HealthShare Exchange

190 N. Independence Mall West | Suite 701 | Philadelphia, PA 19106 | www.healthshareexchange.org | 215-391-4905

Data Handling, Labeling, and Storage Policy

Version	Approval Date	Owner
1.2	September 1, 2019	Chief Information Security Officer

1. Purpose

To establish handling, labeling and storing policies for HealthShare Exchange (HSX) enterprise data in order to protect this data from unauthorized disclosure or misuse.

2. Scope

This policy covers all HSX enterprise data and the associated meta-data where federal or state regulations exists, and data where external contract requirements exists regardless of whether the data is stored on a HSX owned or managed system 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 Handling, Labeling, and Storage Policy:

- All HSX enterprise data shall be handled, labeled, and stored in accordance with this policy.
- Data handling shall be based upon its data classification according to the *Data Classification Policy*.
- Any data covered by federal or state laws or regulations or contractual agreements must also meet the security requirements defined by those laws, regulations, or contracts in addition to the requirements of this policy.

- As per the HSX Participation Agreement (PAR 17.17), all facilities processing, transmitting and storing Data shall be restricted to be geographically located within the United States of America.
- All covered information storage shall be kept to a minimum. Per HSX business operations, minimum data is defined as including but not limited to all elements referenced in the *Data Classification Policy*.

The following table specifies the minimum security controls for HSX

- Tier 1: Confidential Data
- Tier 2: Internal-Use-Only Data
- Tier 3: Public Data:

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
Access Controls	Viewing and modification restricted to authorized individuals as needed for business-related roles (need to know and minimum necessary). Data owner or designee grants permission for access. Requires approval from CISO or Executive Director. Authentication and authorization required for access. Confidentiality agreement or Non-Disclosure Agreement (NDA) required.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data owner or designee grants permission for access. Requires approval from HSX Management Team Authentication and authorization required for access.	No restrictions for viewing. Authorization by data owner or designee required for modifications; CISO and Executive Director approval required if not a self-service function.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
Auditing	Logins, access and changes.	Logins	Not required
Backup and Disaster Recovery	Daily backups required. Off-site storage in a secure location required.	Daily backups required. Off-site storage recommended.	Backups required; daily backups recommended.
Copying and Printing Applies to both paper and electronic forms	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and who have signed a confidentiality agreement or who have an NDA. Data must not be left unattended, such as on a printer, fax, desktop, or any public location. Copies must be conspicuously labeled "Confidential". If sent via internal mail, must be must be marked "Confidential".	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data must not be left unattended on a printer, fax, desktop, or any public location. May be sent via Internal Mail.	No restrictions.
Data Storage	Storage on a secure server required. Storage in secure data center required.	Storage on a secure server recommended. Storage in a secure data center recommended.	Storage on a secure server recommended. Storage in a secure data center recommended.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	Should not store on an individual workstation or mobile computing device (e.g., a laptop computer). If stored on a workstation or mobile computing device, that device must use whole-disk encryption. Encryption on backup media required. Paper or hard copy: do not leave unattended where others may see it; store in a secure location for example a locked file cabinet.	Should not store on an individual's workstation or a mobile computing device (e.g., a laptop computer). If stored on a workstation or mobile computing device, that device must use whole-disk encryption.	
Media Sanitization and Disposal hard drives, CDs, DVDs, tapes, paper, etc.	Shred reports. Destroy electronic media at end of life.	Recycle reports. Wipe and erase media.	No restrictions.
Mobile Computing Devices	Password protected, locked when not in use, Encryption required. Remote delete capability of confidential data by HSX required.	Password protected, locked when not in use.	Password protection recommended, locked when not in use

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
Network Security	Protection with a network firewall using "default deny" (Deny All, Permit by Exception [DAPE]) rule set required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data must not be visible to the entire Internet, nor to unprotected subnets like the guest wireless networks. Logical and/or physical network partitioning of confidential data from other types strongly recommended. Must have a firewall rule set dedicated to the system. The firewall rule set must be reviewed periodically.	Protection with a network firewall required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data must not be visible to the entire Internet. May be in a shared network server subnet with a common firewall rule set for the set of servers.	May reside on a public network. Protection with a firewall recommended. IDS/IPS protection recommended. Protection only with router ACLs acceptable.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
Physical Security	Computing devices must be locked or logged out when unattended. Hosted in a secure data center required. Physical access must be monitored, logged, and limited to authorized individuals 24x7.	Computing devices must be locked or logged out when unattended. Hosted in a secure location required; a secure data center is recommended.	Recommend that computing devices be locked or logged out when unattended. Host-based software firewall recommended.
Remote Access to systems hosting the data	Access restricted to local network or https. Unsupervised remote access by third party for technical support not allowed.	Access restricted to local network or https. Remote access by third party for technical support limited to authenticated, temporary access via secure protocols over the Internet.	No restrictions.
System Security	Must follow HSX-specific and Operating System (OS)-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended.	Must follow HSX-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended.	Must follow general best practices for system management and security. Host-based software firewall recommended.
Training	General security awareness and HIPAA training required.	General security awareness and HIPAA training required.	General security awareness and HIPAA training recommended.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	Data security training required. Applicable policy and procedure training required.	Data security training required.	
Transmission	Encryption required (e.g., SSL or secure file transfer protocols) in accordance with the *Encryption Policy*. Cannot transmit via email unless encrypted and secured with a digital signature.	No requirements.	No restrictions.
Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Cannot share the same virtual host environment with guest virtual servers of other security classifications.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Should not share the same virtual host environment with guest virtual servers of other security classifications.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.

4. Procedure

The following procedures apply to HSX internal operations only:

- Data Handling, Labeling, and Storage Procedure
- Encryption Procedure

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)(3)(ii)(A), HIPAA § 164.310(b), HIPAA § 164.310(c), HIPAA § 164.310(d)(1), HIPAA § 164.310(d)(2)(iv), HIPAA § 164.312(c)(1)
- HITRUST Reference: 09.q Information Handling Procedures
- PCI Reference: PCI DSS v3 3.2, PCI DSS v3 3.2.1, PCI DSS v3 3.2.2, PCI DSS v3 3.2.3, PCI DSS v3 3.3, PCI DSS v3 9.5, PCI DSS v3 9.6, PCI DSS v3 9.6.3, PCI DSS v3 9.7

Policy Owner	Chief Information Security Officer	**Contact**	brian.wells@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	September 1, 2019
Date Policy In Effect	September 1, 2019	**Version #**	1.2

Original Issue Date	May 15, 2017	**Last Review Date**	October 24, 2023 December 3, 2022 September 29,2021 September 17, 2020 September 15, 2019
Related Documents	Data Classification Policy Change Management Policy Encryption Policy Glossary		