Issue Date: 11/2020

Review and/or Revision Date: _____

SUBJECT		CHAPTER	SECTION	SUBJECT
Telecommuting		03	01	11
CHAPTER	**SECTION**			
Information Management	Technology			
WRITTEN BY	**REVIEWED BY**		**AUTHORIZED BY**	
Jason Radmacher			PIHP Board	

I. APPLICATION:

☐ PIHP Board ☐ CMH Providers ☐ SUD Providers
☒ PIHP Staff ☐ CMH Subcontractors

II. POLICY STATEMENT:

It is the policy of the Region 10 PIHP to optimize workforce efficiency and productivity through effective use of remote technologies that enable staff to work remotely (telecommute) where feasible, safe, and allowable by law. As such, Region 10 PIHP will make reasonable technology accommodations to equip eligible staff to perform some or all their job duties from a qualified remote location.

III. DEFINITIONS:

Bandwidth – Internet connection speed and reliability to allow for access to Region 10 PIHP information technology (IT) resources.

Eligible Employee/Staff – Employees under consideration or approved to telecommute to perform remote work on behalf of the agency.

Internet Access – The ability to connect to the Internet safely and securely as provided by the eligible staff, ensuring adequate bandwidth to support work as if the person were working in the office.

Remote Work: Work performed in a location other than a Region 10 office space which may or may not be performed during regular business hours. Depending on the nature of the work, this could include (as an example) an employee's home, hotel, etc.

Unsecured PHI: Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

VPN – Virtual private network, allows eligible staff working off-site to securely connect to Region 10 IT resources as if they were in the office.

SUBJECT	CHAPTER	SECTION	SUBJECT
Telecommuting	03	01	11
CHAPTER Information Management	**SECTION** Technology		

Workforce: Workforce means employees, volunteers, trainees, and other persons under the direct control of the PIHP, whether or not they are paid by the PIHP.

IV. PROCEDURES:

A. Telecommuting is an arrangement for eligible staff to engage remote work in a location other than their primary office. It may be a temporary approval, such as approvals for those attending a conference, or a more permanent allowance for work completed at a home office. The approvals are under the authority of the Chief Information Officer (CIO) and may be delegated as they see fit to no lower than the Supervisor level. No individual outside of the Chief Executive Officer (CEO), Chief Operations Officer (COO) or CIO may self-approve their own telecommuting.

B. Telecommuting may or may not be specified within the job description of the eligible staff and will be allowable under the provisions of Region 10 Personnel Manual.

C. A supervisor may suggest telecommuting as an option for completing work. For telecommuting requests, the eligible staff's supervisor shall review why telecommuting is advisable for the benefit of the Region 10 PIHP. The request for telecommuting cannot be considered if there are any legal or practical barriers to effective telecommuting as described.

D. Before forwarding the request, the supervisor will discuss the feasibility and practicality of the request by reviewing the following factors with the eligible staff:
    i. Internet connectivity at the remote site(s).
        1. Unless otherwise approved by the CIO, the eligible staff is responsible to provide the necessary Internet access with appropriate bandwidth.
    ii. Physical environment of the remote site.
        1. If the remote site would make sensitive information visible to unauthorized persons, the request cannot be approved unless 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. Telecommuting staff are responsible for protecting visibility to the information they access.
    iii. The nature of the work to be performed at the remote site.
        1. If the work involves any sensitive information, in addition to managing physical visibility on the computer screen, the eligible staff must first connect to a VPN or otherwise ensure a secure connection to Microsoft 365 to ensure that sensitive data cannot be accessed by unauthorized parties.
        2. If the work is to be completed on a public network such as Internet access provided by restaurant or hotel, the eligible staff must first connect to the

VPN before accessing any Region 10 PIHP IT resource, including Microsoft 365.

3. If the work involves regular access to protected healthcare information (PHI), it may require special approvals and considerations so that it is not unsecured PHI.
    a. Local storage on the client endpoint technology (e.g. personal computer, laptop, tablet, etc.) used for telecommuting must be encrypted.
    b. VPN access is required.
4. If there are limitations on the type of work that is to be performed remotely, those must be spelled out in the approval.

iv. The client endpoint technology used for telecommuting must be owned and provided by Region 10 PIHP. Exceptions to this policy are only allowable with the approval of the CEO, COO or CIO.

E. Provided there are no barriers to telecommuting, the appropriate written approval by the CIO (or by those to whom they have delegated approval authority) shall be considered. If granted, the approval will be provided in writing via email or hardcopy memorandum.
F. CIO/Supervisor will ensure remote equipment are available to the telecommuting user.
G. If at any point the telecommuting arrangement ceases, any unneeded PIHP-provided equipment shall be returned to Region 10 PIHP, and unneeded remote user logins are to be disabled.
H. Eligible staff are expected to comply with all Region 10 PIHP policies and procedures while telecommuting. Eligible staff accept the consent to monitoring as implied in their use of telecommuting.

V. EXHIBITS:

None

VI. REFERENCES:

None