1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Access Control Policy

Version	Approval Date	Owner
1.3	December 16, 2019	Chief Information Security Officer

1. Purpose

To establish HealthShare Exchange (HSX) requirements for managing and controlling access to information assets and information services in support of compliance with legal regulations (e.g., HIPAA) and to protect and lower risk to business operations.

To ensure that HSX's information assets and information services are properly protected against unauthorized access, while meeting the access requirements for all authorized users.

To ensure that only appropriate and specifically-authorized Members and Participants gain access to the HSX.

2. Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX information assets are required to comply with this policy.

This policy covers access to all enterprise data regardless of whether that data is stored on or provided via HSX information assets or on a third-party-hosted service or equipment.

3. Policy

Access Control Policy

- HSX shall manage access to HSX information assets based upon business requirements, regulatory and legal compliance, and information security risk management best practices.
- Group, shared, or generic accounts and passwords shall not be used.

- There shall be a formal written Access Control Plan that defines the processes necessary to implement the *Access Control Policy*. The Access Control Plan shall also define the roles and responsibilities related to access controls.
- Records generated while carrying out the Access Control Plan shall be retained according to the *Compliance Policy*.
- The *Access Control Policy*, Access Control Plan, and associated access control procedures shall be reviewed at least annually.

Access Controls and Authorizations

- Access controls shall be consistently implemented and managed for all information assets across all HSX networked and distributed environments.
- Application and system menus shall be pre-configured to the minimum necessary set based upon roles and responsibilities. Non-administrative users shall not have administrative rights to alter the authorized menus.
- Access control rules and rights shall be determined and managed by HSX. These rules and rights shall be clearly defined in standard user access profiles (e.g., roles) that are based on need-to-know, need-to-share, and least privilege requirements and principles.
- The Access Control Plan shall define an access control authorization process that addresses requests for access, changes to access, removal of access, and emergency access.
- Access authorization (e.g., access requests, approvals, and provisioning) shall be segregated among multiple individuals.
- Access control management shall take into consideration the data classification level of the information asset in accordance with the *Data Classification Policy*.
- Information assets identified as confidential or internal-use-only according to the *Data Classification Policy* shall always require access control management and associated protective measures.
- Administrative privileged user access credentials shall be separate from normal business access credentials unless otherwise specifically approved by the CISO
- Administrative privileged user access shall require multi-factor authentication
- Hardware tokens shall not be utilized
- Access granted to external parties is limited to the minimum necessary and granted only for the duration required
- BYOD devices shall not be whitelisted for access to HSX services. BYOD device access shall be limited to office applications.
- Upon termination or changes in employment for employees, contractors, third-party users or other workforce arrangement, physical and logical access rights and associated materials (e.g., passwords, keycards, keys, documentation that identify them as current members of the organization) are removed or modified to restrict

access within 24 hours and old accounts are closed after 90 days of opening new accounts.

User Registration

- The Access Control Plan shall define the process for granting and revoking access to HSX information assets by users and at a minimum shall include the following:
    - Authentication methods
    - Authorization verification process
    - Types of accounts including third party accounts, maintenance accounts, and senior leadership accounts
    - Status changes including terminations and transfers
    - Processes for removing, disabling or otherwise securing inactive and unnecessary accounts
- System Administrators shall be notified by an HSX Senior Manager when an individual's access rights change (e.g., termination, change in position) and IT shall make the necessary changes within sixty (60) minutes.
- Automated mechanisms shall delete emergency accounts within twenty-four (24) hours and delete temporary accounts within three hundred sixty-five (365) days.
- User identities shall be verified prior to establishing accounts.
- Users shall be provided a written statement of their access rights, which they shall be required to sign physically or electronically to indicate that they understand the conditions of access.

