Backup Policy

1. Purpose
To ensure HealthShare Exchange (HSX) the maintenance, integrity, and availability of essential enterprise data for recovery in the event of a failure.

2. Scope
This policy applies to all employees, interns, contractors, members, participants, users, and third parties who use (HSX) information assets and to all uses of those assets, regardless of physical location.

3. Policy
Backup Policy
- On a weekly basis, HSX shall make full backup of essential enterprise data, system documentation, and software using an automated backup system.
- On a daily basis, HSX shall make an incremental backup of essential enterprise data, system documentation, and software using an automated backup system.
- HSX shall store backup media in a physically secure remote location, at a sufficient distance to make the backup media reasonably immune from damage to data at the primary site. Physical and environmental controls shall be in place for the backup media.
- HSX shall maintain inventory records of the backup media, including content and current location.
- Backups shall be encrypted according to the Encryption Policy.
- HSX shall conduct regular tests of the backup media and restoration process to ensure the integrity and security of the back-up copies are maintained for future availability in accordance with the agreed backup policy. Any potential accessibility problems with the back-up copies are identified and mitigated in the event of an area-wide disaster.
• Backup media shall be physically protected according to the *Physical and Security Access Policy.*
• Backup media at the end of life shall be taken out of service according to the *Data and Media Sanitization Policy* and the *Media Protection Policy.*
• When backup service is delivered by a third party, the Service Level Agreement (SLA) shall include details on controlling confidentiality, integrity, and availability of the backup information according to the *Third Party Risk Management Policy.*

**Back Up Plan**

• HSX shall define and document a Backup Plan containing the following for each system:
  o Scope of data to backup
  o Frequency of backup including time of day
  o Type of backup (e.g., full, differential, incremental)
  o Location of backup media
  o Retention of backup media
  o Restoration procedures including restoration time
• The Backup Plan shall define the storage location for backup logs automatically generated by the backup system.

**4. Procedures**

None

**5. Enforcement**

• HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
• 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 shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
• The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
• The Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
• The 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

- HIPAA Regulatory Reference: HIPAA §164.308(a)(7)(ii)(A), HIPAA §164.308(a)(7)(ii)(B), HIPAA §164.310(d)(2)(iv), HIPAA §164.312(c)(1)
- HITRUST Reference: 09.1 Back-up
- PCI DSS v3 9.5.1

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Information Technology</th>
<th>Contact</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By</td>
<td>HSX Leadership</td>
<td>Approval Date</td>
<td>December 28, 2021</td>
</tr>
<tr>
<td>Date Policy In Effect</td>
<td>December 28, 2021</td>
<td>Version #</td>
<td>1.1</td>
</tr>
</tbody>
</table>
| Original Issue Date | November 29, 2018 | Last Review Date | October 19, 2023
|               |                        |         | December 28, 2021
|               |                        |         | September 29, 2021
|               |                        |         | September 16, 2020
|               |                        |         | November 29, 2018 |

Related Documents
- Backup Plan
- Data and Media Sanitization Policy
- Encryption Policy
- Glossary
- Media Protection Policy
- Physical and Security Access Policy
- Third Party Risk Management Policy