



DEPARTMENT: Information Systems	POLICY NUMBER: 009
DISTRIBUTION: All Staff	EFFECTIVE DATE:
SUBJECT: Security Incident Reporting and Response	REVISION DATE:

POLICY:

Equinox Inc. shall identify, document, and respond to unauthorized use of the systems that contain EPHI.

PROCEDURE:

Person(s) Responsible:	Procedures:
Workforce Members Director of Information Systems Managers and Supervisors	<p>1. <u>Incident Reporting</u></p> <p>(a) All security incidents, threats to, or violations of, the confidentiality, integrity or availability of EPHI shall be reported and responded to promptly.</p> <p>(b) Incidents that shall be reported include, but are not limited to:</p> <ul style="list-style-type: none"> (i) EPHI data loss due to disaster, failure, error or theft; (ii) Loss of any electronic media that contains EPHI; (iii) Loss of the integrity of EPHI; (iv) Virus, worm, or other malicious code attacks; (v) Persistent network or system intrusion attempts from a particular entity; (vi) Unauthorized access to EPHI on an EPHI based system or network; and (vii) Facility incidents, including but not limited to: <ul style="list-style-type: none"> (1) Unauthorized person found in a facility (2) Facility break-in (3) Lost or stolen key. <p>(c) Workforce members shall notify the Director of Information Systems of any suspected or confirmed security incident. The Director of Information Systems shall evaluate the situation to determine if it is a</p>

Person(s) Responsible:	Procedures:
	<p style="text-align: center;">potential security incident, and initiate the response process as required by the type of incident.</p> <p>(d) If a facility incident occurs, the Manager or Supervisor shall immediately report the incident to the Director of Information Systems.</p>
<p>Director of Information Systems</p> <p>Privacy Officer</p> <p>IT Team Members</p>	<p>2. <u>Incident Response and Resolution</u></p> <p>(a) The Director of Information Systems shall receive and record basic information on the incident and forward the information to the appropriate staff for response to that type of incident, <i>i.e.</i>, a computer virus incident to the IT Staff that provides anti-virus support.</p> <p>(b) The IT Staff shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The IT Staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify the Director of Information Systems.</p> <p>(c) The Director of Information Systems shall evaluate the incident to determine if a breach of EPHI occurred in consultation with the Privacy Officer. If it is determined that a breach has occurred, the incident shall be reported as set forth in the Breach Notification Policies and Procedures (<i>see</i> policy, Notification in the Case of Breaches of Protected Health Information).</p>
<p>Director of Information Systems</p>	<p>3. <u>Incident Logging</u>. All HIPAA security related incidents and their outcomes will be logged and documented by the Director of Information Systems or his or her designee.</p>
<p>Workforce Members</p>	<p>4. Workforce members are responsible to promptly report any potential security related incident to their manager, supervisor, or the Director of Information Systems. Managers and Supervisors must inform the Director of Information Systems.</p>