HealthShare Exchange

190 N Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareecxchange.org

Data Handling, Labeling, and Storage Procedures

Version	Approval Date	Owner
1.3	December 18, 2019	Chief Information Security Officer

I. Purpose of Procedure

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

II. Procedure Scope

These procedure 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 these procedures.

III. Definitions

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

IV. Procedures

A. The following table specifies the minimum security controls for HSX

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	Viewing and modification restricted to authorized individuals as needed for business-related roles.	No restrictions for viewing. Authorization by data owner or designee required for modifications; CISO and Executive Director approval

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	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.	Data owner or designee grants permission for access. Requires approval from HSX Management Team Authentication and authorization required for access.	required if not a self-service function.
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. Backups may either be stored on a separate server located in the cloud or at Off-site storage.	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. Rights to copy or print confidential data are granted by the HSX CISO by exception to individuals who are also authorized to access the data and who have signed a confidentiality agreement or who have an NDA and who have submitted a Policy Exception Request Form that is approved by the HSX CISO. The HSX Engineering Team	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know and are granted copying rights by exception The HSX Engineering Team and HSX Enterprise Project Management Office (EPO) are hereby granted permission to copy data in the performance of their duties and responsibilities. Data must not be left unattended on a printer, fax,	No restrictions.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	and HSX Enterprise Project Management Office (EPO) are hereby granted permission to copy data in the performance of their duties and responsibilities. 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".	desktop, or any public location. May be sent via Internal Mail.	
Data Storage	Storage on a secure server required located in a facility located in the United States Storage in secure data center required located in the United States. 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.	Storage on a secure server recommended. Storage in a secure data center recommended. Should not store on an individual's workstation or a mobile computing device (e.g., a laptop computer). However, if temporary storage is required on a workstation for a specific technical support purpose approved by the HSX CISO, then such minimally necessary data may be temporarily copied to a	The placement of any information onto a publicly accessible information system requires approval by the HSX President and /or Chief Operating Officer. Storage on a secure server recommended. Storage in a secure data center recommended. Storage on a secure server recommended.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	Paper or hard copy: do not leave unattended where others may see it; store in a secure location for example a locked file cabinet. As soon as the data is known to be unneeded, it must be deleted. Hold a quarterly review of data entering this category and log in operations checklist.	designated workstation with whole-disk encryption. It is expressly required that such data be removed immediately after the intended use is completed. PHI may never be stored on a BYOD device.	Storage in a secure data center recommended.
Media Sanitization and Disposal hard drives, CDs, DVDs, tapes, paper, etc.	Shred reports. Destroy electronic media at end of life. Unneeded protected data on shared device with necessary protected data should be wiped over 3 times with random data.	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. Documents, files and other data should be saved to HSX Onedrive.	Password protection recommended, locked when not in use
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 a network firewall required. IDS/IPS protection required. Protection with router ACLs optional.	May reside on a public network. Protection with a firewall recommended. IDS/IPS protection recommended.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	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.	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.	Protection only with router ACLs acceptable.
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	No restrictions.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
		access via secure protocols over the Internet.	
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. Data security training required. Applicable policy and procedure training required.	General security awareness and HIPAA training required. Data security training required.	General security awareness and HIPAA training recommended.
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. Confidential data may not be printed or otherwise obtained and mailed via any other "snail mail" mail service (e.g., USPS, FedEx, UPS or any other similar service)	No requirements.	No restrictions.

Security Control Category	Tier 1 Confidential Data	Tier 2 Internal Use Only Data	Tier 3 Public Data
	Data may not be transmitted outside of the United States Unless approved by exception by HSX CISO. Such approval shall be requested and approved through the HSX Exception Form.		
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.

1. **All covered information is encrypted when stored. See Encryption Procedure and above stipulations. Any exceptions need to proceed through the Change Management Procedure and be approved by the CISO.**
2. **All covered information storage is kept to the minimum per HSX business operations through the following process:**
    1. HSX will only receive data included within the *Data Elements in the CDR* document unless approved by Technical Operations and/or the Privacy and Security Officers.
    2. This list will be reviewed and maintained by Technical Operations.
3. **Copy, move, print (and print screen), and storage of sensitive data is prohibited when accessed remotely without a defined business need by the following procedure:**
    3. The HSX system does not limited factors based on location as HSX information is always "remote" in that HSX functionality is cloud-based.
    4. CISO must grant permission and document when changes occur.
    5. HSX employees are required to follow HSX Remote Access and Teleworking Policies and attest to doing so.
4. Protected Information

6. HSX shall ensure patient information subject to special handling, e.g., HIV test results and mental health and substance abuse-related records, is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines.

Responsible Owner:	Security Officer	**Contact: email**	Brian.Wells@healthshareexchange.org
Approved By:	Brian Wells	**Version #**	1.3
Current Approval Date:	December 18 2019	**Prior Reviews**	October 27, 2023 December 6, 2022 October 5, 2021 October 17, 2020 December 18, 2019 September 15, 2019 December 1, 2018 May 15, 2017
Date Procedure to go into Effect:	December 18, 2019		
Related Documents:	Data Handling, Labeling, and Storage Policy Data Classification Policy Change Management Policy Encryption Policy Remote Access Policy Teleworking Policy Glossary		