


Department: Health Information Management (HIM)
Policy Number: HHS-4118-HIM **Attachments:** _____
Policy Title: Logging of Activity in the RPMS Electronic Health Record (EHR)
Date: 12/12 **Revised:** _____
Approved by:  **Date:** 3/13/13

Policy Statement:

The Mille Lacs Band Health Services recognizes the importance of establishing policy, procedures and responsibilities concerning the logging of activity in the RPMS EHR.

POLICY:

Facilities within the MLBHS need to ensure that those individuals entering information into the RPMS EHR are aware that system audit trail functionality is monitored and audited according to facility policy and procedures, allowing them to legally access, amend, retract, correct, or edit entries. Entries into the RPMS EHR should be made at or near the time the care and treatment was provided to the patient to ensure the accuracy, timeliness, completeness, and integrity of data.

An audit trail is a business record of all transactions and activities, including access, associated with the EHR. Monitoring audit trails in the system will ensure that users can be held accountable for following the Indian Health Service (IHS) policies and procedures and federal privacy and security regulations.

RESPONSIBILITY: Assign Responsibility for Auditing of Log Entries and Reported Exceptions:

1. Leadership and management are ultimately responsible for securing privacy, confidentiality, security, and integrity of the RPMS EHR audit process. This includes the policies and procedures which assign and outline responsibilities to professional and ancillary leadership staff to determine system security and usability as well as report any inefficiencies or discrepancies potentially resulting in fraudulent entries into the EHR.
2. Leadership and management should always adhere to legal and federal regulatory standards and follow ethical business principles when auditing the system for integrity and trustworthiness of the data.

Note: The HIPAA Title II Security Rule CFR Part 136.316 (b) (1) (taken from the February 20th, 2003 Federal Register, page 8368) mandates audit trails be maintained within the EHR. Internal audit processes must be in place and regular system activity reviews must be completed for logins and accessing files. Security incidents must be monitored and resolved.

PROCEDURE:

For a random sampling of visits to use for auditing in RPMS:

1 Random Sample of Visits by DX and Date [APCL P QA AZQ2AUD] (AUD)

The RPMS EHR system's auditing function has limited capabilities. The Sensitive Patient Tracking (SPT) module of the Patient Information Management System (PIMS) package is utilized to generate an Access audit report.

There are several IHS Handbooks that lay out Standard Operating Procedures (SOP) for Information System Privacy and Security. It is imperative that Health Information Management (HIM) professionals work closely with Information System Security personnel in developing and carrying out a comprehensive privacy, confidentiality, and security audit plan based on facility areas of risk.

- User Login/Logout
- Chart Created/Viewed/Updated/Deleted
- System Security Administration
- System Start/Stop
- Scheduling Activities
- Query Functionality
- Order Entry
- Node-Authentication Failure
- Signature Authentication/Validation
- Protected Health Information (PHI) Import, (e.g., From External Information Source and System Administration)

The SPT records the following information:

- Date and time of the access
- The RPMS application the user accessed
- Patient Name and Health Record Number
- The SPT User Manual can be referenced for further reporting capabilities at www.ihs.gov.

SPT access should be limited to those with a need to know, such as Compliance Officers, Privacy Officers, Security Officers, and HIM managers. *See* Health Insurance Portability and Accountability Act (HIPAA) Policy and Procedure IHM Exhibit 2-7-K "Limiting the Use or Disclosure of and Requests for Protected Health Information to the Minimum Necessary".

Retention Periods and Procedures for Log Records:

- The system should generate a backup copy of the application data, security credentials, and log/audit files.
- The system restore functionality should result in a fully operational and secure state. This state should include the restoration of the application data, security credentials, and log/audit files to their previous state.

- The audit report must include a copy of the output of the audit as well as the steps taken to produce the report.
- Retention of audit logs is based on state and/or federal laws, whichever applies to the facility.

ATTACHMENTS: Sensitive Patient Tracking User Manual

REFERENCES:

RECISSION:

DISTRIBUTION: All Staff