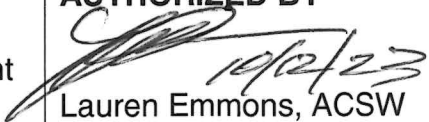


CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 40
SECTION Information System		DESCRIPTION Remote Work and Access	
WRITTEN BY Sandy Koyl, BHSA IT, Billing and Data Management Supervisor	REVISED BY Sandy Koyl, BHSA IT and Data Management Supervisor	AUTHORIZED BY  Lauren Emmons, ACSW CEO	

APPLICATION:

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

POLICY:

Lapeer County Community Mental Health (LCCMH) optimizes workforce efficiency and productivity through effective use of remote technologies enabling staff to work remotely where feasible, safe, and allowable by law.

STANDARDS:

- A. LCCMH make reasonable technology accommodations to equip staff to perform some or all of their job duties from a qualified remote location.
- B. Working remotely requires approval of the Chief Executive Officer (CEO).
- C. Remote access is granted to staff who are assigned information technology (IT) equipment that can be used to access the LCCMH IT network from outside the agency’s buildings.
- D. Working remotely may or may not be specified within staff job descriptions.

PROCEDURES:

- A. A supervisor may request working remotely as an option for staff under their supervision.
- B. Before making a request, the supervisor discusses secure remote access procedures with staff and assures the appropriate equipment is available.
- C. Agency assigned cell phones with hot spot capability are used. If a cell phone is not available, Internet access at the remote site must be secure and have appropriate bandwidth. Staff receives LCCMH IT Department approval prior to use.
- D. Staff working remotely are responsible for protecting the confidentiality of the information they access. Staff assures sensitive information is not visible to unauthorized persons, measures are taken to protect the computer screen, such as a privacy screen or moving to a location where the display is only visible to the user.
- E. When accessing the agency network resources the staff must use the agency Virtual Private Network (VPN) to connect.
- F. When using a home or public network, such as Internet access provided by restaurant or hotel while attending a conference or training, the staff must first connect using the agency VPN.
- G. Any limitations on the type of work to be performed remotely are written at the time of the approval.
- H. All computers/tablets used for working remotely must be owned and provided by LCCMH. Exceptions to this policy are only allowable with the approval of the CEO or IT Department.
- I. IT Supervisor or designated IT staff ensures remote equipment is available to staff approved to work remotely.
- J. LCCMH-provided equipment needs to be returned to the IT department and remote user logins will be disabled when working remotely is no longer approved. IT staff completes Form #282.
- K. While working remotely, staff are expected to comply with all LCCMH policies and procedures.
- L. Technical support can be accessed through email or calling the IT Department.

DEFINITIONS:

Bandwidth: Internet connection speed and reliability to allow for access to LCCMH IT resources.

Internet Access: The ability to connect to the Internet safely and securely.

Working Remotely: Working in a location other than a LCCMH office space, this could include (as an example) an employee's home, community setting with a person served, hotel, etc.

Virtual Private Network (VPN): A suite of protocols which establishes a secure connection to LCCMH IT resources.

SK:lr