DEPARTMENT: Information Systems	**POLICY NUMBER: 0011**
DISTRIBUTION: All Staff	**EFFECTIVE DATE:**
SUBJECT: User Access Management Policy	**REVISION DATE:**

POLICY:

Equinox Inc. shall establish and maintain policies to ensure access is granted on a need-to-know basis and at the minimum access level necessary for each user to perform his/her job duties. This policy should be read in conjunction with Equinox's policy entitled **User Account Control.**

PROCEDURE:

Person(s) Responsible:	**Procedures:**
Director of Information Systems	1. <u>Management and Access Control</u>. (a) Only the Director of Information Systems or an appropriate designee can authorize access to Equinox's EPHI information systems. (b) The Director of Information Systems or an appropriate designee will assign a unique name and/or number for identifying and tracking the identity of a user of the EPHI information systems. (c) Access to the EPHI information systems may be revoked or suspended if there is evidence that an individual is misusing information or resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.
Director of Information Systems	2. <u>Minimum Necessary Access</u>. (a) Equinox Inc. shall ensure that only workforce members who require access to EPHI are granted access. (b) The Director of Information Systems or an appropriate designee is responsible for ensuring that the access to EPHI granted to the

Person(s) Responsible:	Procedures:
	workforce member is the minimum necessary access required for each work role and responsibilities. (c) If the workforce member no longer requires access, it is the responsibility of the Director of Information Systems or an appropriate designee to complete the necessary process to terminate access.
Director of Information Systems	3. Granting Access to EPHI. The Director of Information Systems or an appropriate designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI is appropriate.
Workforce Member	4. Sign Security Acknowledgement. Prior to being issued a User ID or logon account to access any EPHI, each workforce member shall review and execute the **Staff Acknowledgment of Receipt of Training** before access is granted to the network or any application that contains EPHI, and thereafter shall comply with all Equinox's security policies and procedures. *See* policy, **Training Regarding the Use and Disclosure of Protected Health Information**.
Director of Information Systems	5. Security Awareness Prior to Getting Access. Before access is granted to Equinox Inc. EPHI information systems, the Director of Information Systems or an appropriate designee shall ensure that workforce members are trained to a minimum standard including: (a) Proper uses and disclosures of the EPHI stored in the systems or application; (b) How to properly log on and log off the systems or application; (c) Instructions on contacting the Director of Information Systems or an appropriate designee when EPHI may have been altered or destroyed in error; (d) Reporting a potential or actual security breach; and (e) Instructions regarding internet security, virus protection, password security and confidential data handling.
Director of Information Systems Chief Executive Officer	6. Granting Access in an Emergency. The Director of Information Systems or an appropriate designee has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if: (a) The Director of Information Systems or an appropriate designee, or the Chief Executive Officer declares an emergency or is responding to a natural disaster that makes individual

Person(s) Responsible:	Procedures:
	information security secondary to personnel or individual safety; or (b) The Director of Information Systems or Chief Executive Officer determines that granting immediate access is in the best interest of the individual. (c) If emergency access is granted, the Director of Information Systems shall review the impact of emergency access and document the event within 24 hours of it being granted. (d) After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.
Director of Information Systems	7. <u>Termination or Suspension of Access</u>. The Director of Information Systems or an appropriate designee is responsible for terminating a workforce member's access to EPHI in these circumstances: (a) If there is reason to believe the workforce member is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies; (b) If the workforce member or anyone else has reason to believe the user's password has been compromised; (c) If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave; or (d) If the workforce member's work role changes and system access is no longer justified.