

Secure Disposal Policy

Version	Approval Date	Owner
1.0	November 29, 2018	Chief Information Security Officer

1. Purpose

The purpose of this 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.

2. Scope

This policy applies to all media, paper media, removable media, business mobile computing devices, and information assets that belong to HealthShare Exchange.

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 workforce members 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. Enforcement

Each member will ensure that all employees maintain compliance with their mandatory HIPAA training. In addition, each member shall report any suspected breach or misuse of systems offered by HSX to the HSX Privacy and Security Officer. HSX will investigate any reported violations and will take appropriate actions that includes up to suspension of services or access.

5. Definitions

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

6. 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	Daniel.wilt@healthshareexchange.org
Approved By	HSX Leadership	Approval Date	November 29, 2018
Date Policy In Effect	November 29, 2018	Version #	1.0
Original Issue Date	November 29, 2018	Last Review Date	November 29, 2018
Related Documents	Data Classification Policy Glossary Information Asset Management Policy Media Protection Policy		