190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Password Management Policy

Version	Approval Date	Owner
1.3	December 5, 2019	Chief Information Security Officer

1. Purpose

To protect HealthShare Exchange (HSX) information assets by managing and enforcing password requirements.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, and third parties who use HSX information assets and related resources.

This policy applies to centrally-administered and managed information asset technologies, personally-owned computing devices connected by wire or wireless to the HSX network, and to off-site computing devices that connect remotely to the HSX network.

This policy applies to System Administrators and developers who manage or design systems that require passwords for authentication.

3. Policy

Password Management Policy:

- Passwords shall be controlled through a formal password management process.
- Controls shall be implemented to maintain the security of passwords:
    - HSX shall employ automated tools to assist the user in selecting strong passwords and authenticators.
    - Strong passwords shall be required with a minimum length of eight (8) characters and which either meet three of four complexity requirements or otherwise has an equivalent strength (entropy):
        - Easy to remember;

    - Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, and dates of birth etc.);
    - Not vulnerable to dictionary attack (do not consist of words included in dictionaries);
    - Free of consecutive identical characters; and
    - A combination of alphabetic, upper- and lower-case characters, numbers, and special characters (combination of any three [3] of the above four [4] listed is acceptable).
  - Passwords shall not display as they are entered.
  - Passwords shall be changed whenever there is any indication of possible system or password compromise.
  - An individual's identity shall be verified before performing password resets.
  - Passwords shall not be included in any automated log-on process (e.g., stored in a macro or function key).
  - Failed log in attempts shall result in system lock out after six failed attempts.
  - A lockout duration of 30 minutes shall be required and implemented.
  - Documented approval by the Chief Information Security Officer (CISO) shall be required for information assets not utilizing an automatic lock out process.
  - Privileged users (e.g., System Administrators) shall be required to utilize a two-factor authentication method approved by the CISO.
- Controls shall be implemented to maintain the security of initial or temporary passwords:
  - Users shall be provided with an initial or temporary strong password that is unique and random.
  - Passwords shall be provided in a secure manner.
  - Transmitting passwords through the use of third parties or unencrypted (clear text) email messages shall be prohibited.
  - Users shall acknowledge receipt of passwords.
  - Initial or temporary passwords shall be changed at the first log in.
  - Initial or temporary passwords shall expire after 72 hours.
- Passwords shall be changed every 90 days.
- Passwords shall not be reused for at least six (6) generations and at least (4) characters must be changed.
- Passwords are changed for default system accounts, at first login following the issuance of a secure temporary password, when there is a suspected compromise,

and no less than every ninety (90) days for regular accounts or 60 days for privileged (i.e., administrator accounts).

Vendor Password Management:

- Vendor-supplied default accounts shall be deleted, disabled or otherwise altered.
- Vendor-supplied passwords shall be changed.
- Vendor-supplied Simple Network Management Protocol (SNMP) community strings shall be changed.

Password Management Systems:

- Systems for managing passwords shall be interactive and shall ensure strong passwords.
- A password management system shall be implemented to:
    - Enforce the use of unique individual User IDs and passwords to maintain accountability.
    - Prevent the use of the same password for multiple System Administrator accounts.
    - Allow users to select their own passwords and include a confirmation procedure to allow for input errors.
    - Force users to change temporary passwords at the first log-on.
    - Prevent the display of passwords on the screen as they are being entered.
- The password management system shall enforce all password policy requirements:
    - Protection of passwords at rest or in transit using strong encryption algorithms such as 3DES or AES or strong hashing algorithms such as SHA-1 or SHA-256.
    - Storage of password files separately from application system data
    - Strong passwords
    - Password changes
    - Prevent re-use
- When a password is changed or reset, an email shall automatically be sent to the owner of that account.
- Electronic signatures are the same as hand written signatures and are legally binding when used in accordance with the provisison of the Contracting and Signatory Authorization Policy.
- Authorized persons who use application based electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

- Identity verification of the individual is required prior to establishing, assigning, or certifying an individual's electronic signature or any element of such signature.
- Maintaining the uniqueness of each combined identification code and password, such that no two (2) individuals have the same combination of identification code and password.
- Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging);
- Following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls;
- The use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and
- Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
- Electronic signatures not based upon biometrics shall employ at least two distinct identification components that are administered and executed.
- Electronic signatures, unique to one individual, cannot be reused by, or reassigned to, anyone else.
- Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners.

- HSX shall maintain a list of commonly-used, expected or compromised passwords. HSX shall update the list at least every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly.
  - HSX shall verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected or compromised passwords.

Health Information Exchange (HIE) Password Policy:

- Members shall be informed and trained on:
  - Selecting a strong password
  - Not sharing or posting passwords
  - Not writing down their password and placing it at or near the terminal
- Audit trails of all HIE log-ins shall be maintained by HSX.

- Members, participants and users shall not be permitted to share passwords or enter data under another person's password.
- If passwords are shared, disciplinary actions shall be taken, in accordance with the *Sanctions Policy*.

4. Procedures

The following procedures apply to HSX internal operations only:

- Access Control Procedure
- Electronic Signature Procedure
- Password Management Procedure

5. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- The CISO shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

6. Definitions

For a complete list of definitions, refer to the *Glossary*.

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308(a)(5)(ii)(D)
- HITRUST Reference: 01.d User Password Management, 01.r Password Management System
- PCI Reference: PCI DSS v3 2.1, PCI DSS v3 8.2.2, PCI DSS v3 8.2.3, PCI DSS v3 8.2.5, PCI DSS v3 8.2.6

190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Policy Owner	Chief Information Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	December 5, 2019
Date Policy In Effect	December 5, 2019	**Version #**	1.3
Original Issue Date	May 13, 2015	**Last Review Date**	December 5, 2019 September 15, 2019 September 28, 2018
Related Documents	Acceptable Use Policy Glossary		