HSX HealthShare Exchange

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

Information Security Management Program Policy

Version	Approval Date	Owner
1.0	January 19, 2017	Chief Information Security Officer

1. Purpose

This policy establishes the high-level requirements for HealthShare Exchange's (HSX) Information Security Management Program (ISMP). The ISMP will reduce risks to HSX by protecting and supporting the confidentiality, availability, and integrity of information assets.

HSX is committed to conducting business in keeping with its core organizational values and established policies and in compliance with all industry standards and applicable laws and regulations. In particular, HSX is committed to compliance with the regulatory requirements established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of electronic protected health information ("ePHI"), also known as the "Security Rule" and all subsequent Security Rule updates, as well as all state-level regulatory compliance requirements that apply to its area of operations.

2. Scope

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

3. Policy

Protecting HSX confidential data and reducing information security risks is the responsibility of all HSX employees, interns, contractors, and third parties. HSX shall establish formal information security, privacy, and risk management programs. These programs shall work together with the common goal of reducing risk to HSX. These programs shall be reviewed and updated annually.

HSX shall design, implement, and maintain a comprehensive and effective ISMP to ensure acceptable levels of risk throughout the organization. The ISMP shall be continuously assessed and improved upon through governance, risk management, information security protective operations, awareness and training, and incident response activities.

- HSX shall implement a formal ISMP to ensure the confidentiality, availability, and integrity of information assets. The ISMP shall be designed to the specific characteristics of HSX and shall be established and managed via continuous monitoring, maintenance and improvement.
- The ISMP shall be formally documented and actively monitored by the Chief Information Security Officer (CISO).
- The ISMP shall be reviewed and updated as often as needed, but a least annually, to ensure program objectives continue to meet the needs of HSX and the plan addresses any new risks.
- Independent audits shall be conducted and reported to the CISO annually to determine whether the ISMP is:
  - Managing risk effectively
  - Compliant with federal and state laws and regulations
  - Approved by senior leadership
  - Communicated to stakeholders
  - Adequately resourced

ISMP Strategy:

- The HSX ISMP shall be based on an industry standard framework such as the HITRUST Common Security Framework (CSF). The industry-accepted HITRUST CSF framework is designed to provide compliance with a large number of industry standards and regulatory requirements.
- The HITRUST CSF framework is designed to give HSX a single strategy allowing repeatable measured compliance over any and all of these listed areas, and at a level of control suitable for the organization's size and structure. The CSF is adaptive and designed to allow HSX to comply with relevant standards as business strategy or organizational needs change in the future.
- The ISMP shall be implemented, organized, and supported by the CISO to ensure it is capable of accomplishing its primary tasks of information security:
  - Governance
  - Risk management
  - Information security protection operations
  - Education, training, and awareness
  - Incident response activities

ISMP Content:

- At a minimum, the ISMP shall include:
    - HSX approved information security policies and procedures
    - Mission, vision, structure and objectives of the information security program
    - Governance structure and business continuity
    - HITRUST common security framework
    - Annual risk assessment
    - Risk management measures and actions
    - Education, training, and awareness plan and materials
    - Information security plans for: information systems, end user devices, applications, networks including wireless, IT security devices and systems
    - Disaster recovery
- The ISMP shall meet applicable legal, regulatory and appropriate best security practices as determined by the CISO.
- The ISMP shall be periodically reviewed and communicated to relevant stakeholders.

Commitment to Information Security:

- HSX senior leadership shall actively support information security within the organization through clear direction, demonstrated commitment, incorporation into strategic planning, and acknowledgment of information security responsibilities.
- A CISO shall be appointed as designated in the *Privacy and Security Roles Policy*.
- Formal governance shall be chartered and active to ensure institutional oversight, coordination, and synchronization of information security at HSX.
- The formal governance body shall review the effectiveness of the ISMP and evaluate and accept security risks.
- Capital planning and investment requests shall consider information security. The requests shall include resources necessary for implementing information security capabilities necessary to address any risks associated with such capital plans and requests. HSX shall ensure such resources are available for expenditure and applied appropriately.
- Annual risk assessments shall be performed by an independent organization. The results shall be reported to the CISO, and shall be incorporated into the ISMP's Risk Management Plan.
- CISO shall be responsible for developing a plan of action to address identified risks and reporting status against those risks. Senior leadership shall be responsible for review, approval and appropriate oversight of such plan.

