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

Direct Secure Messaging Policy

Version	Approval Date	Author
1.1	November 8, 2018	Daniel Wilt

1. Purpose

HSX is committed to maintaining the privacy and security of Data exchanged through HSX. HSX complies with the Direct Project specifications and standards as may be applicable in facilitating Direct Secure Messaging between participants. Participants are responsible for all encryption and decryption activities when using HSX capabilities to exchange Data through Direct Secure Messaging.

2. Scope

Applicable to HSX and all Direct Secure Messaging Participants.

3. Policy

3.1. Compliance with Direct Specifications and Protocols

HSX will comply or ensure that the vendor complies at all times with applicable Direct Specifications when facilitating Direct Secure Messaging between participants. This includes, but is not limited to authentication, verification of signatures and certificates, and other security and trust capabilities.

3.2. Direct Message Encryption

HSX will facilitate encryption of all Message Content, which is sent using Direct Secure Messaging. Message Content may include but is not limited to Protected Health Information (PHI), de-identified data, pseudonymized data, meta data, credentials and schema. HSX may have access to unencrypted Message Content based on the use cases. Each participant will be responsible for encrypting or decrypting Message Content as follows:

- Participants may use the HSX provider directory to send Direct Secure Messages to a provider or organization, which has a registered its Direct address with HSX for example organization@direct.organization.org,

individual@direct.organization.org, or patient@direct.organization.org. Members may also send Direct Secure Messages manually to any HSX trusted Direct domain.

- HSX will facilitate capabilities for any participant to encrypt Message Content prior to transmitting such to an intended recipient. Message Content must be encrypted prior to the Direct Secure Message being sent and will remain encrypted until received by the recipient "End-to-End Encryption".

- Participants must ensure that no PHI or other patient identifying information is contained in the Subject Line of any Direct Secure Message.

- HSX will facilitate capabilities for any intended recipient participant to decrypt Message Content upon receipt from another participant or provider with a Direct Address. Participants are solely responsible for ensuring that only such individuals who are associated with a Direct Address for example an individual or organizational have access to decrypted Message Content.

3.3. Audit Logs

HSX will maintain reasonable and appropriate audit logs to verify send and receipt of Direct Secure Messages by their intended recipients, any applicable confirmation of receipts and the integrity of End-to-End Encryption. HSX will perform periodic audits as needed to ensure compliance by HSX with the Direct Specifications.

3.4. Business Associate (BA) Services

HSX is a data transmission entity acting as a conduit and storage for the exchange of encrypted Data and is a HIPAA Business Associate of the Members. HSX may maintain Message Content as needed to transmit the Direct Secure Message to an intended recipient through End-to-End Encryption. HSX may have access to Message Content or other Data on a routine or frequent basis.

To the extent HSX routinely accesses Message Content or other Data, or maintains, transmits or otherwise uses or discloses any Data, which would establish a Business Associate relationship between HSX and the Members, HSX will require and comply with the terms of the applicable HIPAA Business

Associate Agreements (BAA) and such HSX policies governing access to and use of Member PHI.

4. Procedures

None

5. Enforcement

Each participant will ensure that all authorized users maintain their mandatory HIPAA training as it relates to password management. In addition, each participant shall report any suspected breach or misuse of the Direct Secure Messaging system offered by HSX to the HSX Privacy and Security Officer. HSX will investigate any reported violations and will take appropriate actions which includes up to suspension of services or access.

6. Definitions

Direct Project: HSX facilitates the exchange of Data between Members using Direct Project specifications and protocols. The exchange of Data transported using Direct Project specifications and protocols is known as "Direct Messaging" or a "Direct Message." Direct Messages are transported by HSX in compliance with the Applicability Statement for Secure Health Transport (the Direct Specifications) available at http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport, as may be amended from time to time.

Direct Secure Messaging Participants: Individuals or entities that have executed an agreement and a business associate agreement with HSX.

7. References

Policy Owner	Security Officer	Contact	Daniel.wilt@healthshareexchange.org
Approved By	HSX Leadership Team Executive Committee	Approval Date	November 8, 2018
Date Policy In Effect	April 7, 2016	Version #	1.1
Original Issue Date	April 7, 2016	Last Review Date	November 8, 2018
Related Documents	Audit and Monitoring Policy Credentialing Policy Data Misuse Policy Opt Out and Opt Back In Policy Compliance Policy Glossary Participation Agreement Use Case Governance		