DEPARTMENT: Information Systems	**POLICY NUMBER: 006**
DISTRIBUTION: All Staff	**EFFECTIVE DATE:**
SUBJECT: Password Management and Authentication Policy	**REVISION DATE:**

POLICY: Information systems used to access EPHI shall uniquely identify and authenticate workforce members. Workforce members are required to treat their IDs and password as sensitive and confidential information. IDs and passwords are prohibited from being shared and users are responsible for their use unless authorized by Equinox Inc.

PROCEDURE:

Person(s) Responsible:	**Procedures:**
Director of Information Systems	1. <u>Authentication Standards</u>. (a) The password file on the authenticating server shall be adequately protected and not stored in plaintext (unencrypted). (b) Network and application systems shall be configured to enforce at a minimum: (i) Automatic password expiration at User ID creation and password reset; (ii) Automatic password expiration every ninety (90) days; (iii) A minimum password length of eight (8) characters; and (iv) A minimum of twelve (12) previous passwords that cannot be reused with a User ID.
Workforce Members Director of Information Systems	2. <u>User ID and Password Management</u>. (a) All workforce members are assigned a unique User ID to access Equinox Inc.'s EPHI information systems and are responsible for creating and maintaining the confidentiality of the password associated with their unique User ID.

Person(s) Responsible:	Procedures:
	(b) The Director of Information Systems or an appropriate designee is required to ensure that the workforce understands the user responsibilities for securely managing confidential passwords. (c) Upon receipt of a User ID, the workforce member assigned the User ID is required to change the password provided by the administrator to a password that only he or she knows. Strong passwords shall be created in order to secure access to EPHI. (d) Workforce members who suspect that their password has become known by another person shall change their password immediately and immediately notify the IT Department. Workforce members shall not share with or reveal their password to anyone, including their supervisor, or IT support staff. (e) All privileged system-level passwords (*e.g.*, root, enable, application administration accounts, etc.) shall be changed when IT staff leave the agency and annually, where possible. (f) All passwords are to be treated as sensitive and confidential. If an emergency situation requires access to a workforce member's account, *see* policy, **User Access Management**.
Workforce Members	3. <u>Strong Password Guidelines</u>. Select strong passwords that have the following characteristics: (a) The password contains at least eight (8) characters. (b) The password contains both upper and lower case characters. (c) The password contains at least one number or special character, such as @, #, $, %, and &. (d) The password is not so hard to remember that you have to write it down and is difficult for others to guess. (e) Passwords cannot contain easy to guess words (first/last names, social security numbers, etc). (f) Avoid using dictionary words.
System Administrators	4. <u>Support Responsibilities</u>. Anyone designated by Equinox Inc. as a system administrator shall: (a) verify the identity and the authority of the workforce member or an authorized requester, such as the member's manager or supervisor, before providing the password for a new User ID; (b) verify the identity and the authority of the workforce member requesting a password reset; and

Person(s) Responsible:	Procedures:
	(c) verify the identity and the authority of an authorized requester, such as the workforce member's manager or supervisor, to request a password reset for another workforce member.
Workforce Members	5. <u>Workforce Member Responsibilities</u>. (a) Workforce members shall create and securely manage strong passwords for access to systems containing EPHI. (b) Workforce members shall follow the password protection requirements to protect the confidentiality of their passwords to ensure security of EPHI: (i) Passwords shall not be shared with or revealed to anyone, including their supervisor, manager or IT support staff; (ii) Passwords shall never be revealed on questionnaires or security forms; (iii) Passwords shall be memorized, not written down; (iv) The password used to access the network shall not be used anywhere else; and (v) password shall be changed immediately if the workforce member suspects it has become known by another person.