Information Security Coordination:

- Managing information security risks is the responsibility of all employees, contractors, members, participants, users, and third parties. Risk reduction activities shall be coordinated and communicated by representatives from different parts of HSX respective to their roles and job functions.
- Security activities (e.g., implementing controls, correcting non-conformities, penetration testing) shall be coordinated in advance and shall be communicated across the entire organization.
- Security requirements for information systems shall be identified and resources shall be allocated as either capital or operating resources in a separate budget line item.
- An internal security information sharing mechanism shall exist to communicate non-conformities and lessons learned to senior leadership.

Information Security Responsibilities:

- All information security responsibilities shall be formally defined in writing.

Authorization Process for Information Assets and Facilities:

- A management authorization process for acquiring new information assets (e.g., systems and applications), and facilities (e.g., data centers or offices where covered information will be processed), including their maintenance, shall be defined and implemented according to the *Information Systems, Acquisition, Development and Maintenance Policy*.
- A vendor vetting process shall be defined and implemented to ensure that any potential processing facility or vendor can provide documentation to demonstrate that appropriate security measures are followed at a level necessary to meet all regulatory requirements, HSX security policies and industry standards.

Contact with Authorities:

- Appropriate contacts with relevant authorities shall be maintained.
- The CISO shall review and update the list at least annually to keep it current.

Maintaining current knowledge of external threats and the changing security environment:

- Appropriate contacts with special interest security groups and other specialist security forums and professional associations shall be maintained.

Independent Review of Information Security:

- HSX's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed annually by an independent organization, or when significant changes to the security implementation occur.

- The review shall be carried out by individuals with the necessary expertise.

The review shall generate a corrective action plan that is reported to senior leadership by the CISO.

4. Procedures

The following procedures apply to HSX internal operations only:

- Information Security Management Program
- Incidence Response Plan
- Risk Management Plan

5. Enforcement

- The CISO and the Privacy Officer 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)(2), HIPAA §164.308(a)(1)(i), HIPAA §164.308(a)(1)(ii)(A), HIPAA §164.308(a)(1)(ii)(B), HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(2), HIPAA §164.308(a)(5)(ii)(A), HIPAA §164.308(a)(8), HIPAA §164.310(a)(2)(ii), HIPAA §164.316(a), HIPAA §164.316(b)(1), HIPAA §164.316(b)(1)(i), HIPAA §164.316(b)(2)(iii), HIPAA §164.316(b)(2)(iii)
- HITRUST Reference: 0.a Information Security Management Program, 05.a Management Commitment to Information Security, 05.b Information Security Coordination, 05.c Allocation of Information Security Responsibilities, 05.d Authorization Process for Information Assets and Facilities, 05.f Contact with Authorities, 05.g Contact with Special Interest Groups, 05.h Independent Review of Information Security
- PCI Regulatory Reference: PCI DSS v3, PCI DSS v3 12.4, PCI DSS v3 12.5, PCI DSS v3 12.5.1, PCI DSS v3 12.5.2, PCI DSS v3 12.5.3, PCI DSS v3 12.5.4, PCI DSS v3 12.5.5

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org
Approved By	HSX Board HSX Management Team Privacy and Security Workgroup	**Approval Date**	September 20, 2017
Date Policy In Effect	June 18, 2015	**Version #**	1.0
Original Issue Date	June 18, 2015	**Last Review Date**	September 17, 2020 December 1, 2018
Related Documents	Glossary Information Systems, Acquisition, Development and Maintenance Policy Privacy and Security Roles Policy		