WHITING FORENSIC HOSPITAL
OPERATIONAL PROCEDURE MANUAL

SECTION II:	**ORGANIZATIONAL FOCUSED FUNCTIONS**
CHAPTER 9	**MANAGEMENT OF INFORMATION**
Governing Body Approval:	April 27, 2018
REVISED:	

VALUE - Whiting forensic hospital (WFH) uses Management of Information Systems (MIS) to aid in the planning and the monitoring of hospital and patient care functions vital to the mission of the Department of Mental Health and Addiction Services (DMHAS) and WFH. These systems record, measure and monitor the nature, effectiveness and economy of treatment and rehabilitation services provided, the use of least restrictive treatment for the shortest time, the resources used in providing care, and the integration of community agency services to help achieve those goals.

GOAL - WFH uses managed care methodology to provide patients with effective and economical services. Such methods require complete, accurate, timely and accessible data about patient needs and characteristics, treatment outcomes, staffing patterns, and operating expenses. These data are used by clinicians to assist in treatment and by management to monitor the degree to which services meet the stated goals and are cost effective. Specific goals for the WFH Information Management policies are:

1. Completeness – the information system contains data sufficient to answer relevant questions;

2. Accuracy – data is demonstrably accurate;

3. Timeliness – data is entered as close to the point of its collection as possible so that it is available for retrieval;

4. Accessibility – information is easily retrievable by authorized personnel. An

automated representation of manually kept data is considered where aggregate data retrieval is needed, and such retrieval is more widely available than data about individuals;

5. Integration – data from various sources are designed to be combined and compared by adequately trained Management of Information Systems (MIS) staff;

6. Standardization – uniform data definitions, data capture methods, minimum data sets, classifications and terminology are standardized; and

7. Privacy – protection of patients' rights to privacy regarding use and disclosures of Protected Health Information (PHI).

POLICY -

The WFH Governing Body or its designee(s) conducts needs analyses, monitors implementation, and performs evaluation of the performance of the information systems used to assist clinicians and administrators and to support program evaluation activities.

A. Current systems include:

1. a patient medical records system consisting of:

   a. a manually kept patient chart which is initiated and maintained for every patient and contains sufficient information to identify the patient, support the diagnosis, justify the treatment, document the course and results, and promote continuity of care among health care providers; and

   b. an automated clinical Behavioral Health Information System (BHIS) which stores selected identifying, demographic, clinical and cost information and is maintained by DMHAS/Information Systems Division (ISD) for all DMHAS facilities.

2. an incident reporting system which records and retrieves reported accidents, assaults, injuries, etc.;
3. a restraint and seclusion reporting system which records and retrieves information related to all reported events;
4. a treatment/activity system which records and retrieves prescribed and prescheduled treatment activities;
5. an automated pharmacy component;
6. an automated infection control component;
7. an automated employee health component;

8. a medical library which affords access to several knowledge databases and external databases which are used for bench marking;
9. fiscal information;
10. a human resource information system with both manual and automated components as well as access to external databases;
11. an automated staffing system for nursing;
12. an automated dietary system; and
13. a plant operations system.

B. Program Managers, Unit Directors, the Medical Staff, and professional discipline leaders are all demonstrably involved in needs assessment, implementation, and performance evaluation of the Hospital's information systems. Hospital leadership ensures confidentiality of patient identifying information, data reliability, relevance, accessibility, integration, and standardization in planning, implementation and performance evaluation.

C. Each system operates according to written standards and procedures for data collection, entry, integrity, storage, retrieval, and monitoring.

D. Technical support (hardware and software) for all automated systems is available onsite. Policy for software licensure and its oversight by technical staff is in place.

E. The following discipline leaders have primary responsibility for the proper functions of each system:

1. The Behavioral Health Services Manager and the Director of Accreditation, Compliance and Performance Improvement are responsible for the Management of the Automated Clinical Information Systems, the Data Processing Technical Support Staff, the Local Area Network (LAN), hardware and infrastructure and all software licensing at WFH. In addition, they act as liaison (MIS Coordinator) for WFH with the DMHAS Department of Information Technology.

