


CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security	
WRITTEN BY Arthur Williams, MCSA & Michelle Gould-Rice, LMSW, Quality Improvement Coordinator	REVISED BY Arthur Williams, BS, MCSA Network Administrator Sandy Koyl, BHSA IT and Data Management Supervisor	AUTHORIZED BY  Brooke Sankiewicz, LMSW, CADC, CEO	

APPLICATION:

<input checked="" type="checkbox"/> CMH Staff	<input checked="" type="checkbox"/> Board Members	<input checked="" type="checkbox"/> Provider Network	<input checked="" type="checkbox"/> Employment Services Providers
<input checked="" type="checkbox"/> Employment Services Provider Agencies	<input checked="" type="checkbox"/> Independent Contractors	<input checked="" type="checkbox"/> Students	<input checked="" type="checkbox"/> Interns
<input checked="" type="checkbox"/> Volunteers	<input type="checkbox"/> Persons Served		

POLICY:

Lapeer County Community Mental Health (LCCMH) administrative and technical control processes assure the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). This policy applies to all persons and resources involved in the creation, modification, storage, transmission, use, and management of protected health information.

STANDARDS:

- A. **Assigned Security Responsibility:** LCCMH ensures a Privacy Officer and Security Officer are assigned and the duties and responsibilities of same are established. The Security Officer has the overall and final responsibility for compliance relating to the safeguarding of electronic Protected Health Information (ePHI) at the agency. The Security Officer addresses security issues as they arise and recommends and approves immediate security actions to be

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

undertaken. It is the responsibility of the Security Officer to identify areas of concern within the agency and act as the first line of defense in enhancing the security posture of the agency. REFERENCES: 45 CFR § 164.308(a)(2)

- B. **Access Control and Management:** LCCMH ensures protected health information access privileges are only provided to authorized personnel and such access authorization for viewing and editing functions is based on roles and job requirements. It also outlines the actions required to be performed at the time an employee or contractor is terminated and no longer requires access to confidential information as part of their job function. REFERENCES: 45 CFR §§ 164.308(a)(4), 310(a)(1) & 312(a)(1); 45 CFR § 164.308(a)(3)
- C. **Encryption:** LCCMH assures the integrity and confidentiality of health information while at rest or in transit by requiring the application of encryption technology on the computer network, computing and storage devices (mobile and stationary), and software programs. REFERENCES: 45 CFR § 164.312(a)(1) & 312 (e)(1)
- D. **Network Security:** In addition to the measures stipulated under the Access Control and Management, and Encryption policies, LCCMH establishes additional measures to protect the network environment from unauthorized access and malicious activities. REFERENCES: 45 CFR § 164.312(e)(1)
- E. **Management and Exchange of Health Information:** LCCMH establishes standards for the proper management and secure exchange of health information with persons served and external entities. REFERENCES: 45 CFR § 164.312(e)(1)
- F. **Acceptable Use & Secure Disposal of Computing Resources:** LCCMH specifies the proper use of computers, internet connectivity, and removable media/data storage devices. LCCMH also establishes measures required for securely decommissioning and disposing of computer assets. REFERENCES: 45 CFR § 164.310(b), (c), & (d)(1)
- G. **Secure Software & Malicious Code:** LCCMH ensures the use of authorized software and guard against malicious software programs.
- H. **Risk Management & Risk Analysis:** LCCMH establishes procedures to reduce risks and vulnerabilities to the agency to reasonable and acceptable levels. LCCMH conducted an initial risk analysis, to be followed by recurring risk analyses for the purpose of determining what security measures are appropriate

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

to prevent, detect, contain, and correct security violations. REFERENCES: 45 CFR § 164.308(a)(1);

