SUBJECT Integrity of Electronic Data	**CHAPTER** 03	**SECTION** 01	**SUBJECT** 02
CHAPTER Information Management	**SECTION** Technology		
WRITTEN BY Kathy Tilley and Kelly VanWormer	**REVIEWED BY** Pattie Hayes	**AUTHORIZED BY** PIHP Board	

I. APPLICATION:

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

II. POLICY STATEMENT:

It shall be the policy of the Region 10 PIHP that the PIHP and all providers/sub-contractors will ensure that data in their Information System is accurate and entered into the Information System in a timely fashion, in order to promote the use of this data and appropriate information tools for decision making, operations, and third party reporting. The PIHP and Agencies must employ best practice procedures to ensure the safety and integrity of such data, and to continuously monitor and improve its quality.

III. DEFINITIONS:

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

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.

Integrity of Data: A condition in which the data compiled and manipulated by the Information System is believed to be valid and accurate as a result of processes employed by the agency to protect the accuracy, security, comprehensiveness, and standardization of the data.

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.

Protected Health Information (PHI): PHI, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), with revisions from the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), includes 18 identifiers that can be used to uniquely identify a person by their demographic information, health conditions, medical histories, assessment/laboratory/test results, services or insurance beneficiary information as 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. (See HIPAA Privacy Rules for more information).

Security: Methods used to protect the Information System and its contents from fraud, computer viruses, power failure, sabotage, destruction, and unauthorized access or alteration in compliance with Federal law and rules (e.g. HIPAA, HITECH, etc.), State law, and contractual obligations.

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

IV. STANDARDS:

A. All Agency policies and procedures regarding paper records and/or standards of conduct also apply to the data and files in the Information Systems, including response to the Freedom of Information Act, HIPAA Privacy & Security regulations, confidentiality policies, and any other applicable policies and procedures.

B. PIHP and Agency technical staff will establish proper authorities and permissions to ensure that access to and operations on data and files are consistent with individual job roles and responsibilities.

C. PIHP staff will make appropriate on-line documentation available to PIHP staff, CMH Administrative Staff, and CMH Providers/Sub-contractors and SUD Providers, that define processes and data elements of the PIHP Information System.

V. PROCEDURES:

INFORMATION MANAGEMENT SYSTEMS

The PIHP will maintain an information management system, including a managed care information system ("MIX") and other necessary databases and systems which shall be a subset of PIHP, CMH Administrative, CMH Providers/Sub-contractor & SUD Provider electronic data, particularly the data received from MDHHS and submitted to the PIHP by CMH providers and sub-contractors.

This data includes, but is not limited to, funding information, encounters, Performance Indicator data, Behavioral Health Treatment Episode Data Set (BH TEDS) for both BH and SUD clients, authorization, eligibility, and other data as required by MDHHS or needed by the PIHP for operation, data analysis and management.

A. The PIHP's information management system will include protection and security features to ensure confidentiality, data integrity and protection from intrusion, including risk mitigation and management procedures for a loss of confidential data or security breach to include notification of affected consumers.

B. The accuracy and timeliness of data submitted by CMH Administrative Staff, CMH Providers/Sub-contractors and SUD Providers will meet timelines established by the PIHP necessary to fulfill the requirements of the Michigan Department of Health and Human Services (MDHHS), and all other necessary payers, accrediting organizations, or regulatory entities.

C. PIHP management, assisted by the PIHP technical staff, will monitor the accuracy and timeliness of this data.

D. CMH/SUD Providers/Sub-contractors will have policies and procedures requiring that data shall be entered into the EHR as soon as practical.

E. CMH/SUD Providers/Sub-contractors will have policies and procedures requiring that only users authorized to enter, alter, or remove data, and trained in the appropriate standards and procedures, shall enter or alter data in their EHR/Information System.

F. CMH/SUD Providers/Sub-contractors must have policies and procedures requiring that demographic (BH TEDS) data submitted to the PIHP must be reviewed and updated at any known event which affects relevant information for the individual served, and at least quarterly. Third-party reimbursement data shall be reviewed and updated as often as necessary to ensure that the PIHP remains the payer of last resort. Specific responsibilities include:
   - Access and Crisis workers who register new or returning clients are responsible to capture and update, to the extent possible, all client demographic and eligibility information in the computer record, or to ensure that the information is entered into the correct computer record in a timely manner.
   - Primary Caseholders are responsible to review and ensure the accuracy and completeness of the client's demographics at least quarterly.

G. CMH/SUD Providers/Sub-contractors must have policies and procedures requiring that clinical documentation shall be signed in accordance with the PIHP’s documentation rules and must be reviewed for accuracy by management and billing personnel as needed.

VI. EXHIBITS: N/A