



MONTANA STATE HOSPITAL POLICY AND PROCEDURE

MEDICAL RECORDS ACCESS AND SECURITY

Effective Date: May 6, 2019

Policy: HI-07

Page 1 of 4

- I. PURPOSE:** To insure 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 the clinical service director.
- III. DEFINITIONS:** For the purposes of this policy, the following definition applies.
 - A. Protected Health Information (PHI): Individually Identifiable Health Information which is transmitted electronically in any medium or maintained in any medium.
- 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. Access limited to authorized personnel. Entrances will be locked at all times.
 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. The Health Information Department will be locked at all times with access granted to authorized personnel. The Health Information Department hours are 7:30 AM to 4:30 PM Monday through Friday. The Hospital Operations Specialists have access to the Health Information Department after hours and on weekends to perform various Health Information duties.
2. The following hospital staff have keys to the Health Information Department:
 - a. All Health Information Staff including the Front Desk Hospital Operation Specialists,
 - b. House Supervisor,
 - c. Security Officers, and
 - d. Maintenance Supervisor.

B. Emergency Access to the Health Information Department.

1. The House Nursing Supervisors, Hospital Operation Specialists and Security Officers 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 Medical Records Department 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. Each employee is responsible for his/her own uses and disclosures of PHI.
2. Employees must sign confidentiality statements before obtaining access to PHI. Staff are assigned data access rights according to the needs of their position.
3. Log-off screen must be used to assure no unauthorized access to computers with PHI. A screen saver set to activate within five minutes, locking the workstation manually, or a complete computer log-off can be used.
4. Employees may not share passwords or computer access. (See DPHHS Information Security Policy and Department of Administration State Information Technology Services Division POL-Information Security Policy – Appendix A, B, C, D).
5. Each employee must ensure that PHI 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 being used, or minimizing all applications when away from the workspace or when approached by an unauthorized person.
6. E-mail messages containing PHI are not available as public information.
7. MSH employees will utilize SharePoint accounts or ePass Montana File Transfer service to transmit any electronic PHI. E-mail messages containing PHI sent outside the state's e-mail system must either be encrypted, or the PHI must be contained in a password-protected attachment. The password should be provided to the intended recipient via separate contact.
8. When an employee leaves DPHHS, their computer access must be immediately terminated, and their password discontinued. Interim access to critical information is the responsibility of the supervisor.

VI. REFERENCES: M.C.A § 53-21-166; Department of Administration State Information Technology Services Division POL-Information Security Policy – Appendix A, B, C, D; DPHHS Privacy of Protected Health Information 001; DPHHS Physical Security for Protected Health Information 013.

VII. COLLABORATED WITH: Hospital Administrator and Director of Health Information.

VIII. RESCISSIONS: HI-07, *Medical Records Access* dated June 3, 2014; HI-07, *Medical Records Access and Security* dated November 2, 2009; HI-07, *Medical Records Access*

and Security dated October 30, 2006; HI-07, *Medical Records Access and Security* dated September 1, 2002; HI-07, *Medical Records Access and Security* dated February 14, 2000; HOPP HI-06-96-R, *Medical Records, Access and Security* dated November 15, 1996.

- IX. DISTRIBUTION:** All hospital policy manuals.
- X. ANNUAL REVIEW AND AUTHORIZATION:** This policy is subject to annual review and authorization for use by either the Administrator or the Medical Director with written documentation of the review per ARM § 37-106-330.
- XI. FOLLOW-UP RESPONSIBILITY:** Director of Health Information.
- XII. ATTACHMENTS:** None.

Signatures:

Kyle Fouts
Interim Hospital Administrator

Melinda Bridgewater
Director of Health Information