DEPARTMENT: Information Systems	**POLICY NUMBER: 002**
DISTRIBUTION: All Staff	**EFFECTIVE DATE: 1/22/2020**
SUBJECT: Audit Controls	**REVISION DATE:**

POLICY:

Equinox Inc. monitors system access and activity of workforce members.

PROCEDURE:

Person(s) Responsible:	Procedures:
Director of Information Systems IT Support Team	1. Log-In Monitoring. To ensure that access to servers, workstations, and other computer systems containing EPHI is appropriately secured, the following log-in monitoring measures shall be implemented: (a) A mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable. (b) To the extent that technology allows, a means to disable any User ID that has more than three (3) consecutive failed log-in attempts within a five (5) minute period. (c) A review of log-in activity reports and logs when required to identify any patterns of suspicious activity, where a complaint or investigation warrants such a review.
Director of Information Systems IT Support Team	2. Information System Activity Review. Information system activity reviews and audits may be conducted using third party software to: (a) Ensure integrity, confidentiality, and availability of information and resources. (b) Investigate possible security incidents to ensure compliance with Equinox Inc. security policies. (c) Monitor user or system activity as required.

	(d) Verify that software patching is maintained at the appropriate security level. (e) Verify virus protection is current.
Director of Information Systems IT Support Team	3. Information System Audit Controls. To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met: (a) Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. (b) Once every three (3) months, at a minimum, the Director of Information Systems or designated IT team members shall review audit logs, activity reports, or other mechanisms for indications of improper use. (c) Indications of improper use shall be reported to management for investigation and follow up. (d) Audit logs of access to networks and applications with EPHI shall be archived and protected from unauthorized access, modification, and deletion.