Mobile Computing Device Access

- Mobile computing devices shall be granted access according to the *Mobile Computing Device Security Policy*.
- Appropriate security measures shall be adopted to control access and protect against the risks of using mobile computing devices.
- Remote access to HSX enterprise data across public networks using mobile computing devices shall only take place after successful identification and authentication, and with suitable access control mechanisms in place.
- All mobile devices permitted for use through HSX's Bring Your Own Device (BYOD) program or a HSX-assigned mobile device shall allow for remote wipe by the HSX Privacy Officer or shall have all company-provided data wiped by the HSX Privacy Officer. See *Mobile Computing Device Security Policy* for instructions on how to conduct a remote wipe.

- Bring your own device (BYOD) and/or company-owned devices are configured to require an automatic lockout screen, and the requirement is enforced through technical controls.

System and Other Computing Device Access

- The Access Control Plan shall define the process for granting and revoking access to HSX information assets by systems and computing devices and at a minimum shall include the following:
    - Verifying authorization and identity prior to granting access
    - Status changes such as equipment taken out of service
    - Processes for removing, disabling or otherwise securing inactive and unnecessary accounts
- HSX shall remove, disable, or otherwise secure unnecessary accounts on systems or computing devices given access to HSX information assets.
- Group, shared, or generic accounts and passwords shall not be used on systems or computing devices given access to HSX information assets.

Data and Applications Access

- Applications shall control the access rights of users (e.g., read, write, delete and execute).
- Access rights between applications shall be controlled.
- Confidential data shall be encrypted at rest, in transit, and in storage according to the *Encryption Policy*. HSX shall document exceptions and their rationale.
- Outputs from application systems handling confidential data shall be limited to the minimum necessary and sent only to authorized terminals/locations.
- No actions may be performed without identification and authentication.
- Copy, move, print (and print screen), and storage of confidential data outside of HSX's networks shall be strictly prohibited.
- The use of database management utilities for any database containing confidential data or internal use only data shall be restricted to authorized database administrators only.

Operating Systems Access

- Access to HSX Operating Systems shall be controlled by a secure log-on procedure.
- All users shall have a unique identifier (user ID) for their individual use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user.

- Systems for managing passwords shall ensure strong passwords according to the *Password Management Policy*.
- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
- Inactive sessions shall automatically shut down after 15 minutes of inactivity.
- Employee-issued computers shall lock the desktop session (login screen) by turning off the monitor or using a screensaver after two minutes, requiring the user to re-enter their access credentials.
- Employee-issued computers shall close all network connections after 30 minutes of inactivity.
- Restrictions on connection times shall be used to provide additional security for high-risk applications.

Privilege Management

- The allocation and use of privileged access to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.
- Privileged access credentials shall be separate from normal business access credential.
- Privileged access must be conducted with multi-factor authrentication.
- The allocation of privileges shall be controlled through a formal access authorization process administered by the When and where deemed necessary by the Chief Information Security Officer (CISO).
- Access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) shall be restricted.
- Privilege allocation shall follow the principle of least privilege.
- The access privileges associated with each system (e.g., Operating System, database management system, individual applications) and the users to which they need to be allocated shall be identified.
- Privileges shall be allocated to users based upon on data classification, work roles and job function, and business requirements. Privileges shall be granted based upon the minimum requirement for a user's functional role, and only when needed.
- An authorization process and a record of all privileges allocated shall be maintained. Privileges shall not be granted until the authorization process is complete.
- The development and use of systems and applications which avoid the need for elevated privileges shall be promoted.
- Elevated privileges shall be assigned to a different user ID from those used for normal business use. All users shall access privileged services in a single role.

- The use of System Administration privileges any feature or facility of an information system that enables the user to override system or application controls) shall be minimized.
- Security relevant information shall be restricted to explicitly authorized individuals.