- I. **Security Incident Management:** LCCMH establishes guidelines for the proper management of security incidents. REFERENCES: 45 CFR § 164.308(a)(6)
- J. **Audit Controls & Information Systems Activity Review:** LCCMH records and routinely examine all activities on its information systems. REFERENCES: 45 CFR §§ 164.308(a)(1) & 312(b)
- K. **Business Continuity & Disaster Recovery:** LCCMH implements and maintain a contingency and recovery plan to respond to natural and man-made disruptions that may compromise the confidentiality, integrity or availability of the protected health information maintained by LCCMH. Procedures are in place for managing and documenting encounters with persons served when Electronic Health Record (EHR) and Practice Management (PM) systems are unavailable due to planned or unexpected outages. REFERENCES: 45 CFR §308(a)(7)
- L. **Security Awareness Training:** LCCMH provides an ongoing security awareness training program for all employees. The security awareness program provides employees with best practices to maintain the confidentiality, integrity, and availability of the agency’s protected health information. REFERENCES: 45 CFR § 164.308(a)(5)

PROCEDURES:

A. Assigned Security Responsibility

- 1. LCCMH has established a Privacy Officer and Security Officer as required by HIPAA. This Privacy Officer in conjunction with the Security Officer oversees all ongoing activities related to the development, implementation, and maintenance of the LCCMH privacy policies in accordance with applicable federal and state laws.
 - a. The current Privacy Officer for LCCMH is
 - i. Quality Improvement Supervisor
 - ii. Telephone Number: 810-245-8550
 - b. The current Security Officer for LCCMH is

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

- i. IT & Data Management Supervisor
 - ii. Telephone Number: 810-245-8280
2. The Privacy Officer and Security Officer are responsible for developing all policies and procedures relating to the security rules governing ePHI.
 3. The Privacy Officer and Security Officer are responsible for the implementation of all the policies and procedures related to the use and disclosure of ePHI, as required by the security rules.
 4. The Network Administrator/IT Consultant and Security Officer are responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. The log also documents security enhancements and features implemented to further protect all sensitive information.

B. Access Control and Management:

1. Access Grants

- a. Access privileges to the computer network and all systems and programs in which protected health information is created, modified, stored, transmitted or maintained is restricted to employees or contractors based on job function and need to know.
- b. Individual access to the computer network and all information systems is based on unique identifications so each user has a unique identifier and user-specified password.
- c. The password created by an employee is case sensitive and cannot be less than eight (8) characters in length and may contain alpha-numeric characters (letters and numbers). The password cannot be provided to any other person. The password is set to expire and be changed at least once every ninety (90) days. The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts for the Electronic Health Record and ten (10) unsuccessful logon attempts for network computers which then require the passwords to be reset by

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

the Network Administrator or IT and data staff.

- d. Access to information is a privilege and with it comes responsibility. Employees use information and computer resources only for the purposes intended. Employees access data on a "need to know" basis only. Any access to electronic data not for a specific need or business related to the person served is strictly prohibited.
- e. Violation of this policy leads to disciplinary action. Any employee who accesses information about a person served without a specific "need to know" may be subject to immediate termination.
- f. System privileges must be defined based on job function so:
 - i. The authority to grant access privileges is limited to the Network Administrator/IT Consultant and the IT and Data Management Supervisor or designee after reviewing access needs with the staff program supervisor.
 - ii. IT Staff or contractors are granted the minimal necessary access to production information relevant to the work which they are contracted to perform.
- g. Quarterly, the Network Administrator/IT Consultant facilitates entitlement reviews to ensure all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect the data of the person served.
- h. All user login IDs are audited at least quarterly by the Human Resources Department, Contracts Management Department, and IT & Data Department. An Active Directory user list is generated and emailed, they respond with needed changes and then the Network Administrator confirms and makes the designated changes.
- i. User activity reports in the electronic health record are generated quarterly and reviewed by the IT and Data Management Supervisor. User accounts are updated as needed based on user location and job functions.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

- j. The Human Resources Department notifies the IT and data staff via emailing the 'Staffing Updates' distribution group upon the departure of all employees and contractors, at which time all specified credentials are revoked.
- k. The IT and data staff inactivate all login ID's to EHR accounts based on the quarterly audit.
- l. Entitlement reviews and user log ID audit activities are tracked so a record of these activities is available if needed. Active Directory User List activity is maintained by the Network Administrator.
- m. All users of LCCMH information resources sign, as a condition for employment, an appropriate confidentiality agreement. See LCCMH Form #143.
- n. All temporary workers and third-party employees not already covered by a confidentiality agreement signs LCCMH Form #143 before accessing LCCMH information resources.

