DEPARTMENT: Information Systems	**POLICY NUMBER: 008**
DISTRIBUTION: All Staff	**EFFECTIVE DATE:**
SUBJECT: Risk Analysis and Management	**REVISION DATE:**

POLICY:

Equinox Inc. shall perform risk analysis and management through periodic assessments and implementation of controls to mitigate risks.

PROCEDURE:

Person(s) Responsible:	Procedures:
Director of Information Systems	1. Risk Analysis. In order to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the EPHI held by Equinox Inc., the following activities shall be conducted and documented under the direction of the Director of Information Systems: (a) Periodic program assessments including a security review of facility access controls, protection of network server closets, workstations, portable devices, and document destruction capabilities. (b) Assessments of new or existing information system applications that contain, or are used to protect, EPHI. (c) Assessments of modifications to existing facilities or development of new facilities that maintain or house EPHI. (d) Assessments of new programs, departments or changes in the mode or manner of service delivery involving EPHI.
Director of Information Systems	2. Risk Management. Security measures and controls, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, shall be implemented: (a) Workforce security training and awareness reminders. (b) Access controls, authorization and validation procedures.

Person(s) Responsible:	Procedures:
	(c) Detection and activity reviews. (d) Applications and data criticality analysis. (e) IT systems change management. (f) Incident reporting and response procedures. (g) Sanctions for noncompliance. (h) Contingency, Data Backup and Disaster Recovery Planning.
Director of Information Systems	3. <u>IT Change Management</u>. The risk management process shall include change controls for all alterations that occur in the information systems that support, contain, or protect EPHI. These alterations include, but are not limited to: (a) Installation, update or removal of network services and components. (b) Operating systems upgrades. (c) Installation, update or removal of applications, software and database servers. (d) IT change management notification and implementation shall follow the policies and procedures as documented by IT support.