SUBJECT HIPAA Privacy & Security Measures		**CHAPTER** 03	**SECTION** 03	**SUBJECT** 01
CHAPTER Information Management	**SECTION** Health Records			
WRITTEN BY Kathy Tilley & Kelly VanWormer	**REVIEWED BY**		**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 that the PIHP, CMH and CMH subcontractors, SUD providers preserve the integrity and the confidentiality of health care information and meet the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards.

III. DEFINITIONS:

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. The breach must not only constitute a violation of the HIPAA Privacy Rule, but must also pose a significant risk of financial, reputational, or other harm to the individual. Exceptions to the term 'breach' are listed in Title XIII of Division A, Subtitle D, section 14300 of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5).

Business Associate: An individual, group or agency with whom the PIHP has a relationship and the Business Associate role is that of a non-covered entity and protected health information is shared as part of doing business.

Covered Entity: Shall refer to the Region 10 PIHP.

Health Information: Any information, whether oral or recorded in any format or medium that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual in 45 CFR §160.103.

Integrity of Data: A condition that data which is compiled, utilized, and analyzed that is believed to be accurate and valid and is a result of processes employed to protect the accuracy, security, comprehensiveness and standardization of the data and electronic information.

SUBJECT		CHAPTER	SECTION	SUBJECT
HIPAA Privacy & Security Measures		03	03	01
CHAPTER	**SECTION**			
Information Management	Health Records			

Protected Health Information: Individually identifiable health information: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. For PHI exclusions see 45 CFR §160.103.

Unsecured Protected Health Information: If information is rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods identified per the technologies and methodologies in the HITECH Act, then such information is not unsecured.

IV. STANDARDS:

A. Region 10 PIHP and any subcontractors protects the confidentiality of individuals' information to the highest degree possible so that individuals are not concerned with providing information for purposes of treatment.

B. Region 10 PIHP officers and employees will not use or supply individual or employee confidential or privileged information for non-health care uses, such as direct marketing, employment, or credit evaluation purposes without the appropriate consent.

C. Protected information will only be used to provide proper diagnosis and treatment; with the individual's knowledge to receive reimbursement for services provided; for research and similar purposes designed to improve the quality and to reduce the cost of health care; and as a basis for required reporting of health information.

D. Individuals' information collected must be accurate, timely, complete, and available when needed.

E. All staff will store individuals' information in a secure fashion; log off of workstations when not in use; secure material away when not being worked on; secure interoffice mail in confidential envelopes; put away individual information when left temporarily; will not leave client information unattended and will not routinely fax any identifiable individual information. In accordance with the HIPAA Security guideline 45 CFR § 164.530(c), 45 CFR § 164.306, staff must verify that that the individual, clinician, or employee has submitted a request to release protected health information to another party. The HIPAA Privacy Rule does permit physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by secure fax or other means. Covered entities must have in place reasonable and appropriate administrative, technical and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact correct for the receiver's location, and placing the fax machine in a secure location to prevent unauthorized access to the information.

SUBJECT		CHAPTER	SECTION	SUBJECT
HIPAA Privacy & Security Measures		03	03	01
CHAPTER	**SECTION**			
Information Management	Health Records			

F. All staff must:

1. Treat all individual(s) record information as confidential in accordance with professional ethics, accreditation standards, and legal requirements.

2. Not divulge record information for purposes other than treatment, payment or operation of the agency, unless the individual (or his or her authorized representative) has properly consented to the release or the release is otherwise authorized by law.

3. Take appropriate steps to prevent unauthorized disclosures, such as specifying that the recipient may not further disclose the information without the individual's consent or as authorized by law.

4. Remove individual identifiers when appropriate, such as in statistical reporting and in medical research studies.

5. Not disclose financial or other individual's information except as necessary for billing or other authorized purposes as authorized by law and professional standards.

G. For PIHP staff, violation of this policy is grounds for disciplinary action, up to and including termination of employment in accordance with the PIHP's discipline policy.

H. All electronic transmissions of protected health care information must meet the security regulations of HIPAA and the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.

I. Region 10 PIHP, CMHs, subcontractors, and SUD providers designate specific staff as Privacy Officer and Security Officer.

V. PROCEDURES:

Staff

1. Provides individuals receiving services with Privacy Notice.

2. Collects and uses individual information only for the purposes of providing Mental Health, Substance Use Disorder, or Co-Occurring Disorder services and for supporting the delivery, payment, integrity, and quality of those services.

3. Uses their best efforts to ensure the accuracy, timeliness, and completeness of data and ensure that authorized personnel can access the data when needed.

4. Completes and authenticates records in accordance with the law, ethics, and accreditation standards.

SUBJECT HIPAA Privacy & Security Measures		**CHAPTER** 03	**SECTION** 03	**SUBJECT** 01
CHAPTER Information Management	**SECTION** Health Records			

5. Maintains records for retention periods required by law, professional standards, and according to policy.

6. Does not alter nor destroy an entry in a record, but rather designates it as an error while leaving the original entry intact and creates and maintains a new entry showing the correct data.

7. Permits individual(s) access to their records, within 60 days of the request, except when access would be detrimental to the individual under therapeutic exception in the Mental Health Code.

8. Provides an individual receiving service an opportunity to request correction of inaccurate data in their records in accordance with the law.

9. Reports all improper disclosures of protected health care information to the respective Privacy Officer.

10. Ensures that faxing of protected personal health information is done in accordance with the HIPAA guidelines as noted in the Standards section within this policy, and the requirements of the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.

VI. EXHIBITS: N/A