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

Business Associate Privacy Policy

Version	Approval Date	Owner
1.0	July 28, 2015	Privacy Officer

1. Purpose

To ensure the legitimate access and use of Data by HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) as a HIPAA Business Associate of Covered Entities and to extend the same requirements to Sub-contractors of HSX.

2. Scope

This policy covers all HSX privacy practices across all departments and business units including consulting arrangements. All HSX HIPAA Business Associates are required to comply with this policy.

3. Policy

HSX as a HIPAA Business Associate:

- HIPAA-compliant Business Associate Agreements (BAA) shall be executed when required under HIPAA and HITECH and applicable law.
- HSX as a Business Associate is responsible for reporting any breach to a covered entity as per an executed BAA.
- HSX takes seriously its obligations and responsibilities for operations of the HSX Health Information Exchange (HIE). The HIE technology and HIE services (collectively known as "Services") are made available to HSX Members and Participants through executed Participation Agreements.
- In connection with performing Services, HSX shall sign a BAA with each Member/Participant of the HIE, and in its role as a Business Associate will limit its access to and use of any Data that a Member/participant may have supplied or made available to HSX to the following purposes only:
    - Testing functionality of the Member/Participant's connection to HSX, including interfaces;
    - Troubleshooting HSX technology-related issues;

  - Auditing for compliance with policies;
  - Data analyses and reporting in compliance with approved use cases and HIE Services.
  - Facilitating security and privacy incident and breach investigations; and
  - Any other Services that a Member/Participant may specifically request HSX to perform on the Member/Participant's behalf which require HSX's access to or use of Member/Participant's Data, to the extent permitted under applicable law.
  - If any of the Services requested are broader than those listed, then a written addendum to the Participation Agreement shall be signed by the Member/Participant and by HSX before HSX performs any such expanded Services on behalf of a particular Member/Participant.
  - As a Business Associate, HSX and its vendors would need to respond in a legally appropriate and timely manner in the event of a breach.
- HSX shall implement adequate technical, administrative and physical safeguards in accordance with HSX policies to prevent employees, interns, consultants, third parties and contractors engaged in performing Services for Members/Participants from disclosing any Data to others at HSX who have no role or responsibilities in connection with performing Services for Members/Participants.

Sub-Contractors of HSX:

- All Sub-Contractor arrangements requiring the use or disclosure of Protected Health Information (PHI) shall be reviewed, approved and documented by the Chief Information Security Officer (CISO) and/or Privacy Officer.
- In dealing with Sub-Contractors, HSX shall allow a Sub-Contractor to create or receive PHI on its behalf. However, HSX shall ensure that an appropriate BAA is executed under the direction of HSX legal counsel for an arrangement with a Sub-Contractor unless the Sub-contractor is deemed an agent of HSX.
- Sub-Contractors that are deemed to be agents of HSX will be required to execute a Confidentiality Agreement that binds the individual to all the HSX privacy and security policies and procedures.
- HSX shall not enter into any Sub-Contractor Agreement, addendum or other amendment unless approved by the Executive Director and Legal Counsel. The approved Sub-Contractor Agreement may not be negotiated or modified in any way without the approval of the Executive Director and Legal Counsel.
- Sub-Contractor would have to require the same restrictions and responsibilities as covered by the HSX BAA to any designees.

4. Procedure

None

5. Enforcement

- The CISO and Privacy Officer shall be responsible for ensuring compliance with this policy under the direction of the Executive Director.
- If HSX becomes aware of a pattern of activity or practice violating the satisfactory assurances the Sub-Contractor has provided to HSX, the Sub-Contractor shall be deemed non-compliant with the agreement, and immediate action shall be taken by HSX to cure or end the violation.
- Violations of the terms of the Sub-Contractor Agreement must be immediately reported to the Privacy Officer. If measures taken to end the violation are unsuccessful, the feasibility of terminating the Sub-Contractor Agreement shall be considered. If termination is not feasible, the violation shall be reported to the Secretary of Health and Human Services (HHS) by HSX.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.502(e), HIPAA § 164.504(e), HIPAA § 164.504(g)
- HITRUST Reference: 13.n Organizational Requirements

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	Board HSX Management Team HSX Privacy and Security Workgroup	**Approval Date**	July 28, 2015
Date Policy In Effect	July 8, 2015	**Version #**	1.0
Original Issue Date	July 8, 2015	**Last Review Date**	December 3, 2022 September 29, 2021 September 17, 2020 December 22, 2016
Related Documents	Business Associate Agreement (BAA) Confidentiality Agreement Glossary Information Security Management Program Policy Participation Agreement Third Party Risk Management Policy		