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

Privacy and Security Officer Roles

Version	Approval Date	Author
1.2	September 12, 2021	Privacy and Security Officer

1. Purpose

The purpose of this policy is to establish a transparent, coherent, and uniform principle for a consistent and coordinated approach to privacy and security roles for HealthShare Exchange (HSX) and its participants. Privacy and security challenges pertaining to electronic health information exchange (HIE) are addressed in this policy and are applicable regardless of the legal framework that may apply to a particular HSX participant. Roles and related responsibilities of individuals who hold and exchange HIE are stated and defined.

HIE is beneficial for individuals and the healthcare system as it improves care and reduces costs. It is a critical factor to establish and maintain trust in the electronic exchange of information so that healthcare consumers are willing to disclose necessary health information. HSX has an objective to achieve this high level of trust among healthcare consumers, providers, and HSX participants by developing and establishing adherence to a systematic approach to privacy and security.

2. Scope

This policy demonstrates the importance HSX places on privacy and security. It covers the regulatory framework and government mandates. It defines the purpose, objective, scope, standard, procedure, definitions, job description and assignment of responsibilities for implementation, and the associated guidelines.

3. Policy

The Health Insurance Portability and Accountability Act of 1996, (HIPAA) permits covered entities to disclose protected health information (PHI) to public health authorities that are legally authorized to receive such information. All individual PHI in the HIE will be available for public health and quality reporting. PHI shall not be used or disclosed for purposes other than those for which it was collected unless by expressed consent of the individual or as required by law. All disclosures and use of health information obtained through the HIE shall be consistent with all applicable

federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose.

Business associates may be authorized to access PHI for purposes consistent with lawful and ethical HIE, and business associates are subject to the same HIPAA privacy and security provisions and penalties that apply to covered entities.

HSX shall establish role based access standards to enable employees and contractors to only access PHI that is necessary for the performance of his or her authorized activities. In addition, only the minimal amount of information and least amount of privilege shall be granted to authorized employees to execute the job function.

Privacy Officer Role Description

The Privacy Officer is responsible for implementation and compliance of HSX's privacy policy, procedures, and programs.

HIPAA requires every practice or healthcare organization to designate a Privacy Officer. For HIPAA compliance, this role shall oversee all continuous activities relevant to development, implementation, and maintenance of the practice or organization's privacy policies in compliance with federal and state laws.

Responsibilities of the Privacy Officer

- Identify, implement, and maintain HSX privacy policy and procedures.
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Ensures delivery of privacy training and orientation to all permanent and temporary employees, volunteers, staff, and applicable business associates. Performs ongoing compliance and business associate agreements monitoring.
- Works with all HSX personnel involved with any aspect of release of PHI to ensure full adherence to policies, procedures, and legal requirements, and restrict access to PHI as appropriate.
- Works with legal counsel and the Chief Information Security Officer to maintain appropriate privacy and confidentiality consent & authorization forms, information notices and materials reflecting current HSX legal practices and requirements.
- Establishes and maintains a mechanism to track access to PHI, and as required by law to allow qualified individuals to review or receive a report on such activity.

- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the HSX privacy policy and procedures.
- Cooperates with the U.S. Department of Health and Human Service's Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Collaborates with the Pennsylvania eHealth Authority in ensuring that HSX' privacy policies are aligned with the Commonwealth.

Chief Information Security Officer Role Description

The Chief Information Security Officer is responsible for managing information security at HSX during development, transition, and production operations.

Senior-level executive at HSX held responsible for executing the organization's technology vision and directing strategies that ensure protection of organization-owned Information Technology (IT) assets and systems.

Responsibilities of the Chief Information Security Officer

- Approves and issues policies that ensure consistency with HIPAA, federal and state laws, and regulations.
- Combines technical with executive functions to build relationships and consensus for implementing security policies and programs that establish support for the President. Establishes security awareness and employee understanding as well as compliance to organization policies.
- Investigates, resolves, and develops processes, procedures, and documentation related to security of computers, systems, networks, and telecommunications in accordance with HIPAA, federal and state laws, regulations and standards, confidentiality, and HSX privacy policy. Lead investigator addressing health information security and privacy issues.
- Reviews and studies all information published by U.S. Department of Health and Human Service's Office of Civil Rights and other regulatory bodies relative to health information security and privacy.
- Develops and directs technical teams in the investigation and resolution of complex privacy and security issues.
- Ensure the confidentiality, integrity, and availability of information to authorized individuals, and direct and implement the necessary controls and procedures to protect organization-owned IT assets and systems from deliberate or inadvertent access, modification, disclosure, or destruction.

- Responds to incidents that include any suspected and/or confirmed breaches, manages security technologies, directs the implementation of policies and procedures, and establishes appropriate standards and controls.
- Ensures that all contracted third-party service providers maintain an appropriate cybersecurity program of its own commensurate with the type of service and accessible information.

4. Procedures

The President assigns the roles of Privacy Officer and Chief Information Security Officer to HSX Personnel.

5. Enforcement

The President sets the tone for the accountable and appropriate conduct in role execution for the Privacy Officer and Chief Information Security Officer.

6. Definitions

Privacy: An individual's interest in protecting their personal health information and the obligation of those involved in HIE to respect those interests through protected and fair practices.

Security: The physical, technological, and administrative safeguards used to protect individually identifiable health information.

7. References

Regulatory References:

- HIPAA Regulatory

Policy Owner	Privacy and Security Officer	**Contact**	Brian.Wells@healthshareexchange.org Don.Reed@healthshareechange.org
Approved By	Board HSX Management Team HSX Privacy and Security Workgroup	**Approval Date**	October 22, 2018
Date Policy In Effect	June 4, 2015	**Version #**	1.2
Original Issue Date	June 4, 2015	**Last Review Date**	December 4, 2022 September 30, 2021 September 15, 2020 June 7, 2017
Related Documents	Acceptable Use Policy Confidentiality Agreement Glossary Privacy and Security Training Policy Privacy and Security Compliance Agreement		