Pondera Medical Center
Administrative Policy/Procedure

Policy Number: **84.03.2017.OP.88**

TITLE: **Electronic Health Records (EHR) Audit Policy**

AREAS AFFECTED: **All Areas**

PURPOSE: Pondera Medical Center (PMC) shall audit access and activity of electronic protected health information (ePHI) applications and systems in order to ensure compliance. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system, and/or network auditing capabilities and resources. PMC shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

POLICY:
Information Security Management Program Access, Control Policy, Audit Logging, Protection of Log Information, Monitoring System Use and Prevention of Misuse of Information.

Applicable Standards from the HIPAA Security Rule:

- 45 CFR §164.308(a)(1)(ii)(D) - Information System Activity Review
- 45 CFR §164.308(a)(5)(ii)(B) & (C) - Protection from Malicious Software & Log-in Monitoring
- 45 CFR §164.308(a)(2) - HIPAA Security Rule Periodic Evaluation
- 45 CFR §164.312(b) - Audit Controls
- 45 CFR §164.312(c)(2) - Mechanism to Authenticate ePHI
- 45 CFR §164.312(e)(2)(i) - Integrity Controls

Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to PMC's IT Director. The IT Director shall:
    - Assign the task of generating reports for audit activities.
    - Assign the task of reviewing the audit reports to the appropriate department manager.
    - Organize and provide oversight to a team structure charged with audit compliance activities (Compliance Meetings held monthly).
    - All connections to PMC are monitored. Access is limited to certain services, ports, and destinations.
2. PMC's auditing processes shall address access and activity at the levels listed below.
    - **User:** User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
    - **Application:** Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
    - **Network:** Network level audit trails generally monitor information regarding what is operating, penetrations, and vulnerabilities.
3. PMC shall log all incoming and outgoing traffic in its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and other relevant details that are available to PMC.
4. PMC's IT Director and Privacy Officer are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others. These tools may include, but are not limited to:
    - Scanning tools and devices;
    - Password cracking utilities;
    - Network "sniffers."
    - Passive and active intrusion detection systems.

The process for review of audit logs, trails, and reports shall include:

- Description of the activity as well as rationale for performing the audit.
- Identification of which PMC workforce members will be responsible for review.
- Determination of significant events requiring further review and follow-up.
- Identification of appropriate reporting channels for audit results and required follow-up.

5. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.
   - Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
   - Testing shall be done on a routine basis.
6. Software patches and updates will be applied to all systems in a timely manner.

Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, IT Director, or department manager. A request for an audit for specific cause must include time frame, frequency, and nature of the request.
2. A request for an audit must be approved by PMC's Privacy Officer and/or IT Director before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.
   - Should the audit disclose that a workforce member has accessed ePHI inappropriately; the minimum necessary/least privileged information shall be shared to determine appropriate sanction/corrective disciplinary action.

Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner.
2. Relevant audit log findings are added to the Issue; these findings are investigated in a later step. Once those steps are completed, the Issue is then reviewed again.
3. Once the review is completed, Compliance committee approves or rejects the Issue. Relevant findings are reviewed at this stage. If the Issue is rejected, it goes back for further review and documentation. The communications protocol around specific findings are outlined below.
4. If the Issue is approved, the Compliance committee then marks the Issue as Done, adding any pertinent notes required.
5. The reporting process shall allow for meaningful communication of the audit findings to those workforce members.
   - Significant findings shall be reported immediately in a written format.
   - Routine findings shall be reported through the Compliance meeting in a written report format.
6. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
7. Security audits constitute an internal, confidential monitoring practice that may be included in PMC's performance improvement activities and reporting.
8. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible manager.

Auditing Partner Activity

1. Periodic monitoring of Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between PMC and any 3rd party. PMC will make every effort to assure partners do not gain access to data outside of their own Environments.
2. If it is determined that a Partner has exceeded the scope of access privileges, PMC's leadership must remedy the problem immediately.
3. If it is determined that a Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, PMC must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.
3. Audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.

Workforce Training, Education, Awareness and Responsibilities

1. PMC staff is provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. PMC's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. PMC staff members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detects a workforce member's failure to comply with organizational policies.

External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, PMC shall:
    - Outline the audit responsibility, authority, and accountability;
    - Choose an audit firm that is independent of other organizational operations;
    - Ensure technical competence of the audit firm staff;
    - Require the audit firm's adherence to applicable codes of professional ethics;
    - Obtain a signed HIPAA business associate agreement;

Retention of Audit Data

1. Audit logs shall be maintained based on organizational needs. There is no standard or law addressing the retention of audit log/trail information. Retention of this information shall be based on:
    - Organizational history and experience.
    - Available storage space.
2. Reports summarizing audit activities shall be retained for a period of six years.

Date of Origin: 03/17
Date(s) of Revision: 07/17; 09/17
Date of Last Review: 04/18
Effective Date: 09/17

Contact Person(s): IT Director; HIPAA Privacy Officer; Compliance Officer; Chief Executive Officer

Executive Approval: 

Date of Board of Director's Review: 9/26/17