2. Access Termination

- a. When any workforce member no longer works for LCCMH, the Supervisor or Data Management Staff must review the individual's access status and request termination from the Network Administrator/IT Consultant (before the individual's actual departure, if possible) for all information systems access.
 - i. All access rights must be terminated immediately upon the departure of such employee.
 - ii. The Supervisor and/or IT staff or designee must retain and/or retrieve every property of the agency in the possession of the terminated employee or contractor. See LCCMH Form #148 and Form #282.
 - iii. Keypad codes are revoked or changed.

C. Encryption:

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

1. **Network Encryption** In order to maintain the security of the computer network environment, appropriate encryption technology must be activated on the appropriate network devices.
2. **Encryption of Devices & Software Programs**
 - a. All computing or data storage devices such as desktop computers, laptops, tablets, flash drives, tapes, compact disks, and floppy disks used for processing and storing health information of a person served must be encrypted. LCCMH staff does not transport any PHI on USB drives/flash drives, tapes, compact disks, floppy disks, or mobile phones.
 - b. All software programs used in processing the health information of a person served have the applicable levels of encryption or data security measures activated.

D. Network Security:

1. There is an active firewall to monitor and secure internet traffic.
2. All remote connections to the computer network environment must use secure network technology such as a Virtual Private Network (VPN); and properly encrypt, authenticate, and log VPN connections.
3. Wireless network encryption must be activated for all wireless computer networks.
4. The computer network devices are securely located to safeguard the physical security of those assets.
5. Server racks are locked and access to the room in which they reside is also locked, but accessible only to authorized personnel.

E. Management and Exchange of Health Information:

1. Access to health records – Persons served have an inalienable right to their health records and upon request receive copies of the same without hindrance.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

2. The exchange of health information of persons served with external entities is only for the authorized purposes of administering appropriate care or for the legal and authorized use of health information for public and population health.
3. The bi-directional or uni-directional electronic transmission of health information is completed securely to assure the privacy and security of the health information of the person served.

F. Acceptable Use & Secure Disposal of Computing Resources:

1. Workstation usage—All functions performed at any workstation are consistent with the agency policies relating to the use, disclosure, and maintenance of protected health information. All workstations are provided for business purposes and the use of these facilities for non-business or unauthorized purposes, without approval, are regarded as improper use of the facilities.
2. All workstations, including all LCCMH-owned laptops are used securely and in accordance with the following requirements:
 - a. Authorized users are assigned unique IDs. Users create their own specific passwords.
 - b. Authorized users are assigned a workstation. In some circumstances, a workstation can be shared by more than one person.
 - c. Authorized users log on to work with confidential information including electronic protected health information only when there is a need to do so and they immediately log off when finished.
 - d. Authorized users lock or log off from the workstation when leaving the area of the workstation.
 - e. Automatic locking procedures are implemented after fifteen (15) minutes of inactivity.
 - f. Workstations are located in areas to minimize unauthorized visibility. Monitors in public-access areas are to be pointed away from public view when possible.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

3. The use of unauthorized, non-LCCMH-owned computing devices including workstations, laptops, or phones for processing health information, or any other work-related purposes other than to access Oasis or Web Access email is prohibited and the security of these devices is the responsibility of the owner.
4. Use of the agency's internet connection for non-work related purposes is limited to those permitted by management.
5. Removable Storage Devices –LCCMH does not permit the use of removable devices such as flash drives and CDs for storing the health information of persons served. Any exceptions to this policy statement require prior approval from the Network Administrator and Security Officer and the device must be encrypted.
6. Only approved removable data storage devices owned by the LCCMH are used in the agency.
7. The removal of such data storage devices from the premises of the LCCMH must be authorized by the Network Administrator and Security Officer.
8. Upon decommissioning a computing resource (including but not limited to computers, printers, and removable devices), adequate steps must be taken to forensically erase the agency's data residing in such assets. The erasure must be such that conforms to industry standards in order to prevent unauthorized access to protected health information.
9. Decommissioned computing assets are removed from the premises of the agency to be physically destroyed or disposed of as appropriate.
10. A record of destruction is maintained by the IT department.

