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

Backup Policy

Version	Approval Date	Owner
1.0	November 29, 2018	Information Technology

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.
- 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:
    - Scope of data to backup
    - Frequency of backup including time of day
    - Type of backup (e.g., full, differential, incremental)
    - Location of backup media
    - Retention of backup media
    - 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.l Back-up
- PCI DSS v3 9.5.1

Policy Owner	Information Technology	**Contact**	Brian.Wells@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**	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		