

Transmission Security and Encryption Policy

Version	Approval Date	Owner
1.3	February 24, 2022	Chief Information Security Officer

1. Purpose

The transmission of PHI using secure and encrypted means is required for HealthShare Exchange (HSX) to ensure we protect the information being shared.

2. Scope

This applies to all employees, contractors, members, participants, users, vendors, and third parties that transmit PHI with HSX.

3. Policy

- HSX strives to contract with appropriate vendors to protect against unauthorized access to PHI that is being transmitted over an electronic communication network through implementation of “reasonable and appropriate” security measures to ensure that electronically transmitted ePHI is not improperly modified without deletion until disposed of.
- HSX shall require its contracted vendors to implement encryption, on a routine basis for any and all PHI accessed or transmitted through the exchange, including but not limited to PHI transmitted through email.
- HSX shall ensure that the confidentiality and integrity of electronic commerce are maintained.
- HSX shall ensure electronic commerce and online transactions are checked to determine if they contain covered information.
- Where a trusted authority is used (e.g., for the purposes of issuing and maintaining digital signatures and/or digital certificates), security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

- HSX shall ensure that the storage of the transaction details are located outside of any publicly accessible environments (e.g. on a storage platform existing on the organization's intranet) and not retained and exposed on a storage medium directly accessible from the Internet.
- HSX shall ensure FIPS-validated cryptographic mechanisms (TLS 1.1 or later) are used during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by an organization-defined alternative physical measures. This requirement includes transmission over less trusted /open public networks.

4. Procedures

1. The Security Officer together with the respective departments and management shall be responsible on an ongoing basis for identifying, evaluating, implementing, monitoring and updating cyber security mechanisms as necessary and appropriate to reasonably safeguard the confidentiality, integrity and availability of all IT and data from cyber security threats and vulnerabilities and minimize the impact of such threats and vulnerabilities on business operations. The Security Officer shall identify all key personnel responsible for implementation of cyber security controls. The Security Officer, along with key personnel, shall assess, identify and implement additional security mechanisms in the following areas [specify in greater detail the current activity controls in place and being put in place]:
2. If it is not "reasonable and appropriate" to implement encryption, HSX shall document the reasons why and a reasonable alternative here:
 - It is not "reasonable and appropriate" to implement such procedures because:
(insert description here)
 - The reasonable alternative that will be used to implement such procedures is:
(insert description here)
 - The reasonable alternative that will be used to implement such procedures is:
(insert description here)

5. Enforcement

- The CISO shall be responsible for enforcing compliance with this policy under the direction of the President.

6. Definitions

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

7. References

Regulatory References:

- None

Policy Owner	Chief Information Security Officer	Contact	Brian.wells@healthshareexchange.org
Approved By	Board HSX Management Team	Approval Date	December 28, 2021
Date Policy In Effect	February 24, 2022	Version #	1.3
Original Issue Date	December 24, 2013	Last Review Date	October 25, 2023 December 5, 2022 February 24, 2022 December 26, 2021 October 2, 2021 September 16, 2020 January 16, 2019 September 15, 2019
Related Documents	Glossary		