Region 10 PIHP

Date Issued: 10/13
Date Revised and/or Reviewed: 11/18, 4/19

Page 1

SUBJECT		CHAPTER	SECTION	SUBJECT
Information Systems Security & Protection		03	01	05
CHAPTER Information Management	**SECTION** Technology			
WRITTEN BY Kathy Tilley & Kelly VanWormer	**REVIEWED BY** Jason Radmacher & Pattie Hayes		**AUTHORIZED BY** PIHP Board	

I. APPLICATION:

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

II. POLICY STATEMENT:

It shall be the policy of the Region 10 PIHP to ensure that all data gathered and stored in a digital format, or information converted to a digital format for storage, indexing, retrieval, and eventual archival which reside on server platform(s) controlled by the PIHP shall be backed up at intervals no longer than once every business day. All data backups shall be performed on identified media and rotated off-site in accordance with the IT Disaster Recovery Plan. For personally used devices (e.g. PCs, mobile phones, tablets, laptops, etc.), Agency computer users will follow standard procedures to maintain the security and integrity of the information system.

III. DEFINITIONS:

Agency: PIHP, CMH/Administrative Staff, CMH Providers/Sub-contractors & SUD Providers, Contractual Staff, Students, Volunteers.

Authorized Access: A security measure using a separate user identification (login) and password for each personnel which allows entry into programs and files necessary for the performance of assigned duties within the organization.

Cloud: Data storage and resources accessible through the Internet.

Computer Acceptable Use Agreement (CAUA): A document signed by any personnel who has access to the Information System which certifies that the personnel will keep their password secret, keep information confidential, and utilize Information System resources in accordance with all applicable policies and procedures.

Data: The complete set of information stored within the Information System or contained on disks, printouts, CDs or other media, regardless of current format.

Digital Format: Information stored electronically on magnetic, optical or digital media.

SUBJECT		CHAPTER	SECTION	SUBJECT
Information System Security		03	01	05
CHAPTER	**SECTION**			
Information Management	Technology			

Electronic Protected Healthcare Information (ePHI): Any individually identifiable health information stored on hard drives, laptops, and memory sticks; contained in e-mail; or transmitted from or to the PIHP.

EHR (Electronic Health Record): A systematic collection of patient electronic health information generated by one or more encounters in any care delivery setting and including various health-related, demographic and service information.

Information System: The network of computers and other hardware and software used to categorize, store, retrieve, copy, protect, and manipulate data on behalf of the Agency and its clinical and administrative operations.

Managed Care Information System: A data system which is centralized and shared by many users (in this case the CMHs and SUD Providers) and used for data transactions, reporting and data analysis.

Multi-factor Authentication: User access to systems that employs a combination security approaches, most commonly a username, a password, and additional security measures (e.g. pass codes, tokens, IP addresses, etc.)

Password: The individual alphanumeric code used by each personnel to access an Information System.

Restricted Access: A security measure used to limit the number of personnel who can gain entry for the purpose of reading or writing to data files. Access is allowed on a need-to-know basis and is controlled, in part, through the use of individual user passwords.

Security: The protection of data systems by consistent adherence to policies, procedures and processes that combine physical, electronic, hardware and software security measures to protect Information Systems and their contents from fraud, computer viruses, power failure, sabotage, destruction, and unauthorized access or alteration. Includes alarms, monitoring, firewalls, and restricted physical access by means of locked rooms and limited distribution of keys and access cards, which limits physical access to the main computer system, to other computer equipment and to data from the Information System and which otherwise protects the system from damage.

Security Measures: In addition to those noted above, mechanisms and processes established to maintain the integrity of the system and its contents such as back-up tapes, offsite storage of back-up tapes, secondary power sources, physical security of equipment, virus detection and protection software, data redundancy configuration, training, password security agreements, etc.

User: Individual who has access to an Information System as personnel, contractor, temporary employee, client, or other person who uses Agency computers.

SUBJECT	CHAPTER	SECTION	SUBJECT
Information System Security	03	01	05
CHAPTER	**SECTION**		
Information Management	Technology		

IV. STANDARDS:

CMH/SUD Providers/Sub-contractors must have policies and procedures regarding the following standards.

A. PIHP must require passwords to be used to restrict access to Information Systems.

B. Systems will be set up in such a way that each user who receives access does so by entering their user ID and personal password. The CIO and technical staff must ensure that operational guidelines exist to ensure that excessively simple passwords cannot be used, and to ensure that passwords be regularly changed. These guidelines will balance the risk from changing passwords frequently with the risks from changing passwords infrequently. In addition, where multi-factor authentication is available as an additional measure for agency systems, it shall be utilized.

C. PIHP strictly prohibits users from sharing their password(s) with any other individuals, including administrative or technical personnel, and to report any suspected password breach.

D. PIHP requires all computer users to read and sign a Computer Acceptable Use Agreement (CAUA), indicating understanding and willingness to abide by its terms and conditions. The user's supervisor must request access in keeping with the individual's roles and responsibilities. A responsible administrator must sign the CAUA prior to granting requested access.

E. PIHP requires notification to technical staff of employee, vendor or subcontractor termination, voluntary or involuntary, and the process for termination of that user's access to PIHP Information Systems. Providers will notify the PIHP immediately of any staff with MIX access who either leave the program or no longer need access to MIX so that his/her screen name and password can be deactivated, per HIPAA security standards.

F. PIHP provides education of all users in awareness of restrictions related to confidentiality and privacy of consumers and protection of consumer information from unauthorized use, access, revision, duplication, deletion or dissemination.

G. PIHP must ensure the security of computer servers which house Agency shared data systems, including that they must be stored in a secure location, must have proper hardware and software maintenance of these servers to ensure their ongoing accessibility and security, and a daily backup must be made and stored securely using industry standard methods.

H. PIHP must require Information Systems, including operating systems, the managed care information system (MIX), and any electronic health records (EHRs), to automatically terminate (e.g., log the user off and/or close the application) after a period of inactivity.

I. PIHP must require Agency computers to be protected from viruses and similar destructive programs.

J. PIHP must ensure that no individuals can install programs which can be used to obstruct or disrupt the use of any computing system or network. Users shall not by any means attempt to infiltrate (e.g., gain access without proper authorization) a computing system or network.

K. PIHP must require the Agency's technical staff to continuously review ways that unauthorized access might be gained to Agency networks and computers and implement methods as necessary to thwart that access.

L. All PIHP and Agency server resources (whether "on premise" or hosted in the cloud) are to be backed-up to mitigate the potential loss of data. Backups shall be monitored regularly to ensure proper operation through periodic restoration of test files (no less than twice annually).

M. If PIHP or Agency server backups have been found to not be successful, an immediate solution will be sought to rectify regular backups, and notification provided by technical staff to the Region 10 PIHP CIO. An interim backup may be executed during business hours to ensure the protection of data, even if it deteriorates network or server performance.

N. To ensure protection of data outside of the primary data center, backups will be stored in an off-site location at least 2 miles away from the primary data center (either physically stored in an off-site fire-resistant safe or in a secure location hosted in the cloud).

V. PROCEDURES: N/A

VI. EXHIBITS: N/A