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

Data and Media Sanitization Policy

Version	Approval Date	Owner
1.1	November 8, 2018	Chief Information Security Officer

1. Purpose

The purpose of the policy is to protect HealthShare Exchange (HSX) confidential data from unauthorized access or use by establishing proper sanitization of media, paper media, removable media, business mobile computing devices, and information assets.

The purpose of the procedures is to guide employees, consultants, interns, subcontractors, and vendors of HSX through the use of standardized tools and processes to securely sanitize data and hard disks of computers that are being:

- Disposed of data and media drive that is no longer needed
- Stored in Cloud Services or Hosted that is no longer needed
- Reassigned to other individuals

This is necessary to reduce the possibility of inappropriate exposure of data and unauthorized use.

2. Scope

The policy applies to all media, paper media, removable media, business mobile computing devices, data storage devices within end-user computers, servers, copiers, appliances, fax machines and other information assets that either belong to HealthShare Exchange and contracted vendors.

The process applies to all employees, consultants, interns, subcontractors, and vendors of HSX who shall be fully responsible for ensuring storage data and media including, but not limited to, hard drives that have been sanitized or destroyed prior to asset disposition or internal reassignment or in cloud services.

3. Policy

HealthShare Exchange shall sanitize all media, paper media, removable media, business mobile computing devices, and information assets prior to disposal, release outside of organizational control, or release for reuse in order to render confidential data permanently non-retrievable by any means:

- Determination of whether confidential data contained on HealthShare Exchange media, paper media, removable media, business mobile computing devices, and information assets must be retained prior to disposal, release out of organizational control, or release for reuse shall be made by the data owner.
- HealthShare Exchange shall develop sanitization processes and procedures that include removing and securing confidential data and permanently destroying media, paper media, removable media, business mobile computing devices, and information assets prior to disposal, release out of organizational control, or release for reuse.
- HealthShare Exchange shall develop processes and procedures for submitting media, paper media, removable media, business mobile computing devices, and information assets for sanitization.
- Only authorized employees, contractors, and third parties shall complete sanitization processes and procedures.
- HealthShare Exchange shall maintain a log of all sanitization activities.
- Authorized third party vendors shall be required to provide a certificate of destruction to account for all media, paper media, removable media, business mobile computing devices, and information assets they destroy.
- Re-formatting is not approved nor authorized as a singular, stand-alone means of sanitizing media, removable media, business mobile computing devices, and information assets, as re-formatting does not permanently overwrite the data.

Secure Disposal or Re-Use of Information Assets:

- All information assets that are hardware shall be checked to ensure that all confidential data and licensed software has been removed and secured prior to re-use or release outside of organizational control.
- All information assets being permanently taken out of service shall be removed from the information asset inventory according to the *Information Asset Management Policy*.
- All information assets that are hardware or software and that are being taken out of service shall be destroyed either by an authorized third-party vendor or by other means such as drilling, crushing or other demolition methods that render any and all confidential data on the information asset non-retrievable by any means.

Secure Disposal or Re-Use of Media and Removable Media:

- All media and removable media shall be checked to ensure that all confidential data and licensed software has been securely removed prior to re-use or release outside of organizational control.
- All media and removable media being taken out of service shall be destroyed either by an authorized vendor or by other means such as degaussing, using a commercially available disk cleaning program, drilling, crushing or other demolition methods that render the confidential data non-retrievable by any means.
- Where HealthShare Exchange is using removable media for the purpose of system backups and disaster recovery, and the removable media is stored and transported in a secure environment in accordance with the *Media Protection Policy*, the use of a data destruction tool between uses is not necessary.

Secure Disposal of Paper Media:

- Paper media containing confidential data shall be kept in locked bins until destruction.
- Paper media containing confidential data shall be destroyed either by an authorized vendor or other methods such as cross-cut shredding, disintegration, incineration, and pulverization.
- Department managers shall be responsible for overseeing secure disposal of paper media in their area.

4. Procedures

When electronic computing devices or electronic storage media are to be transferred or surveyed, unless an agreement between HSX and a vendor sets forth another method of destruction or sanitation, HSX or vendor personnel, as appropriate, shall complete the following steps:

- All electronic computing devices or electronic storage media must be overwritten using approved and validated overwriting technologies/methods/tools without exception.
- Only instances involving an inoperable hard drive that cannot be cleared will require its removal from the electronic computing device in order to ensure proper destruction.
- Inoperable electronic computing devices and/or electronic storage media must be isolated and secured until properly destroyed. These devices will be destroyed using a degausser.
- The designated staff or vendor must complete and sign a Data and Media Sanitization Certification Form for the item(s) to be transferred or surveyed.

- The Media Sanitization Certification must be submitted to HSX.

Upon approval, the item(s) may then be transferred or disposed of.

Standard Procedure

To protect the confidentiality of information and the related privacy rights of HSX and its members and participants, and the privacy and security of their patients. HSX must ensure that electronic data in its possession is secure at all times. When electronic computing devices and/or electronic storage media are removed from service, all electronic data must be properly sanitized prior to release of custody. The sanitization process ensures that recovery of information is not possible and that information security objectives are not compromised. Several methods can be used to sanitize media; however, the two major types of sanitization are *clearing* and *destroying.*

Clearing information is a level of media sanitization that protects the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities and must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing media. The security goal of overwriting is to replace written data with random data. There are several overwriting software products to overwrite storage space on media. Various services provide software tools and instructions to securely clean the data from electronic storage media. Overwriting cannot be used for media that is damaged or not rewritable. In such cases, electronic media should be destroyed.

When electronic media is inoperable and cannot be cleared, the electronic media must be physically destroyed. While physical destruction can be accomplished using a variety of methods, a degausser for destruction of hard drives and a shredder for the destruction of other electronic media is preferred.

5. Enforcement

- The Chief Information Security Officer (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(d)(1), HIPAA §164.310(d)(2)(i,), HIPAA §164.310(d)(2)(ii)
- HITRUST Reference: 08.l Secure Disposal or Re-Use of Equipment
- PCI Reference: PCI DSS v3 9.8.1, PCI DSS v3 9.8.2

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Management	**Approval Date**	November 8, 2018
Date Policy In Effect	November 7, 2014	**Version #**	1.1
Original Issue Date	November 7, 2014	**Last Review Date**	September 15, 2020 November 8, 2018
Related Documents	Data and Media Sanitization Certification Form Data Classification Policy Glossary Information Asset Management Policy Media Protection Policy		