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

Encryption Policy

Version	Approval Date	Owner
1.2	November 4, 2019	Chief Information Security Officer

1. Purpose

To establish the methods for protecting the confidentiality, authenticity and integrity of enterprise data at rest, in transit, and in storage by cryptographic methods.

To ensure that encryption standards meet national and international regulations and industry standards.

The intent of this policy is to provide guidance regarding the use of encryption to protect confidential data. Mobile computing devices, removable media, and confidential data in storage and transmission, including email containing confidential information, must be encrypted to protect against unauthorized access, loss, or alteration.

2. Scope

All employees, interns, contractors, members, participants, vendors and third parties who have access or exposure to HealthShare Exchange (HSX) confidential data are required to comply with this policy.

3. Policy

Regulation of Encryption:

- Cryptographic controls shall be used in compliance with all relevant agreements, laws, and national and international regulations.
- Compliance with all relevant regulations shall be reviewed on an annual basis.

Encryption Policy:

- All encryption mechanisms and procedures for ensuring encryption must be approved by the Chief Information Security Officer (CISO).

- All encryption mechanisms implemented to comply with this policy must support a minimum of 256-bit AES (Advanced Encryption Standard) encryption.
- Encryption shall be used to protect enterprise data on mobile computing devices and removable media and across communication paths based on pre-determined criteria.
- Any "write" operation (e.g., file copy) of enterprise data to any removable media connected to HSX computing devices must employ an approved encryption mechanism to protect against unauthorized access to or modification of the data.
- When transmitting enterprise data using removable media the sending party must:
    - Use an encryption mechanism to protect against unauthorized access or modification.
    - Authenticate the requesting person or entity.
    - Send the minimum amount of enterprise data required by the receiving person or entity.
- If un-encrypted enterprise data is discovered on removable media, the enterprise data shall be transferred either to a HSX-managed computing device or to an approved, encrypted removable media format.
- If un-encrypted media has been used for enterprise data storage, the unencrypted media must be turned in to the CISO for proper disposal as soon as the data has been transferred to an approved, encrypted media and format.
- Encryption keys and/or passwords shall not be printed nor allowed to directly accompany removable media. They must be kept physically and electronically separate.
- Encryption key management shall be implemented based on specific roles and responsibilities and in consideration of national and international regulations, restrictions and issues.
- Encryption keys shall be limited to a period of time not to exceed one year.
- Specific mechanisms shall be put in place to recover information in case the encryption keys are lost.
- The policy that all enterprise data written to removable media must be encrypted may be waived by the CISO or their designee for good cause. Individuals or departments may request a waiver by submitting a proposal to the CISO. The case and wavier decision shall be documented. If deemed necessary, the CISO may grant a temporary waiver pending the waiver process completion. Examples of waivers would include, but are not limited to the following situations:
    - Where it is not technically possible to encrypt the enterprise data and the data being transferred or stored is neither protected health information (PHI) nor otherwise sensitive in nature.

- Where institutional processes cannot support this mandate and a documented plan by which an equivalent level of protection may be achieved is on file.

4. Procedure

The following procedures apply to HSX internal operations only:

- Encryption Procedures

5. Enforcement

- 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

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308(a)(1)(ii)(D), HIPAA § 164.312(a)(2)(iv), HIPAA § 164.312(e)(2)(ii)
- HITRUST Reference: 06.f Regulation of Cryptographic Controls, 10.f Policy on the Use of Cryptographic Controls, 10.g Key Management
- PCI DSS v3 3.5, PCI DSS v3 3.5.1, PCI DSS v3 3.5.2, PCI DSS v3 3.6, PCI DSS v3 3.6.1, PCI DSS v3 3.6.2, PCI DSS v3 3.6.3, PCI DSS v3 3.6.4, PCI DSS v3 3.6.5, PCI DSS v3 3.6.6, PCI DSS v3 3.6.7, PCI DSS v3 3.6.8, PCI DSS v3 8.2.2

Policy Owner	Security Officer	**Contact**	BrianWells@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	November 4, 2019
Date Policy In Effect	May 15, 2017	**Version #**	1.2

Original Issue Date	May 15, 2017	**Last Review Date**	September 14, 2020 November 4, 2019 September 15, 2019
Related Documents	Confidentiality Agreement Glossary		