DEPARTMENT: Information Systems	**POLICY NUMBER: 004**
DISTRIBUTION: All Staff	**EFFECTIVE DATE:**
SUBJECT: Devices and Media Controls	**REVISION DATE:**

POLICY:

Equinox Inc. shall protect hardware and electronic media that contain EPHI. This includes, but is not limited to, workstation computers, laptops, smartphones, USB drives, backup storage devices, and CDs.

Equinox Inc. is required to have policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI outside of an Equinox Inc. facility/site, and the movement of these items within the facility/sites. Procedures shall include maintaining asset tracking software, including a process for approving the use of personal devices (personal smartphones, personal laptops) by members of the workforce.

PROCEDURE:

Person(s) Responsible:	Procedures:
Director of Information Systems Workforce Members IT Support Privacy Officer	1. <u>Portable Media Protection</u> (a) Equinox Inc. workforce members will not use their personal electronic media, including smartphones, tablets or laptops unless approved by the Director of Information Systems. (b) Workforce members shall sign and acknowledge the **Workforce Member Mobile Device Attestation** (see attached) before using any electronic media, including smartphones, to use or access EPHI. (c) Workforce members shall limit the quantity of EPHI on portable electronic media, including smartphones, to the minimum necessary for the performance of their duties. (d) All workforce members shall receive permission from their supervisor before transporting EPHI outside of the secured physical perimeter of an Equinox Inc. site. Approvals shall include the time period for authorization, which shall be a maximum of one year, but information taken out of the perimeter of a site shall be returned as soon as possible.

Person(s) Responsible:	Procedures:
	(e) Smartphones or portable media issued by Equinox Inc. shall utilize wiping or remote disabling to erase data on the device if lost or stolen. (f) If a smartphone or portable media device that may contain EPHI is lost or stolen, workforce members are responsible to immediately notify their supervisor and the Privacy Officer or Director of Information Systems. (g) Workforce members shall not leave portable media that contains EPHI visible in their vehicles or in any other unsecured location.
Director of Information Systems Workforce Members IT Support	2. <u>Security Requirements for Portable Media Devices Issued by Equinox Inc. that will hold EPHI</u>: (a) use a password or other authentication; (b) install and enable a firewall to block unauthorized access; (c) install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks; (d) keep security software up to date; (e) disable and do not install or use file sharing applications, except as directed (so, for example, Dropbox is used through the website, not the desktop application); (f) install and activate wiping and/or remote disabling to erase the data on the device if it is lost or stolen; and (g) to the extent able, EPHI at rest, which includes data that resides in databases, file systems, flash drives, memory, smartphones, and any other structured storage medium shall be encrypted consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Equinox Inc. is working toward ensuring that any EPHI that is placed on portable electronic media, including smartphones issued by Equinox Inc., shall be encrypted so that access to the EPHI can only be attained by authorized individuals with knowledge of the decryption code.
Director of Information Systems Workforce Members IT Support	3. <u>Disposal of Data</u>. (a) Electronic media, including hard drives (copiers and fax machines included) and smartphones, will be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. (b) Hard drives shall be either wiped clean by IT or destroyed to

Person(s) Responsible:	Procedures:
	prevent recognition or reconstruction of the information. The hard drive shall be tested to ensure the information cannot be retrieved. (c) Smartphones shall have all stored EPHI erased or shall be physically destroyed. (d) Storage media, such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item.
Director of Information Systems Workforce Members IT Support	4. <u>Electronic Media Reuse</u>. (a) All EPHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the EPHI. Hard drives shall be wiped clean by IT before transfer. (b) All other media shall have all of the EPHI removed (the mechanism may vary depending on the media type) and tested to ensure the EPHI cannot be retrieved. If the media is not "technology capable" of being cleaned, the media shall be overwritten or destroyed.
Director of Information Systems Workforce Members IT Support	5. <u>Device Maintenance and Repair</u>. When the technology is capable, all EPHI shall be removed from the device's memory or hard drive before the device is accessed for maintenance or sent out for repair. Devices include computer servers, copiers, printers and other devices capable of storing electronic data.
Director of Information Systems IT Support	6. <u>Device and Media Acquisition</u>. Equinox Inc. shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).