Issue Date: 10/2013

Review and/or Revision Date: 11/2018, 03/2020, 3/2022, 3/2023

SUBJECT	CHAPTER	SECTION	SUBJECT
HIPAA Privacy & Security Measures	03	03	01

CHAPTER	SECTION
Information Management	Health Records

WRITTEN BY	REVIEWED BY	AUTHORIZED BY
Kathy Tilley & Kelly VanWormer	Ashley Piper	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, and its Provider Network, to employ safeguards to ensure the privacy and security of individuals; protected health information (PHI) as well as to preserve the integrity and the confidentiality of health care information to meet the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards, with revisions from the Health information Technology for Economic and Clinical Health Act of 2009 (HITECH), and handle SUD information as required of 42 CFR Part 2.

III. DEFINITIONS:

Breach: The acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the protected health information (45 CFR § 164.402).

Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity (HHS.gov).

Covered Entity: a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by subchapter 45 CFR §160.103. A covered entity may be a business associate. Region 10 PIHP is a covered entity.

Health Information: Any information, including genetic information, whether oral or recorded in any form 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(45

CFR §160.103).

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner (45 CFR § 164.304).

Protected Health Information (PHI): Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years. (45 CFR §160.103).

Provider: Community Mental Health Service Providers (CMHSPs), Substance Use Disorder (SUD) Providers, or any CMHSP subcontracted providers / practitioners.

Unsecured Protected Health Information: Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. (45 CFR § 164.402).

IV. STANDARDS:

A. The PIHP and its provider network protect the confidentiality of individuals' information to the highest degree possible so that individuals are reasonably assured of safeguards for their personal and treatment information.
B. The PIHP will maintain confidentiality, security, and integrity of the beneficiary information that is used in connection with the performance of this Contract to the extent and under the conditions specified in HIPAA, the Michigan Mental Health Code (PA 258 of 1974, as amended), the Michigan Public Health Code (PA 368 of 1978 as amended), and 42 CFR Part 2.
C. The PIHP complies with HIPAA's Privacy Rule, Security Rule, Transaction and Code Set Rule and Breach Notification Rule and 42 CFR Part 2 (as now existing and as may be later amended) with respect to all Protected Health Information and substance use disorder treatment information that it generates, receives, maintains, uses, discloses, or transmits in the performance of its functions.
D. The PIHP will use and disclose medical records and any other health and enrollment information that identifies a particular enrollee in accordance with the privacy requirements in 45 CFR parts 160 and 164, subparts A and E, to the extent that these requirements are

applicable.

E. All staff must ensure confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

a. All staff will not use or supply individual confidential or privileged information for non-health care uses without the appropriate consent.

b. PHI will only be used for the following:

1. to provide proper diagnosis and treatment; with the individual's knowledge and consent; to receive reimbursement for services provided;
2. for research and similar purposes designed to improve the quality and to reduce the cost of health care; and
3. as a basis for required reporting of health information.

c. The PIHP Board and its officers, employees, agents, and providers will not use or supply protected health care information of persons served for non-health care uses, such as direct marketing, employment, or credit evaluation purposes without his/her written authorization.

d. Implementation of technical safeguards to ensure which personnel positions can access which types of protected health information. When technical safeguards are impossible or impractical to establish, staff will be responsible for accessing only the minimum necessary protected health information required to do their job.

1. Minimum necessary does not apply to:
    - Disclosures to or requests by a health care provider for treatment.
    - Uses or disclosures made to the individual.
    - Uses or disclosures made pursuant to an authorization under 42 CFR §164.508.
    - Disclosures made to the Secretary regarding compliance and investigations under 45 CFR Part 160.
    - Uses or disclosures that are required by law.
    - Uses or disclosures that are required for compliance with applicable requirements of 45 CFR.

e. All staff will be trained in agency policies and procedures relevant to their job duties and protected health information.

f. A privacy notice is given to the individuals at the time of their Access Screening and annually.

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

h. All staff will store individuals' information in a secure fashion and ensure the following:

1. logging off / locking of workstations and data systems when not in use / away from desk;
2. secure material(s) away that contain PHI when not being worked on;
3. secure interoffice mail in confidential envelopes;
4. will not leave individuals' information unattended;
5. email PHI in a secure manner; and
6. will not fax any PHI, unless it is necessary.

i. In accordance with the HIPAA Security guideline 45 CFR § 164.530(c), 45 CFR § 164.306, staff must verify that the individual, clinician, or employee has submitted a request to release protected health information to another party. The HIPAA Privacy Rule does permit providers to disclose protected health information to another health care provider for treatment purposes. This can be done by secure email, zip folders attached to secure emails, or fax if necessary. The PIHP has reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed.

j. 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.

k. Region 10 PIHP, CMHSPs, subcontractors, and SUD providers shall designate a specific staff member as a Privacy Officer and a Security Officer.

l. All staff must:

1. Treat individua(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.

m. 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.

V. PROCEDURES:

All Staff:

A. PIHP provides each individual receiving service(s) with a Notice of Privacy Practices upon enrollment, annually, and when there is a material change and subsequently, the Notice of Privacy Practices document.
B. Collects and uses individual information only for the purpose of providing Mental Health, Substance Use Disorder, or Co-occurring Disorder services and for supporting the delivery, payment, integrity, and quality of those services.
C. Uses their best efforts to ensure the accuracy, timeliness, and completeness of data and ensure that authorized personnel can access the data when needed.
D. Completes and authenticates records in accordance with the law, ethics, and accreditation standards.
E. Maintains records for retention periods by law, professional standards, and according to policy.
F. Does not alter nor destroy an entry in a record, but rather indicates it as an error while leaving the original entry intact and creating / maintaining a new entry showing the correct data.
G. 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.
H. Provides an individual receiving service(s) an opportunity to request correction of inaccurate data in their record(s) in accordance with the law.
I. Reports all improper disclosures of protected health care information to the PIHP Compliance Office and / or the provider Compliance Office (See the following PIHP policies for additional information on reporting requirements: Corporate Compliance Program 01.02.01, and Corporate Compliance Complaint, Investigation, & Reporting Process 01.02.05).
J. Ensures that faxing of PHI, if necessary, 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.
K. Ensures protected health information will be stored in a secure fashion which includes:
    - logging off workstation when not in use,
    - locking workstations when away from desk,

- locking materials away when not being worked on,
- secure interoffice mail in confidential envelopes,
- not leaving individuals' information unattended,
- not faxing any identifiable personal information, unless it is an emergency, and
- not emailing identifiable protected health care information.

PIHP Staff:

A. Shall include *Secure:* in the subject line of an email that includes Consumer PHI. This will send a web page to your recipient(s) where they will be able to securely retrieve the message contents.
Note: be sure to include the colon after the word "secure". Also, the word "secure" is not case-sensitive and does not have to be at the beginning of the subject line.

VI. EXHIBITS:

None.

VII. REFERENCES:

American Recovery and Reinvestment Act of 2009 (ARRA)
Health Insurance Portability & Accessibility Act (HIPAA)
Health Information Technology for Economic and Clinical health Act of 2009 (HITECH)
42 CFR § 438.224
45 CFR § 160.103
45 CFR § 164.304
45 CFR § 164.306
45 CFR § 164.402
45 CFR § 164.530
MDHHS / PIHP Contract