



<b>DEPARTMENT: Information Systems</b>	<b>POLICY NUMBER: 003</b>
<b>DISTRIBUTION: All Staff</b>	<b>EFFECTIVE DATE:</b>
<b>SUBJECT: Data Back-Up and Contingency Planning</b>	<b>REVISION DATE:</b>

**POLICY:**

Equinox Inc. shall have documented procedures for implementation in the event of an emergency, disaster or other occurrence (*i.e.*, fire, vandalism, system failure and natural disaster) when any system that contains EPHI is affected, including:

- (1) Applications and Data Criticality Analysis
- (2) Data Backup Plan
- (3) Disaster Recovery Plan
- (4) Emergency Mode Operation Plan

Each of the following plans shall be evaluated and periodically updated as business needs and technology requirements change.

**PROCEDURE:**

<b>Person(s) Responsible:</b>	<b>Procedures:</b>
Director of Information Systems	1. <u>Applications and Data Criticality Analysis</u> (a) Equinox Inc. will assess the relative criticality of applications and data within Equinox Inc. for purposes of maintaining a current Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan. (b) The assessment of data and application criticality will be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.
Director of Information Systems	2. <u>Data Backup Plan</u>

Person(s) Responsible:	Procedures:
	<ul style="list-style-type: none"> <li>(a) Equinox Inc. will establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all EPHI determined to be medium and high risk.</li> <li>(b) EPHI shall not be saved on the local (C:) drive of any workstation.</li> <li>(c) The Data Backup Plan must require that all media used for backing up EPHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.</li> <li>(d) If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the EPHI in an appropriate manner.</li> <li>(e) Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of EPHI can be retrieved and made available.</li> </ul>
Director of Information Systems	<p>3. <u>Disaster Recovery Plan</u></p> <ul style="list-style-type: none"> <li>(a) To ensure that Equinox Inc. can recover from the loss of data due to an emergency or disaster such as fire, vandalism, system failure, or natural disaster affecting systems containing EPHI, Equinox Inc. shall establish and implement a Disaster Recovery Plan for restoring or recovering loss of EPHI and the systems needed to make that EPHI available in a timely manner.</li> <li>(b) The Disaster Recovery Plan shall be documented and be available to the assigned personnel, who shall be trained to implement the Disaster Recovery Plan.</li> <li>(c) The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.</li> </ul>
Director of Information Systems	<p>4. <u>Emergency Mode Operation Plan.</u></p> <ul style="list-style-type: none"> <li>(a) Equinox Inc. shall document and implement procedures to enable continuation of critical business processes for the protection of EPHI while operating in emergency mode. Emergency mode operation must include processes to protect the security of EPHI during and immediately after a crisis.</li> <li>(b) Emergency mode operation procedures shall be tested periodically.</li> </ul>

