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

Personnel Security Policy

Version	Approval Date	Owner
1.1	September 28, 2017	Chief Information Security Officer

1. Purpose

The purpose of personnel security controls is to ensure that HealthShare Exchange (HSX) information assets are protected from the adverse actions of personnel.

Information systems face threats from many sources, including the actions of people—employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt information systems and their facilities or result in unauthorized access to confidential data. These actions can also result in the destruction or modification of the data being processed, denial of service to the end users, and unauthorized disclosure of confidential data, potentially adversely impacting the quality and continuity of HSX business operations.

2. Scope

This policy applies to all interns, employees, contractors, members, participants, users, and third parties who access, use or support HSX information assets, regardless of physical location.

IT resources include all HSX owned, licensed, leased, or managed hardware and software, and use of the HSX network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

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

3. Policy

HSX shall take actions to ensure that HSX information assets are protected from the adverse actions of employees, interns and contractors., members, participants, users, and third parties.

Requirements for Employees including interns and Contractors Performing in Information Security Roles:

- HSX shall define and document roles and responsibilities and entitlements for employees and contractors performing information security work and/or duties in accordance with the *Information Security Management Program Policy*.
- HSX shall assign a risk designation to all security roles and job functions regardless of job title.
- HSX shall review and revise risk designations annually.
- HSX shall define screening criteria for security roles.
- Human Resources and Direct hiring manager shall ensure security roles and responsibilities are clearly communicated to potential job candidates.
- An individual or dedicated team shall be assigned to manage the information security of the organization and its users.

Personnel Screening:

- HSX shall carry out background verification checks on all employees, interns and contractors in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
- Human Resources shall be responsible for conducting HSX personnel screening.
- HSX shall define the procedures and criteria for background verification checks. At a minimum, Human Resources shall verify the identity, current address, and previous employment of the potential job candidate prior to employment or business engagement. In addition, for employees, within 30 days of hire, HSX shall conduct a criminal background check.

Terms and Conditions of Employment:

- Employees, interns, and contractors who are given access to confidential data shall sign a Confidentiality Agreement prior to being given access to information assets.

HSX Chief Information Security Officer (CISO) and HSX Privacy Officer Responsibilities:

- The CISO and Privacy Officer shall ensure that employees, interns and contractors:
    - Are briefed on the incident response plan based upon the individual roles and responsibilities of the employee/intern/contractor.
    - Are properly briefed on information security roles and responsibilities prior to being granted access to confidential data;
    - Are provided with guidelines to the state security expectations of their role within the organization;
    - Are motivated to comply with security policies;

  - Achieve a level of awareness on security relevant to their roles and responsibilities;
  - Conform to the terms and conditions of employment, which includes the information security policies and appropriate code of conduct both in the office and when representing HSX outside the office.
  - Maintain appropriate skills and qualifications related to information security and especially access to confidential data.
  - Provide regular reports to the HSX Executive Committee.
- In accordance with the *HSX Privacy and Security Awareness and Education Policy,* HSX shall establish and have an ongoing education and training program to ensure all employees, interns and contractors who perform information security roles and/or activities stay current and up-to-date on IT security best practices, applicable laws, directives, standards, procedures, policies, instructions, and regulations.
- HSX shall ensure plans for security testing, training, and monitoring activities are developed, implemented, maintained, and reviewed for consistency with the risk management strategy and incident response priorities.
- Acceptable use of information assets by employees, interns and contractors shall be defined and explicitly authorized in the *Acceptable Use Policy*.

Responsibilities for Members Participants and Third Parties

- Members, participants, and third parties who will have access to HSX information assets shall be provided the privacy and security policies and given HIPAA training prior to accessing HSX information assets.
- Acceptable use of information assets by members, participants, users, and third parties shall be defined and explicitly authorized in the *Acceptable Use Policy*.
- Members and participants shall ensure that users under their control and/or within their area of responsibility receive appropriate and sufficient information security training and materials to learn and remain updated on issues, requirements, expectations and procedures for protecting computing devices.
- Members, participants, users, and third parties shall demonstrate understanding of information security policies, procedures, standards and directives through their compliance.

Confidentiality Agreements:

- Confidentiality Agreements shall be applicable to all employees, interns, contractors, and third parties who do not otherwise have a Business Associate Agreement with HSX and are accessing confidential data.
- Confidentiality Agreements shall comply with all applicable laws and regulations for the jurisdiction to which they apply.

- Requirements for Confidentiality Agreements shall be reviewed at least annually and when changes occur that influence these requirements.

4. Procedures

The following procedures apply to HSX internal operations only:

- Access Control Procedures
- HSX New Employee Onboarding Process
- Incidence Response Plan
- Third Party Vendor Selection Process

5. Enforcement

- The HSX Human Resource representative will ensure that all employees, interns, consultants and contractors receive education and training as per this policy.
- The CISO and Privacy Officer are responsible for enforcing compliance with the policy under the direction of the Executive Director.
- Each member, participant and third party will be responsible for ensuring that their respective physicians, care managers and other staff are following the procedures outlined in this policy.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: 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)(ii)(B), HIPAA §164.308(b)(1), HIPAA §164.310(b), HIPAA §164.310(d)(2)(iii), HIPAA §164.314(a)(1), HIPAA §164.314(a)(2)(i), HIPAA §164.314(a)(2)(ii)
- HITRUST Reference: 02.a Roles and Responsibilities, 02.b Screening, 02.c Terms and Conditions of Employment, 02.d Management Responsibilities, 05.e Confidentiality Agreements

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org
Approved By	Board HSX Management Team HSX Privacy and Security Workgroup.	**Approval Date**	September 28, 2017
Date Policy In Effect	June 4, 2015	**Version #**	1.1
Original Issue Date	June 4, 2015	**Last Review Date**	December 1, 2018
Related Documents	Acceptable Use Policy Confidentiality Agreement Employee Manual Glossary Information Security Program Management Policy Privacy and Security Awareness and Education		