2. The Medical Staff and the Director of Accreditation, Compliance and Performance Improvement are responsible for the Patient Medical Records System. Medical Records standards are described in the Health Information Management Policy and Procedure Manual, which contains operating and monitoring procedures for both the paper medical record and the automated components. Standards include:

   a. content, completeness, and timeliness requirements *(*See *HIM P&P Section 2, Policy 2)*;
   b. dated entries, author identified, and when necessary, authentication *(*See *HIM P&P Section 2, Policy 1)*;
   c. identification of staff authorized to make entries *(*See *Operational Procedure 9.1*

Authorization to Document in the Medical Record);

d. use of Physician Orders *(*See *HIM P&P, Section 2, Policy 11)*;

e. accessibility of all components of the medical record *(See HIM P&P, Section 4, Policy 1)*;

f. record retention guidelines *(*See *Operational Procedure 9.8 Records Retention Schedules for State Agencies)*;

g. the requirement of an up-to-date medical record for each individual admitted to the Hospital *(*See *HIM P&P Section 1, Policy1)*;

h. medical record audits, including a sampling of records from all programs, conducted on an ongoing basis, reported quarterly, designed to assure adherence to these standards and utilized to formulate actions taken to improve any deficiencies; and

i. procedures to guard against loss, destruction, tampering, and unauthorized access or use of medical records or information.

3. The Pharmacy Supervisor is responsible for the pharmacy system.

4. The Director of General Medical Services is responsible for the infection control and employee health systems.

5. The Behavioral Health Services Manager is responsible for all fiscal systems.

6. The WFH Director of Human Resources is responsible for all human resources systems.

7. The Behavioral Health Services Manager is responsible for the plant operations and dietary systems.

8. The Director of Accreditation, Compliance and Performance Improvement assumes the responsibility of the WFH Privacy Officer, ensuring that all policies and procedures related to the patient's privacy rights and use and disclosure of PHI are implemented.

10. The MIS Unit has the following responsibilities to:

a. coordinate automated systems and minimize duplication by keeping up-to-date descriptions of the purpose and structure of all information systems used to monitor patient care. The MIS coordinator is notified when current systems or their contents are modified or additional systems are planned, and provides consultation on their development;

b. encourage completeness, accuracy and timeliness, by working with other members of the MIS department and with DMHAS/ISD to provide feedback to Hospital leadership about automated data which is missing, late, or in error;

c. evaluate the degree to which the facility's information needs are met by the current systems and recommend modifications to the Governing Body;

d. develop procedures for the retrieval and distribution of information from automated systems which require a minimal level of computer literacy, but which insure against unauthorized access. The aim is to make both individual patient information and the aggregate data needed to support patient care and operations readily available while protecting confidentiality. Such information includes standardized periodic reports as well as ad hoc requests;

e. provide consultation, education, and training on methods of data retrieval, principles of information management, analysis methods, and use of statistics to decision makers as well as clinical staff;

f. assist Hospital leaders in the definition, collection, and analysis of comparative performance data in a manner consistent with national and state guidelines;

g. contribute to external reference databases; and

h. maintain security and confidentiality of data and information when contributing to or using external databases.

F. Committees which have responsibility for the Management of Information:

1. The Medical Records Committee, a standing committee of the Medical Staff, is responsible for the development and revision of medical record components, including Health Information Management Policies and Procedures. The Medical Records Committee makes its recommendations to the Medical Staff. *(Refer to the Medical Staff By-Laws for more information on the function and membership of the Medical Records Committee).*

2. The MIS Committee is responsible for implementing an automation plan for WFH which currently identifies both hardware and software needs associated with the development of efficient and integrated methods of storing, retrieving, and transmitting information throughout the facility. *(Refer to the Governing Body By-Laws for more information on the function and membership of the MIS Committee).*

