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

Compliance Policy

Version	Approval Date	Owner
1.0	May 15, 2017	Privacy Officer

1. Purpose

HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) has an obligation to comply with laws, regulations, policies, and standards to preserve the confidentiality, integrity, and availability of information assets owned by or entrusted to HSX. The purpose of this policy is to ensure HSX satisfies its legal and ethical responsibilities with regard to information assets.

2. Scope

This policy covers all HSX privacy 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

Compliance with Law:

- All disclosures of data through the HSX Health Information Exchange (HIE) and the use of information obtained from the HSX HIE shall be consistent with all applicable federal, state, and local laws and regulations, and shall not be used for any unlawful or unauthorized purpose.
- If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing data for a particular purpose, the requesting Member shall ensure that it has obtained the required documentation or met the requisite conditions, and shall provide evidence of the same at the request of HSX.
- All HSX employees, interns, contractors, members, participants, users, and third parties shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information.

- All HSX employees, interns, contractors, members, participants, users, and third parties shall be responsible for identifying and notifying the HSX Privacy Officer of any laws and/or regulations relating to the access use and/or disclose of data that may be specific to such Member and that are more stringent than HIPAA and HITECH.
- All HSX employees, interns, contractors, members, participants, users, and third parties shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of all laws and regulations that may affect their use and disclosure of data, and shall inform HSX of any such changes of which it becomes aware.

Intellectual Property Rights:

- HSX shall develop and implement intellectual property rights procedures to ensure compliance with legislative, regulatory, and contractual requirements including copyrights, design rights, or trademarks that may place restrictions on the copying of proprietary material.
- HSX shall develop controls for the use of software products, both purchased and proprietary.
- HSX shall develop and enforce explicit rules governing the installation of software by users.

Protection of Organizational Records:

- HSX shall protect organizational records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
- HSX shall ensure that Protected Health Information (PHI) is safeguarded for a period of seven (7) following the death of the individual.
- HSX shall document compliance with notice requirements by retaining copies of the notices for a period of seven (7) years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement.
- HSX shall document restrictions in writing and formally maintain such writing, or an electronic copy of such writing, as an organizational record for a period of seven (7) years.
- HSX shall document and maintain the designated record sets that are subject to access by individuals, and the titles of the persons or office responsible for receiving and processing requests for access by individuals, as organizational records for a period of seven (7) years.

Documentation and Record Retention:

- HSX shall maintain, until seven (7) years after the later of the date of their creation or last effective date, its policies and procedures, its privacy practices notices,

disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

- HSX must:
    - Maintain privacy policies and procedures in written or electronic form;
    - If a communication is required to be in writing, maintain such writing, or an electronic copy, as documentation; and
    - If an action, activity, or designation is required to be documented, maintain a written or electronic record of such action, activity, or designation.

HSX shall document and maintain accountings of disclosure as organizational records for a period of seven (7) years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting.

4. Procedure

None

5. Enforcement

- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- The HSX 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)(1)(ii)(C), HIPAA § 164.308(a)(1)(ii)(D), HIPAA § 164.308(a)(2), HIPAA § 164.308(a)(8), HIPAA § 164.310(b), HIPAA § 164.414(a), HIPAA § 164.502(f), HIPAA § 164.520(e), HIPAA § 164.522(a)(3), HIPAA § 164.524(e), HIPAA § 164.528(d), HIPAA § 164.530(a), HIPAA § 164.530(j)

- HITRUST Reference: 06.a Identification of Applicable Legislation, 06.b Intellectual Property Rights, 06.c Protection of Organizational Records, 06.d Data Protection and Privacy of Covered Information, 06.e Prevention of Misuse of Information Assets, 06.g Compliance with Security Policies and Standards, 06.h Technical Compliance Checking
- PCI Reference: PCI DSS v3 12.3.1
- PA eHealth Reference: 1.0. HIPAA Compliance

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	May 15, 2017
Date Policy In Effect	May 15, 2017	**Version #**	1.0
Original Issue Date	May 15, 2017	**Last Review Date**	September 17, 2020 May 15, 2017
Related Documents	Acceptable Use Policy Encryption Policy Glossary Media Protection Policy Sanctions Policy Participation Agreement		