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

Information Security Policy

Version	Approval Date	Owner
1.1	November 8, 2018	Chief Information Security Officer

1. Purpose

This document identifies the requirements for the creation and maintenance of information security policies in support of the Information Security Management Program (ISMP). The intent is to ensure that HealthShare Exchange (HSX) information security policies and policy maintenance procedures align with best practices, regulatory requirements, and federal and state laws.

2. Scope

This policy covers all HSX information security practices across all departments and business units. All HSX employees, interns, contractors, members, participants, users, and third parties are required to comply with this policy.

3. Policy

Information Security Policies

- Information security policies shall be developed and approved by management to establish the direction of HSX's information security program and align with best practices, regulatory requirements, and federal and state laws.
- The information security policies shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for senior leadership and officer roles.
- The information security policies shall be published, communicated, and made available to all employees, contractors, members, participants, users, and third parties.

Review of Information Security Policies

- All information security policies shall be reviewed to ensure their continuing adequacy and effectiveness by the Chief Information Security Officer (CISO) on a rolling cycle such that every policy is reviewed at least annually or more frequently if significant organizational, environmental, or regulatory changes occur.
- The review shall include assessing opportunities for improvement of the policy and HSX's approach to managing information security changes related to HSX's environment, business circumstances, legal conditions or technical environment.
- The policy review must include the following as applies:
    - Input from HSX senior leadership, the HSX Executive Committee and the HSX Privacy and Security Workgroup.
    - The HSX Board would conduct substantive policy review on an as needed basis.
    - Results of independent reviews or audits.
    - Status of identified risks and preventive and corrective action plans.
    - Results of previous reviews.
    - Process performance and information security policy compliance.
    - Consideration of changes that could potentially affect HSX's approach to managing information security or its technical environment, including the organizational environment, business circumstances, resource availability, and contractual, regulatory, and legal conditions.
    - Operational changes and impact on the risk profile and risk management needs.
    - IT infrastructure changes and impact on the risk profile and risk management needs.
- The policy review may include:
    - Guidance from professional associations to leverage best practices and to ensure consideration of current assurance requirements.
    - Results of applicable legal cases tested in courts that establish or cancel precedents and the resulting impact on operations.
- The results and conclusions of the policy review shall include any decisions and actions related to:
    - Improvement of HSX's approach to managing information security and its processes.
    - Improvement of control objectives and controls.
    - Improvement in the allocation of resources and/or responsibilities.
- A record of the policy review shall be maintained. Approval for the policy revisions shall be obtained and included in the record of the policy review.

4. Procedures

None

5. Enforcement

- The Chief Information Security Officer (CISO) and the Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President.

6. Definitions

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

7. References

Re Regulatory References

- HIPAA Regulatory Reference: HIPAA § 164.312(c)(1), HIPAA § 164.316(a), HIPAA § 164.316(b)(2)(i), HIPAA § 164.414(a), HIPAA § 164.530(i)
- HITRUST Reference: 04.a Information Security Policy Document, 04.b Review of the Information Security Policy
- PCI Reference: PCI DSS v3 1.5, PCI DSS v3 2.5, PCI DSS v3 3.7, PCI DSS v3 4.3, PCI DSS v3 5.4, PCI DSS v3 6.7, PCI DSS v3 7.3, PCI DSS v3 8.8, PCI DSS v3 9.10, PCI DSS v3 10.8, PCI DSS v3 11.6, PCI DSS v3 12.1

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	Board HSX Management Team HSX Policy and Security Workgroup	**Approval Date**	November 8, 2018
Date Policy In Effect	June 4, 2015	**Version #**	1.1

Original Issue Date	June 4, 2015	**Last Review Date**	September 14, 2020 November 8, 2018
Related Documents	Glossary Information Security Management Program Policy		