G. Secure Software & Malicious Code:

1. All software programs at LCCMH are legally owned or licensed by LCCMH except for those freely distributed by legal copyrights holders or open source software.
2. The use of software programs is limited to those provided and authorized by LCCMH.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

3. Employees and contractors are prohibited from downloading and using any software program unless authorized to do so by the Network Administrator or Security Officer.
4. Antivirus/antimalware programs are installed on all appropriate computing resources to guard against software-based threats.
5. Updates to all software programs are overseen by the Network Administrator and Security Officer.

H. Risk Management:

1. LCCMH develops and implements a Risk Management Program/Plan, specific to the needs of the agency, designed to reduce risks and vulnerabilities relating to the use, disclosure, and maintenance of protected health information within the agency.
2. All employees are trained and educated on those aspects of the risk management program relevant to their job duties.
3. Risk Analysis: The risk analysis considers all relevant losses expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity expected to occur absent the security measures. The degree of response is determined by the risks identified.
 - a. LCCMH conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI.
 - b. LCCMH implements reasonable security measures to reduce risks and vulnerabilities based on results of the risk analysis.
 - c. At the minimum, the Risk Analysis covers the following:
 - i. Identification of Electronic Protected Health Information (ePHI)
 - ii. Identification of Vulnerabilities and Threats
 - iii. Analysis of current Risk Control Measures

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

iv. Determination of Risk Exposure

v. Recommendation of Risk Control Measures

- d. LCCMH conducts periodic evaluations (at least once every year), using the most recent risk assessment as a baseline, to determine whether changes to the agency's security program are warranted.
- e. Vulnerability assessment tools are used to analyze the network for vulnerabilities, and their results are logged along with the Risk Assessment.

I. Security Incident Management:

1. Security Incident – A “security incident” is any incident in which there is an actual or suspected threat to any of the agency's information systems. This includes but is not limited to any unauthorized access to any of the agency's information systems or any unauthorized disclosures of information from the information systems.
2. Security Incident Reporting – If an employee becomes aware of or reasonably suspects a “security incident” has occurred, they are to immediately report such incident to the Network Administrator/IT Consultant and/or the agency Security Officer.
3. Security Incident Response – The Network Administrator/IT Consultant and/or Security Officer immediately assesses the severity of any reported incident and takes the appropriate steps to mitigate any harmful effects of the incident. Once the security incident has been addressed the Network Administrator or Security Officer documents the cause of the incident, if known, and the steps taken to prevent a similar incident in the future. Incidents and remediation are documented in a help desk ticket. If any information for a person served was subject to breach, the agency addresses the breach following the LCCMH Breach Policy # 07.001.35.

J. Audit Controls & Information Systems Activity Review:

1. LCCMH reserves the right to routinely monitor activities on all information systems.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

2. Audit Logs – LCCMH ensures any information system in which electronically protected health information is used and/or disclosed has the capability of maintaining an audit log of all such uses or disclosures. At a minimum, the audit log records:
 - a. The date and time electronic information was accessed and identify the individual accessing the information;
 - b. Whether the information accessed was modified and the identification of the individual modifying the information; and
 - c. Whether new information was created and the identification of the individual creating the information.
3. Review of Audit Logs – The Security Officer periodically reviews the audit logs to determine and ensure the appropriate use of the agency’s information systems. In the event of a known breach or security incident, the Security Officer reviews the audit logs in the course of the investigation of the breach or security incident.
4. Maintenance of Audit Logs – Audit logs relating to use or disclosure of electronic protected health information is maintained for at least seven (7) years. All other audit logs, not involving electronic protected health information, are maintained for at least six (6) months.

K. Business Continuity & Disaster Recovery:

1. Data Backup Plan – LCCMH establishes and maintains a data backup plan whereby it has access to an exact copy of the electronic records maintained in the agency’s information systems. This includes both electronic information and the agency’s electronic business information.
 - a. The EHR software vendor, PCE has a formal Disaster Recovery Plan to restore system functionality in the event of a major event severely affecting system availability. The vendor’s Disaster Recovery Plan includes the implementation of a “Hot Site” with a fully replicated system environment that can be activated if the PCE Data Center is destroyed. PCE’s Hot Site is tested every month.
 - b. PCE has been the software vendor since October 2007. PCE has historically provided no less than 99.9% uptime. PCE makes all

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

reasonable efforts to maintain uptime at 99.9%, which includes all updates to the system.

