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

Media Protection Policy

Version	Approval Date	Owner
1.1	September 28, 2017	Chief Information Security Officer

1. Purpose

The purpose of this policy is to protect all HealthShare Exchange (HSX) media containing confidential data in both paper and digital format, to ensure destruction before disposal, and to ensure compliance with federal and state laws and regulations concerning the security and privacy of confidential data copied onto removable media.

2. Scope

This policy applies to all media, removable media, and paper media containing HSX confidential data regardless of physical location.

3. Policy

Media Protection Policy:

- HSX shall physically and logically protect media and paper media containing confidential data while at rest, stored, or actively being accessed.
- HSX shall develop and implement processes and procedures for implementing the *Media Protection Policy*.
- HSX shall identify media requiring restricted use.
- HSX shall define and implement safeguards necessary to restrict access to, use of, and protection of media.
- Media containing diagnostic and test programs shall be checked for malicious code prior to use.

Data Exchange Policies and Procedures:

- HSX data shall be classified according to the *Data Classification Policy*.

- HSX shall develop and implement retention and disposal procedures and guidelines for all HSX confidential data in any format including media and paper media, in accordance with relevant federal, state, and local legislation and regulations.
- HSX shall restrict access of media and paper media containing confidential data according to the *Access Control Policy*.
- HSX shall limit the use of media on externally-located physical information assets (e.g., laptops, tablets, cameras, and smartphones) to authorized employees and contractors.

Management of Removable Media:

- HSX shall develop and implement processes and procedures for the management of removable media.
- HSX shall restrict the types and use of removable media to maintain security of confidential data.
- HSX shall require the registration of any information asset containing removable media before use.
- Removable media shall be encrypted in accordance with the *Encryption Policy*.
- Removable media shall be handled, labeled and stored in accordance with the *Data Handling, Labeling, and Storage Policy* in addition to this policy.

Media and Paper Media Transport and Storage:

- HSX shall physically control and securely store media and paper media within a controlled area such as a locked drawer, cabinet or room.
- HSX shall protect and control all media and paper media during transport outside of controlled areas to prevent unauthorized access or use.
- HSX shall maintain accountability for all media and paper media during transport outside of controlled areas.
- HSX shall restrict the transport of media and paper media outside of controlled areas to authorized personnel.
- HSX shall document all activities associated with the transport of media and paper media.
- All media backups must be encrypted and marked with the backup frequency (daily, weekly, monthly). Every media backup must have separate encryption key that must be kept in a fire-proof safe.
- HSX shall employ cryptographic mechanisms to protect the confidentiality and integrity of media during transport outside of controlled areas according to the *Encryption Policy*.
- If a third party is responsible for transporting backup media offsite, they shall be responsible for maintaining security according to the *Third Party Risk Management Policy*.

Secure Disposal of Media and Paper Media:

- Media and paper media shall be disposed of securely and safely when no longer needed according to the *Data and Media Sanitization Policy*.
- HSX shall maintain a log and an audit trail of media and paper media disposal activities according to the *Data and Media Sanitization Policy*.

4. Procedure

The following procedures apply to HSX internal operations only:

- Data and Media Sanitation Procedure
- Data Transfer Procedure
- Encrypting and Securing Devices Procedure
- Encrypting and Tracking Data Procedure
- Encryption Procedures
- How to Access ENS Server Procedure
- HSX IT Inventory Procedure
- Sensitive Media Outside Controlled Locations Procedure

5. Enforcement

- 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 §164.310(c), HIPAA §164.310(d)(1), HIPAA §164.310(d)(2)(i), HIPAA §164.310(d)(2)(ii), HIPAA §164.310(d)(2)(iii), HIPAA §164.310(d)(2)(iv), HIPAA §164.312(c)(1)
- HITRUST Reference: 09.o Management of Removable Media, 09.p Disposal of Media, 09.s Information Exchange Policies and Procedures
- PCI Reference: PCI DSS v1.2 9.8, PCI DSS v3 9.8

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Board HSX Management Team	**Approval Date**	September 28, 2017
Date Policy In Effect	May 26, 2015	**Version #**	1.1
Original Issue Date	May 26, 2015	**Last Review Date**	September 16, 2020 December 1, 2018 September 28, 2017
Related Documents	Access Control Policy Data and Media Sanitization Policy Data Classification Policy Data Handling, Labeling, and Storage Policy Encryption Policy Glossary Third Party Risk Management Policy		