CHAPTER: **10**	SECTION: **7**	SUBJECT: **MANAGEMENT OF INFORMATION**
TITLE: **WORKSTATION USE**		
EFFECTIVE DATE: **5/12/03**	REVIEWED/REVISED DATE: **2/11/13, 3/11/14, 9/21/15, 9/1/17, 4/12/19, 6/3/20, 5/6/2021, 12/10/21, 02/16/23, 11/17/23**	
ISSUED AND APPROVED BY: EXECUTIVE DIRECTOR		

I. PURPOSE:

This policy on Workstation Use is intended to meet the privacy requirements of HIPAA. Community Mental Health of Ottawa County (CMHOC) will assure that its staff meets these requirements for the purpose of protecting the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements for in-office and alternative work locations.

II. APPLICATION:

All personnel of CMHOC that use computer terminals and have access to protected health information must be familiar with the contents of this policy and follow its guidance. Familiarity with the plan and demonstrated competence in the requirements of the plan are required for all current staff as of the application date, as well as new staff as a part of their orientation.

III. DEFINITIONS:

Protected Health Information (PHI): PHI is individually identifiable health information that identifies the individual or that provides a basis for identifying the individual that is transmitted or maintained in any form or medium.

Protected Identifiable Information (PII): PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Alternative Work Location (AWL): Alternative Work Location (AWL) is a voluntary alternative to the traditional workplace to allow employees to work at an alternative location (typically the employee’s home) for all or part of their regular workweek.

IV. POLICY:

It is the policy of CMHOC that all employees, and all organizations under contract with CMHOC that maintain health information, will assure that all PHI /PII has integrity, accuracy, and its confidentiality is protected.

V. PROCEDURE:

A. Assumptions

1. Every computer workstation in the facility and alternative work locations is vulnerable to environmental threats, such as fire, water damage, power surges, etc.
2. Any computer workstation in the facility or in alternative work locations can access confidential patient information if the user has the proper authorization.
3. All computer screens may be visible to individuals who do not have access to confidential information that may appear on the screen.

B. Preventative Measures - Persons with access to protected health information/protected identifiable information should carry out the following preventive activities:

1. Report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, if air conditioning fails and the temperature around the computer could exceed a safe level, the user must immediately notify the MIS Department.
2. Make sure all computers plugged into an electrical power outlet use a surge suppresser approved by the Health Information Management Department.
3. All staff using computers will familiarize themselves with and comply with the facility's disaster plans and take appropriate measures to protect computers and data from disasters such as floods.
4. All users should avoid any activity that may damage equipment.
5. Staff logging onto the system will ensure that no one observes the entry of their password.
6. Staff will neither log onto the system using another individual’s password nor permit another individual to log on with their password. Nor will staff enter data under another person’s password.
7. After three failed attempts to log on, the system will refuse to permit access and generate a notice to the system administrator.
8. When working off site, staff must use a VPN or VDI connection. MFA (Multifactor Authentication) must be used such as DUO for secure connection to VPN. Staff must also adhere to appropriate procedures when logging out of the system and locking the computer when leaving the area. Staff will use good judgment to assure that PHI is kept secure when working off site.
9. It is discouraged that employees transport files or physical work product to their alternative work location. All work should be completed using the Electronic Health Record, digital files and notes, and employees should adhere to being paperless.
10. Each person using the facility’s computers is responsible for the content of any data he or she inputs into the computer or transmits through or outside the facility’s system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All staff will familiarize themselves with and comply with the facility e-mail policy.

11. No employees may access any confidential patient or other information that they do not have a need to know. No employee may disclose confidential patient or other information unless properly authorized (see the Confidentiality Policy and the Disclosure Policy).
12. Employees must not leave printers unattended when they are printing confidential patient or other information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
13. Employees may not use the facility's system to solicit for outside business ventures, organizational campaigns, or political or religious causes. Nor may they enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are pornographic. 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 orientation, or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.
14. Employees using the computer system will not write down their password and place it at or near the terminal, such as by putting their password on a yellow post it note on the screen, or a piece of tape under the keyboard.
15. Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period. Supervisors may specify an appropriate period to protect confidentiality while keeping the computer available for use in conjunction with the Health Information Management Department.
16. Except in an extreme emergency, employees must log off the system if he or she leaves the computer terminal for any period of time.
17. Employees shall ensure that data entered into the system is accurate.
18. Hard copy printouts of PHI must be destroyed or placed in the secure shredding bin after use, or after being filed in the consumer's record within 24 hours. Hard copy printouts are available only to those staff with a specific need to know. Any use of hard copy PHI must meet all requirements for release of information.
19. Although all CMHOC computers have hard drive encryption, CMH staff may not download data from the Electronic Health Record (EHR) onto external storage devices such as a diskette, CD, hard drive, fax, scanner, any network drive or any other hardware like flash drives, software, uploading to cloud storage such as Google Drives, Dropbox, etc., or paper without the express permission of the privacy officer, unless specifically required as part of their job.
20. No personnel may download any software without express written permission of the MIS Department. This rule is necessary to protect against the transmission of computer viruses into system.

VI. ENFORCEMENT:

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment, professional discipline, or criminal prosecution in accordance with the Ottawa County Policy.

VII. ATTACHMENT:
Not Applicable.

VIII. REFERENCE:
Ottawa County Policy, Acceptable Use
Ottawa County Policy, HIPPA Compliance
Ottawa County Policy, Information Security
CMHOC Operational Guideline, 1.4 Alternative Work Location