Authentication Methods

- Authentication of user identities shall be accomplished by passwords at a minimum. When and where deemed necessary by the CISO, the use of stronger authentication methods (e.g., encryption, smart cards, tokens, or biometric means) shall be required.
- Communications through an external, non-organization-controlled network (i.e., the Internet) shall require stronger authentication methods.
- Individuals attempting unauthorized access shall be sanctioned according to the *Sanction Policy*.
- Business Associate Agreements shall specify sanctions for unauthorized access attempts by third parties.
- The HSX Support desk requires user identification for any transaction that has information security implications

Review of Access Rights

- Access rights shall be reviewed by the CISO every ninety (90) days following a formalized documented process.
- Accounts deemed to be privileged shall be subject to more frequent reviews than standard accounts. All privileged accounts shall be reviewed by the System Administrator at a minimum every sixty (60) days.
- Access rights shall be reviewed after any personnel changes, such as promotion, transfer, demotion, or termination of employment.
- Evidence of these reviews, including signatures of approval, shall be submitted for review and retention. Follow-up actions resulting from the review shall be documented and included as part of the evidence submitted to the CISO.

Access to Network Services

- The granting of access to network services shall be based on the principle of least privilege.
- Authentication and authorization mechanisms shall be applied for users and equipment.
- HSX shall specify the networks and network services to which users and information assets are authorized access.

- HSX shall determine provisioning of access to specific networks and network services, and shall specify the means of access allowed, including specific ports, protocols and services.
- HSX does not allow network devices capable of dial-up connections.

Remote Diagnostic and Configuration Port Protection

- Physical and logical access to diagnostic and configuration ports shall be controlled.
- Access to network equipment shall be physically protected (e.g., a router must be stored in a room that is only accessible by authorized individuals) such that remote diagnostic and configuration ports are protected. Additionally, logical access to remote management of network equipment shall be protected.
- Controls for the access to diagnostic and configuration ports shall include the use of a key lock.
- Ports, services, and similar applications installed on a computer or network systems, which are not specifically required for business functionality, shall be disabled or removed.

Sensitive System Isolation

- Systems containing confidential data shall have a dedicated and logically and/or physically isolated computing environment.
- The sensitivity level of applications and systems shall be explicitly identified and documented according to the *Data Classification Policy*.
- The isolated computing environment must protect applications and systems based on the explicitly identified and documented data classification and regulatory, business, and information security protection requirements.
- All Systems with sensitive internal-use-only data shall be isolated (physically or logically) from systems with non-sensitive public data. Exceptions must be authorized and documented, including business case justification, acceptance of risk, and the length of the exception. Exceptions longer than one year must be approved by the CISO.
- Shared system resources (e.g., registers, main memory, and secondary storage) shall be released back to the source system and protected from disclosure to other systems, applications, and users.
- Both system owners and the network owner shall ensure that appropriate auditing, logging, and monitoring is in place to ensure system isolation security controls are in effect.
- Unauthorized remote access connections to the network and information systems shall be monitored and reviewed quarterly as stipulated in the *Audit, Logging and Monitoring Policy*.

- The dedicated and isolated computing environment shall only be accessible by authorized personnel. The list of authorized personnel shall be reviewed on an annual basis by the CISO.

Mobile Device Training

- HSX Supervisors will be responsible for ensuring staff members have reviewed and are compliant with HSX policies by
  - Referring staff to the HSX website to review the policies
  - Or conduct a one-on-one or organizational lunch and learn meeting to review HSX policies
  - All staff members, interns, and third-party individual will be required to sign an attestation document acknowledging HSX policies.

4. Procedure

The following procedures apply to HSX internal operations only:

- Access Control Procedures
- Bring Your Own Device Procedure
- Data Handling, Labeling and Storage Procedure
- Incidence Response Plan
- Mobile Computing Device Security Procedure
- Mobile Device Protection Procedure
- Network Protection Procedure
- New Employee Set Up Procedure
- Third Party Vendor Selection Process

5. Enforcement

- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President.
- The CISO shall ensure that monitoring is conducted the current devices attached to the Wi-Fi on a quarterly basis to ensure that a list of all devices on the Wi-Fi is

created and that devices are not reporting a spoofed MAC address to circumvent filtering.

