotapes or other media involved will not be utilized during video conferencing.
- Report any violations of this Audiovisual Recording Security Procedure in accordance with West Michigan CMH Report Procedure.

Individuals in the following roles at WMCMH have the following responsibilities relative to Audiovisual Recording for delivery of healthcare services:

Clinical Director:

- Ensure that Procedures for Clinical Oversite Committee detail the requirements for the practice of Audiovisual Recording, including guidelines for routine and emergency use of Audiovisual Recording.
- Ensure the attending clinician obtains written informed consent to practice Audiovisual Recording (Form CRO10). The consent must give the customer all information that will enable the customer to evaluate knowledgeably the options available and the risks inherent in the practice of Audiovisual Recording.

Support Services Coordinator

- Ensure that WMCMH Consent for Videotaping, Audiovisual aid, and Photographing (Form CRO10) are signed by all parties and are made part of the health record.
- Work with Information Systems Manager to ensure that Audiovisual Recording communications are secure and protected from breaches of confidentiality.
- Maintain required Audiovisual Recording confidentiality documents, such as consents, in accordance with West Michigan CMH Retention and Destruction Policies.

Information Systems Manager

- Establish audiovisual links and storage mechanisms and train staff.
- Perform necessary Audiovisual Recording information asset maintenance.
- Audit Audiovisual Recording for data integrity and for compliance and maintain documentation in accordance with West Michigan CMH policies and procedures.
- Test and revise Audiovisual Recording procedures.
- Maintain documentation of Audiovisual Recording security measures in accordance with West Michigan CMH Retention and Destruction Policies.

Approved by the HIPAA Workgroup 04/06/05 cr; Reviewed & Revised 1/22/15 T. Bonstell; 2/16/16 T. Bonstell; 5/22/17 T. Bonstell; 5/31/19 tf

Appendix 7.1.1.13

Access Establishment Modification Procedure

This procedure can be folded into the existing Policy 5.2.1.1 (Security of PHI and Safeguarding Health Records) that already addresses an employee's need to get at health records information. A few key paragraphs need to be added to that section.

Access authorization is the process of determining whether a prospective data user should be granted access to West Michigan Community Mental Health data. A data user is a person who has been granted explicit authorization to access West Michigan Community Mental Health's data by West Michigan Community Mental Health. Access must be granted in accordance with this Access Authorization and other related policies.

Health care providers, such as physicians and other therapists should have access only to data of Consumers that they have patient responsibility for, with an emergency override to access other Consumer data to respond to emergencies.

Access should be limited to necessary tasks, such as read-only, read and copy, read and edit by adding a new entry.

Electronic signatures must comply with West Michigan Community Mental Health electronic signature Procedure.

Upon receipt of a request to provide access to a named individual, the Information Systems Manager will determine whether any reason exists to deny the request. Grounds for denial include, but are not limited to, the following:

- A security risk unknown to the requester.
- Refusal of prospective data user to sign required documents.
- Inability of prospective data user to properly use applications and system assets after training.

The Information Systems Manager will work with the requester to resolve cases in which the former initially denies access. If the matter cannot be resolved, the Information Systems Manager will report the matter to Human Resources for resolution.

No person should have access who does not need access and no person should have more access than necessary, West Michigan Community Mental Health may determine that an individual or a group of individuals need more, less, or otherwise changed access because of a change in duties or a change in status, such as full-time to part-time, employee to outside contractor, completion of a project, and the like. When a supervisor makes such a determination, the Human Resources Department should be notified and HR should request that the Information Systems Coordinator or his/her designee change the current level of access to another level of access.

Reviewed & Revised 1/22/15 T. Bonstell; 2/16/16 T. Bonstell; 5/19/17 T. Bonstell; 5/31/19tf

Appendix 7.1.1.14

Procedures for selecting Health Record Information for Reviewers

Security Measures:

Reviewers should be able to use a single software-viewing tool to access information.

Reviewers are required to use WMCMH equipment, and access to EHR information that will be kept on the WMCMH network.

Reviewers will be required to use WMCMH provided user ids and passwords that will expire within a specific date as identified by the supporting WMCMH personnel for the review.

Review Measures:

Care will be given to environmental surroundings such as location and unwarranted access to records in order to preserve the integrity and confidentiality of the records being reviewed.

Locking the laptops/workstations is required when unattended.

Automatic logging off for significant idle times will be implemented.

Under no circumstances will EHR information be exported to portable media and/or Reviewers devices.

User logging and record access will be recorded and maintained by WMCMH.

Reviewers must follow the health records procedure on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the printouts, and how to maintain confidentiality of hard-copy printouts.

Reviewed and revisions made 1/22/15 T. Bonstell; 2/16/16 T. Bonstell; 5/19/17 T. Bonstell; 5/31/19 T. Bonstell