2. Notification: The IT and Data Management Supervisor or Network Administrator/IT Consultant notifies all CMH administration, staff, and contract providers as soon as possible in the event of:
 - a. planned downtime of EHR systems,
 - b. unexpected outage of EHR systems, and
 - c. resumption of EHR services following an outage so normal operations may resume.
3. Encounters with Persons Served:
 - a. Clinical staff use their paper calendar to record an encounter with a person served for billing/tracking purposes. Check-in staff verify the person's name, date of birth, telephone number, home address, and insurance information as available on the paper.
4. Disaster Recovery Plan – LCCMH establishes and maintains a Disaster Recovery Plan, which would allow LCCMH to restore any loss of data or access to data. Included within this plan are processes for allowing individual (employee or contractor) access to the facility or resources.
5. Emergency Mode of Operation Plan – LCCMH establishes and maintains an emergency operation plan allowing timely resumption of business operations immediately following a natural or man-made emergency. Included within this plan processes for allowing individual (employee or contractor) access to the facility and/or the electronic information systems while in emergency operations mode.
6. Plan Testing and Revisions – LCCMH periodically conducts table top exercises to test the feasibility of its contingency plans.
7. Applications and Data Criticality – LCCMH assesses its individual information systems and applications to determine the criticality of such systems in order to plan appropriately for recovery.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

L. HIPAA Security/Awareness Training:

1. HIPAA Security Program – There is a standing security awareness training program designed to educate both new and current employees on issues relating to safeguarding protected health information. New employees are provided with training during the orientation process. Existing employees are provided with ongoing training as needed but no less than once per year. Security awareness training may vary based on an employee’s job function; however, all employees are trained on HIPAA Privacy and Security measures relative to the agency.
2. Employees who undergo the security awareness training sign an acknowledgment attesting to their having participated in the training session.

DEFINITIONS:

Code of Federal Regulations (CFR): The codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government.

Electronic Protected Health Information – Electronic protected health information (ePHI) refers to any protected health information (PHI) covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

Encryption – Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Firewall – A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether they are allowed through or not, based on a predetermined rule set.

HIPAA – The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by the United States Congress and signed into law in 1996. Among other provisions, the law addresses the Privacy and Security of health data, and specifies standards meant to improve the efficiency, effectiveness, and safety of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

HITECH - The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

Privacy Officer – Designated staff responsible for the development, implementation and adherence to privacy policies and procedures for the safe use and handling of protected health information.

PCE – Peter Chang Enterprises, d.b.a. PCE

Security Officer - Designated staff responsible for the continuous management of information security policies, procedures and technical systems in order to maintain the confidentiality, integrity and availability of the agency’s information systems.

Virus - A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

VPN – Virtual Private Network – Provides a secure passage through the public Internet.

WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.

REFERENCES/EXHIBITS:

- LCCMH Form #143 Confidentiality Policy Receipt
- LCCMH Form #148 Termination of Employment/Affiliation
- LCCMH Form #282 Inspection and Receipt of Returned Hardware
- 45 CFR-Code of Federal Regulations
- 45 CFR § 164.308(a)(2)
- 45 CFR §§ 164.308(a)(4)
- 45 CFR §§ 164.310(a)(1)

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 20
SECTION Information Systems		DESCRIPTION Information Security Policy	

- 45 CFR §§ 164.312(a)(1)
- 45 CFR § 164.308(a)(3)
- 45 CFR § 164.312(a)(1)
- 45 CFR §§ 164.312 (e)(1)
- 45 CFR § 164.312(e)(1)
- 45 CFR § 164.312(e)(1)
- 45 CFR § 164.310(b)
- 45 CFR §§ 164.310(c)
- 45 CFR §§ 164.310 (d)(1)
- 45 CFR § 164.308(a)(1)
- 45 CFR § 164.308(a)(6)
- 45 CFR §§ 164.308(a)(1)
- 45 CFR §§ 164.312(b)
- 45 CFR §308(a)(7)
- 45 CFR § 164.308(a)(5)

AW: lr