Information Asset Management Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>May 15, 2017</td>
<td>Daniel Wilt</td>
</tr>
</tbody>
</table>

1. Purpose

To establish requirements for management of information assets. The recording, documenting, classifying, and maintenance of information assets is critical for protecting the confidentiality, integrity, and availability of confidential data.

2. Scope

This policy addresses all information assets that are utilized at HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX). All employees, interns, contractors, members, participants, users, vendors, and third parties who have access or exposure to HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) data and use HSX assets are required to comply with this policy.

3. Policy

Information Asset Management Policy:

- HSX information assets belong to HSX, which possesses the exclusive right to manage and direct actions regarding those information assets in accordance with organization policies and procedures so long as asserting and exercising this right does not conflict with federal or state law or regulations.
- No expectation of privacy exists regarding HSX information assets in accordance with organization policies and procedures, excepting privacy rights explicitly protected according to federal or state law or regulation, or in HSX policies and procedures, e.g., privacy of PHI protected under HIPAA, etc.
- Enterprise data contained on HSX systems are the sole property of the members. Employees and contractors do not own or have rights to enterprise data outside of its use in the performance of their HSX duties.
HSX employees, interns, third parties and contractors will safeguard and protect HSX information assets. HSX information assets are vital for the fulfillment of the business needs of HSX Health Information Exchange (HIE) Members. In order to ensure a reasonable and dependable level of access and service, it is essential that each individual exercise responsible, ethical behavior when using information assets. Misuse of HSX’s information assets has the potential to disrupt HSX’s business operations.

Inventory of Information Assets:

- All information assets shall be clearly identified and an inventory of all information assets drawn up and maintained.
- Scans must be conducted on a periodic basis to identify new hardware information assets that have been added to the network. Reports must be generated to provide visibility into information asset inventory changes over time.
- The information asset inventory must include information necessary to recover from a disaster, including type of information asset, format, location, backup information, license information, and business value.
- All activities and documentation associated with creating an information asset inventory shall be performed in such a manner that evidence of the activity can be reviewed by auditors.

Ownership of Information Assets:

- The information asset owner shall be assigned, at a minimum, the responsibility for creating, updating, and removing information assets from the information asset inventory.

Acceptable Use of Information Assets:

- Rules for the acceptable use of information assets shall be identified, documented within the Participation Agreement.

Classification Guidelines:

- Information assets shall be classified in terms of their value, legal requirements, sensitivity, and criticality to the organization.

Data Labeling, Handling and Storage:

- Policies and procedures must be developed for managing the secure acquisition, use, transfer, exchange, and disposal of all HSX information assets.
- An appropriate policy and associated procedures for data labeling, handling, and storage shall be developed and implemented in accordance with the Data Classification Policy.
- Asset tags shall be used to track each non-data information asset.
4. Procedure

None

5. Enforcement

- The CISO 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 §164.310(b), HIPAA §164.310(c), HIPAA §164.310(d)(1), HIPAA §164.310(d)(2)(iii)
- HITRUST Reference: 07.a Inventory of Assets, 07.b Ownership of Assets, 07.c Acceptable Use of Assets, 07.d Classification Guidelines, 07.e Information Labeling and Handling
- PCI DSS v3 11.1.1, PCI DSS v3 12.3, PCI DSS v3 12.3.3, PCI DSS v3 12.3.4, PCI DSS v3 12.3.5, PCI DSS v3 2.4, PCI DSS v3 9.7.1, PCI DSS v3 9.9, PCI DSS v3 9.9.1

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Contact</th>
<th>Security Officer</th>
<th>Approval Date</th>
<th>Daniel Wilt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By</td>
<td></td>
<td>HSX Management</td>
<td>May 15, 2017</td>
<td></td>
</tr>
<tr>
<td>Date Policy In Effect</td>
<td></td>
<td>May 15, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Original Issue Date</td>
<td></td>
<td>May 15, 2017</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Last Review Date: May 15, 2017
<table>
<thead>
<tr>
<th>Related Documents</th>
<th>Acceptable Use Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Classification Policy</td>
</tr>
<tr>
<td></td>
<td>Data Handling, Labeling, and Storage Policy</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
</tr>
</tbody>
</table>