



# MONTANA STATE HOSPITAL POLICY AND PROCEDURE

## MEDICAL RECORDS ACCESS AND SECURITY

**Effective Date:** June 3, 2014

**Policy #:** HI-07

**Page 1 of 4**

- I. PURPOSE:** To insure that all Protected Health Information (PHI) necessary to assist in patient care will be provided to the appropriate health care professional and to safeguard records or PHI against unauthorized access.
- II. POLICY:** To ensure confidentiality and security, access to patient medical records at Montana State Hospital (MSH) is limited to authorized staff. Authorized staff includes all clinical staff (medical, psychiatric, psychology, social work, rehabilitation, nursing and Dietitian) and clinical consultants. Students, interns, and researchers may have access to medical records after obtaining permission from appropriate clinical service director.
- III. DEFINITIONS:** For the purposes of this policy, the following definitions apply:
  - A. Protected Health Information (PHI) – means Individually Identifiable Health Information that is transmitted electronically in any medium or maintained in any medium.
  - B. Individually Identifiable Health Information (IIHI) – is a subset of Health Information (HI) including demographic information, collected from an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse that:
    1. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual;
    2. Identifies the individual; or
    3. There is a reasonable basis to believe the information can be used to identify the individual.
  - C. Health Information – any information, whether oral or recorded in any form or medium, that is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of health care to an individual.

**IV. RESPONSIBILITIES:**

A. Health Information:

1. Maintain PHI in accordance with accepted professional standards and practices.
2. Track records signed out and returned to the Health Information Department.
3. Lock area when unattended.
4. Maintain emergency access to the Health Information Department after hours.

B. Clinical staff:

1. Accept responsibility to protect the confidentiality of the PHI.
2. Assumes responsibility for returning records in good condition and at the designated time.
3. Do not lock charts in their office overnight.

**V. PROCEDURE:**

A. Access to Health Information Department.

1. Health Information Department will be locked whenever it is unattended. The Health Information Department is open from 7:30 AM to 4:30 PM Monday through Friday.
2. The following hospital staff have keys to the Health Information Department:
  - a. All Health Information Staff including Front Desk Hospital Operation Specialists,
  - b. House Supervisor's key ring,
  - c. Security Officers,
  - d. Maintenance Supervisor.
3. Hospital Operations Specialists have access to the Health Information Department on weekends to perform various Health Information duties.

B. Emergency Access to the Health Information Department.

1. The House Nursing Supervisor, Hospital Operation Specialists and Security may access the patient record area for the purpose of retrieving a medical record for authorized staff particularly for an after-hours admission.
  2. Other staff will not enter the Health Information Department after-hours.
- C. Access to records in the Health Information Department.
1. Patient records will be routed to the Health Information Department within 72 hours following discharge.
  2. Patient records will not be removed from the hospital unless by court order, subpoena or statute.
  3. All charts removed from the area must be logged out.
  4. Authorized staff may be limited to viewing records in the Health Information Department should they consistently demonstrate a lack of responsibility for returning records within the designated timeframe.
- D. Security of PHI held in electronic medium (includes discs, tapes, computers, portable drives, etc.)
1. Staff are assigned a client user ID number upon completion of reviewing and signing a confidentiality statement.
  2. Staff are assigned data access rights according to needs of their position.
  3. When an employee leaves MSH, their computer access must be immediately terminated and their password discontinued. Interim access to critical information is the responsibility of the supervisor.
  4. Staff is responsible for his/her own use and disclosure of PHI.
  5. Staff may not share passwords or computer access. (See DPHHS Information Security and Database Access Policy)
  6. Log-off screen must be used to assure no unauthorized access to computers with PHI. A screen saver set to activate within five to fifteen minutes, locking the workstation manually, or a complete computer log-off can be used.
  7. Each employee must ensure that IIIHI on computer screens is not visible to unauthorized persons. This can be accomplished through the use of polarized screen covers, placement of computers out of the visual range of persons other than the authorized user, clearing information from the screen when not actually