- The CISO shall ensure all devices are compliant with the Access Control Policy and the Mobile Computing Device Security Policy.
    - If any unauthorized mobile or wireless connections are found, their access will be prevented from the wireless access control interface through MAC address filtering or additional authentication steps.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA §164.308 (a)(3)(i), HIPAA §164.308 (a)(3)(ii)(a), HIPAA §164.308 (a)(4)(i), HIPAA §164.308 (a)(4)(ii)(B), HIPAA §164.308(a)(3)(i), HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.308(a)(3)(ii)(B), HIPAA §164.308(a)(3)(ii)(C), HIPAA §164.308(a)(4)(i), HIPAA §164.308(a)(4)(ii)(A), HIPAA §164.308(a)(4)(ii)(B), HIPAA §164.308(a)(4)(ii)(C), HIPAA §164.308(a)(5)(ii)(D), HIPAA §164.310(a)(2)(iii), HIPAA §164.310(b), HIPAA §164.312(a)(1), HIPAA §164.312(a)(2)(i), HIPAA §164.312(a)(2)(ii), HIPAA §164.312(a)(2)(ii)(i), HIPAA §164.312(a)(2)(ii)(iv), HIPAA §164.312(a)(2)(iii), HIPAA §164.312(a)(2)(iv), HIPAA §164.312(d)
- HITRUST Reference: 01.a Access Control Policy, 01.b user Registration, 01.c Privilege Management, 01.e Review of user Access Rights, 01.i Policy on the Use of Network Services, 01.j user Authentication for External Connections, 01.k Equipment Identification in Networks, 01.l Remote Diagnostic and Configuration Port Protection, 01.m Segregation in Networks, 01.n Network Connection Control, 01.o Network Routing Control, 01.p Secure Log-on Procedures, 01.q user Identification and Authentication, 01.s Use of System Utilities, 01.t Session Time-out, 01.u Limitation of Connection Time, 01.v Information Access Restriction, 01.w Sensitive System Isolation
- PCI DSS v1.2 8.5, PCI DSS v1.2 8.5.8, PCI DSS v3 1.1.4, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 2.2.1, PCI DSS v3 2.3, PCI DSS v3 7.1, PCI DSS v3 7.1.1, PCI DSS v3 7.1.4, PCI DSS v3 7.2.1, PCI DSS v3 7.2.2, PCI DSS v3 8.1.1, PCI DSS v3 8.1.2, PCI DSS v3 8.1.3, PCI DSS v3 8.1.4, PCI DSS v3 8.1.5, PCI DSS v3 8.1.6, PCI DSS v3 8.1.7, PCI DSS v3 8.1.8, PCI DSS v3 8.2, PCI DSS v3 8.2.2, PCI DSS v3 8.3, PCI DSS v3 8.5, PCI DSS

v3 8.5.1, PCI DSS v3 8.6, PCI DSS v3 8.7, PCI DSS v3 12.3.2, PCI DSS v3 12.3.8, PCI DSS v3 12.3.9, PCI DSS v3 12.3.10

- PA eHealth Reference: 3.1. Access Levels

Policy Owner	Security Officer	**Contact**	BrianWells@healthshareexchange.org
Approved By	Brian Wells	**Approval Date**	December 30 2019 March 19, 2019
Date Policy In Effect	December 30, 2019	**Version #**	1.3
Original Issue Date	June 3, 2015 approved by Daniel Wilt, CISO	**Last Review Date**	September 17, 2020 December 30, 2019 March 19, 2019
Related Documents	Access Control Plan Audit, Logging and Monitoring Policy Compliance Policy Data Classification Policy Encryption Policy Glossary Mobile Computing Device Policy Network Protection Policy Password Management Policy Sanction Policy		