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

Data Classification Policy

Version	Approval Date	Owner
1.1	November 8, 2019	Chief Information Security Officer

1. Purpose

To support HealthShare Exchange (HSX) policies on information asset management by establishing a framework for classifying data in the possession of HSX and by defining the baseline security controls for handling and safeguarding information assets.

The goal of this policy is to classify data into easily understandable and meaningful categories. The resulting data classification categories determine which HSX data requires special protection safeguards, security controls, and risk reduction measures.

2. Scope

This policy applies to all electronic and hardcopy data that is generated or used as part of HSX's business operations. This policy covers all HSX data regardless of where the information is stored, including HSX owned or managed systems or on a third party-hosted service. All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX data are required to comply with this policy.

3. Policy

Data Classification Policy:

- All HSX data shall be classified into one of three sensitivity levels (tiers):
    - Tier 1: Confidential Data
    - Tier 2: Internal Use Only Data
    - Tier 3: Public Data

Tier 1: Confidential Data:

- All HSX HIE applications/services shall be classified as Tier 1

- Data shall be classified as confidential data when the unauthorized disclosure, alteration or destruction of that data causes a significant level of risk. Confidential data is always sensitive.
- The highest level of security controls shall be applied to confidential data. Access to confidential data must be controlled from creation to destruction. Access will only be granted to those persons who require such access in order to perform their job ("need-to-know") in accordance with the principle of least privilege. Access to confidential data must be authorized by the data owner who is responsible for the data.
- Based on state, federal, and contractual requirements data will be classified appropriately based on the required protections
- Protected health information (PHI) defined in accordance with the HSX Business Associate Agreement shall be defined as confidential data and must be protected.

Tier 2: Internal Use Only Data:

- Data shall be classified as internal use only data when the unauthorized disclosure, alteration or destruction causes a low-to-moderate level of risk. Internal use only data is not for release to the general public. Internal use only data is always sensitive.
- A reasonable level of security controls shall be applied to internal use only data.
- By default, all data that are not explicitly classified as confidential data or public data shall be treated as internal use only data.
- Access to internal use only data must be authorized by the data owner who is responsible for the data. Access to internal use only data may be authorized to groups of persons based on job classification or responsibilities ("role-based" access).

Tier 3: Public Data:

- Data shall be classified as public data when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk. Public data is not sensitive but does require a data owner.
- While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.
- As public data is not considered sensitive, access may be granted to any requester or published with no restrictions.
- The integrity of public data shall be protected and the data owner will take measures to ensure public data remains accurate over time.

Data Collections:

- Data owners may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements shall be used to classify the entire body of data as a whole.

Examples of Data Classifications:

<table>
<tr><th>Tier 1: Confidential Data</th><th>Tier 2: Internal Use Only Data</th><th>Tier 3: Public Data</th></tr>
<tr><td>Data protected by state or federal regulations including:
Protected Health Information (PHI)
Personally Identifiable Information (PII)
Social Security Numbers (SSN)
Financial Account Data</td><td rowspan="3">Internal company newsletters
Training program materials
Project plans / documentation
Operations meeting notes
Operations policies and procedures
Employee Handbook</td><td rowspan="3">Provider directory information
Course information
Public event information
Research publications
Member policies
Web content
HSX posts on social media
Advertising
Print collateral
Professional and public presentations</td></tr>
<tr><td>Data protected by confidentiality agreements, including:
Employee personnel records
Non-Disclosure Agreements (NDA).</td></tr>
<tr><td>Internal HSX information that must be protected from unauthorized internal or external disclosure, including:
Merger / acquisition sensitive info
Financial reports and budget information
Sensitive Executive Officer correspondence or information</td></tr>
</table>

Tier 1: Confidential Data	Tier 2: Internal Use Only Data	Tier 3: Public Data
• Board and Executive Committee Minutes • Incident Reports • Intellectual property • Credentialing information (e.g., credentials, password data) that grants access to systems storing sensitive data • Legal products, including contracts, agreements, legal correspondence and data that is subject to attorney-client privilege		
Legal hold data that are the subject of (or are anticipated to be the subject of) any type of investigation and/or legal proceeding		

4. Procedure

None

5. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- The CISO and 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)(A), HIPAA §164.308(a)(1)(ii)(B)
- HITRUST Reference: 07.d Data Classification Guidelines

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	November 8, 2019
Date Policy In Effect	May 25, 2017	**Version #**	1.1
Original Issue Date	May 25, 2017	**Last Review Date**	September 16, 2020 November 8, 2019
Related Documents	Access Control Policy Business Associate Agreement Compliance Policy Data Handling, Labeling, and Storage Policy Glossary Information Asset Management Policy		