1. **Purpose of Procedure**

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 are no longer needed
- Stored in Cloud Services or Hosted that is no longer needed
- Reassigned to other individuals
- Undergoing maintenance procedures

This is necessary to reduce the possibility of inappropriate exposure of data and unauthorized use, which will allow for the protection of 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. **Procedure Scope**

The procedure 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 procedure 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. Procedures

A. Preparation for Sanitation Procedures
   1. 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.
   2. 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.
   3. Media containing diagnostic and test programs are checked for malicious code prior to use by assuring that only vendor approved devices are used.

B. Secure Disposal of Paper Media
   1. Paper media containing confidential data shall be kept in locked bins until destruction.
   2. 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.

C. 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:
   1. All electronic computing devices or electronic storage media must be overwritten using approved and validated overwriting technologies/methods/tools without exception.
   2. 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.
   3. 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.
   4. 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.
   5. The Media Sanitization Certification must be submitted to HSX.
   6. Upon approval, the item(s) may then be transferred or disposed of.
D. The methods Used to Sanitize Media to ensure recovery of information is not possible and that information security objectives are not compromised are the following:

1. 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.

2. 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.

E. To minimize aggregation of media for disposal, all media destined for disposal shall go through the above process every 30 days.

F. When scheduled maintenance occurs and is completed by external organizations, covered information is cleared from equipment prior to maintenance unless explicitly authorized (see above for the details of the clearing procedure).

4. Definitions

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

5. References

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Technical Operations</th>
<th>Contact: email</th>
<th><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Brian Wells</td>
<td>Version #</td>
<td>1.1</td>
</tr>
</tbody>
</table>
| Current Approval Date: | March 19, 2019 | Review Dates: | October 27, 2023  
|                       |               |               | December 6, 2022  
|                       |               |               | October 5, 2021  
|                       |               |               | October 16, 2020  
|                       |               |               | March 19, 2019  
| Date Procedure to go into Effect: | April 1, 2017 |               | April 1, 2017  
| Related Documents: | Data and Media Sanitation Policy | |  
|                       | Glossary     |               |  
|                       | Media Protection Policy | |  