G. The Health Insurance Portability and Accountability Act (HIPAA): Privacy Rule

1. Background and Purpose:

a. Patients enter treatment with the expectation that the information they share will be used and disclosed exclusively for their clinical care. To protect their privacy and avoid embarrassment, stigma, and discrimination, some patients withhold information from their health care providers, provide inaccurate information, doctor-shop, pay out-of-pocket for care that is covered by insurance, and in many cases, avoid care altogether. Today, more and more health care providers, health care plans, and others are utilizing electronic means of storing and transmitting health information. The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those records is often copied and transmitted through electronic means.

b. The provision of high quality health care requires the exchange of personal, often sensitive information between a patient and his/her health care provider. Many patients are concerned that their health information is not protected. Among the factors contributing to this concern are:

1. the growth and number of organizations involved in the provision of care and the processing of claims;

2. the increased use of electronic information technology;

3. increased efforts to market health care and other products to consumers; and,

4. the growing ability to collect highly sensitive information about a person's current and future health status.

c. The HIPAA privacy rule was designed to serve as a minimum level of privacy protection. It is intended to:

1. protect and enhance the rights of patients by providing access to their health information and controlling the inappropriate use of that information;

2. improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of individuals committed to the delivery of care; and

3. improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

d. HIPAA Information Privacy Protections are intended to:

1. give patient’s appropriate control over and access to their health information;

2. set boundaries on the use and release of health records;

3. safeguard that information;

4. establish accountability for inappropriate use and release; and

5. to balance privacy protections with public safety.

2. Patient Privacy Rights:

a. It is the policy of WFH that the HIPAA privacy requirements are integrated with those privacy practices which were already in place at WFH prior to HIPAA. WFH maintains and supports that privacy is a fundamental patient right.

b. WFH shall ensure that the following patients’ privacy rights are implemented:

1. to receive a notice of WFH privacy practices;

2. to access their medical record in order to inspect and/or copy it;

3. to request an amendment of their material record;

4. to receive an accounting of disclosures of protected health information; and

5. receive confidential communications.

c. WFH shall ensure that all PHI is safeguarded. This includes PHI found within the medical record and other records and documents maintained by WFH which contain identifiable patient information. Examples are those found in the Behavior Health Information System (BHIS) and eCura as well as any electronic file such as a Word document, Excel spreadsheet or an Access database.

*(*See *Operational Procedures 9.14 through 9.28 for specific HIPAA Policies and Procedures)*

3. Use and Disclosure:

    a. It is the policy of WFH to review how information is used and disclosed and to make an effort to limit all uses and disclosures to the minimum necessary in order to accomplish the intended purpose.

    b. WFH has established procedures for the use and disclosure of Protected Health Information in accordance with the privacy rule including the following mandated requirements:

        1. to obtain written authorization from all patients prior to using their PHI except in limited prescribed situations;

        2. to provide all patients with an understanding of how their PHI is being used by WFH in the Notice of Privacy Practices in a language they can understand*;*

        3. to default to the more restrictive authorization and/or other written legal permission, when there is a conflict, in order to better protect a patient's PHI;

        4. to verify the identity and authorization of all individuals who request a disclosure of PHI;

        5. to provide an opportunity for patients to request that restrictions be placed on access to their PHI;

        6. to fully comply with all uses and disclosures required by law but do not require patient authorization;

        7. to limit the disclosure of all requests for PHI to the minimum amount reasonably necessary to accomplish the purpose for which the request was made;

        8. to promote the involvement of patients' personal representatives in their care and notification;

        9. to ensure full compliance with laws and regulations when PHI is used or disclosed for research purposes;

10. to de-identify, whenever possible, all PHI prior to its release;

11. to provide limited data sets for research or health care operations when de-identification is not practical; and

12. to obtain satisfactory assurance that all Business Associates will appropriately safeguard the PHI they create or receive from WFH.

*(*See *Operational Procedures 9.19 through 9.28 for specific HIPAA Policies and Procedures)*

Portions of this Policy were excerpted from the Electronic Comprehensive Accreditation Manual for Hospitals,

2003 and the Electronic Comprehensive Accreditation Manual for Behavioral Health Care 2002.