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

Privacy Management Program Policy

Version	Approval Date	Owner
1.0	December 16, 2015	Privacy Officer

1. Purpose

This policy establishes the high-level requirements for HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX)'s Information Privacy Management Program (PMP). The PMP will reduce risks to HSX by protecting and supporting the confidentiality and privacy of information.

HSX is committed to conducting business in keeping with its core organizational values and established policies in compliance with all 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 privacy of protected health information (PHI), also known as the "Privacy Rule" and all subsequent Privacy 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 privacy practices across all departments and business units. All HSX employees, contractors, members, participants, users, and third parties are required to comply with this policy.

3. Policy

HSX shall design, implement, and maintain a comprehensive and effective PMP. The PMP shall be continuously assessed and improved upon through governance, risk management, protective operations, awareness and training, and incident response activities. The PMP shall be reviewed and updated annually. The establishment and maintenance of a trust community among HSX members and participants is a key component to a successful PMP.

- HSX shall implement a formal PMP to ensure the confidentiality and privacy of PHI. The PMP shall be designed to the specific characteristics of HSX and shall be

established and managed via continuous monitoring, maintenance and improvement.
- The PMP shall be formally documented and actively monitored by the Privacy Officer.
- The PMP shall be reviewed and updated as needed but minimally on an annual basis to ensure program objectives continue to meet the needs of HSX.
- At a minimum, the PMP should include appropriate use of patient data in accordance with HSX Use Case Governance process.

The PMP shall be implemented, organized, and supported by the Privacy Officer to ensure it is capable of accomplishing its primary tasks:

- Governance
- Risk management
- Privacy protection operations
- Education, training, and awareness
- Incident response activities

At a minimum, the PMP shall include:

- HSX approved privacy policies and procedures
- Mission, vision, structure and objectives of the PMP
- Governance structure
- Risk management measures and actions
- Education, training, and awareness plan and materials
- The PMP shall meet applicable legal, regulatory and appropriate best security practices as determined by the Privacy Officer.
- The PMP shall be periodically reviewed and communicated to relevant stakeholders.
- The PMP shall evidence opportunities for patient choices with regard to the privacy of health information.

Commitment to Privacy:

- HSX senior leadership shall actively support privacy within the organization through clear direction, demonstrated commitment, incorporation into strategic planning, and acknowledgment of privacy responsibilities.
- A Privacy Officer shall be appointed as designated in the *Privacy and Security Roles Policy*.
- HSX Privacy and Security Workgroup shall ensure oversight, coordination, and synchronization of privacy at HSX under the direction of the Finance and Audit Committee.
- The HSX Board shall review the effectiveness of the PMP and evaluate and accept privacy risks.

Privacy Coordination:

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

HSX Privacy Policies and Member Responsibilities:

- Each Member shall, at all times, comply with all applicable HSX privacy policies.
- HSX privacy policies may be revised and updated from time to time, and reasonable notice of any such changes shall be provided to Members.
- Each Member is responsible for ensuring it has, and is complying with, the most recent version of HSX privacy policies as posted on the HSX website.
- Each Member is responsible for ensuring that it has developed and implemented appropriate and necessary internal procedures to allow it to comply in full with applicable laws and HSX privacy policies.
- In the event of a conflict between HSX policies and a Member's own policies, the Member shall comply with the policy that is more protective of individual privacy and security.

Review and Amending HSX Policies:

- HSX polices shall be regularly reviewed by the Privacy Officer, and monitored by the HSX Privacy and Security Workgroup with any recommendations for changes shall be made as appropriate.
- Final policies, including any amendments, shall be reviewed and approved in accordance with the HSX Board's applicable policies and bylaws for approval of the same.
- Beginning with such effective date, these polices shall be reviewed and amended at least once every 12 months, or sooner as needed.

4. Procedure

None

5. Enforcement

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

Participants and Members are responsible for ensuring compliance with this policy for their own entities.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.316, HIPAA § 164.530(h)

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	HSX Management Team; Privacy and Security Workgroup;	**Approval Date**	December 16, 2015
Date Policy In Effect	December 16, 2015	**Version #**	1.0
Original Issue Date	December 16, 2015	**Last Review Date**	December 4, 2022 September 30, 2021 September 17, 2020 December 22, 2016

Related Documents	Complaints Policy Glossary Information Security Management Program Policy Privacy Management Plan Privacy and Security Roles Policy Risk Management Policy