190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Information Exchange Policy

Version	Approval Date	Owner
1.1	January 19, 2017	Chief Information Security Officer

1. Purpose

The purpose of this policy is to protect the exchange of HealthShare Exchange (HSX) enterprise data in transit through various communication applications and media including but not limited to email, texting, messaging, paging, file transfer, virtual private networks (VPNs), application interfaces, and other communication channels.

This policy also includes the requirement for establishing information exchange agreements with third parties and protecting physical media in transit.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, and third parties who access HSX information assets regardless of physical location.

3. Policy

Information Exchange Policy

- HSX shall protect the exchange and sharing of HSX enterprise data.
- Formal policies, procedures, and controls shall be in place to protect the exchange of HSX enterprise data through the use of all forms of communication media.
- The *Acceptable Use Policy* shall define the acceptable use of electronic communication applications and systems.
- The *Virus and Malware Protection Policy* shall define the use of anti-malware software to protect electronic communications against malicious code.
- The *Wireless Network Security Policy* shall define the network controls necessary to protect electronic communications accessed via the HSX wireless network.
- The *Encryption Policy* shall define the use of encryption to protect the exchange of electronic communications containing confidential data.

- The *Compliance Policy* and *Data and Media Sanitization Policy* shall define the retention and disposal guidelines for electronic communications containing confidential data.
- The *Remote Access Policy* shall define the terms and conditions of access to HSX's information assets and access to external information assets (over which the organization has no control) to protect electronic communications during remote access sessions.
- The *Third-Party Risk Management Policy* shall define the terms and conditions of electronic communications with other organizations owning, operating, and/or maintaining external information systems.
- Employees and contractors shall be educated according to the *Privacy and Security Awareness, Education and Training Policy* regarding HSX policies for safe and approved practices for information exchange.
- Controls and restrictions shall be implemented to prevent the unauthorized forwarding of electronic communications (e.g., automatic forwarding of email to external email addresses).
- HSX shall not send PII/PHI over facsimile (FAX), unless it cannot be sent over other, more secure channels, e.g., delivery by hand, secure email.

Information Exchange Agreements

- Information exchange agreements (including the Participation Agreement) shall be established and implemented for the exchange of information and software between HSX and third parties.
- Information exchange agreements shall not conflict with, nor shall they lower the standards and requirements stated, in any Business Associate Agreement (BAA) between HSX and third parties.
- Information exchange agreements may either be incorporated into a BAA between HSX and third parties or they may be a separate agreement.
- Information exchange agreements shall specify the minimum set of controls for responsibilities, procedures, technical standards, technical solutions, incident management, reporting and notification, access controls, auditing, logging and monitoring, and physical safeguards.
- Information exchange agreements shall specify all applicable HSX policies.
- HSX policies, procedures, and standards regarding protection of the exchange of HSX enterprise data shall be referenced in information exchange agreements.

Physical Media in Transit

- Procedures shall be established and implemented to protect media in its stored physical form (e.g., back-up tapes, USB flash drives, CDs, DVDs, hard drive devices, etc.) while in transit.

- Physical media containing confidential data shall be protected against unauthorized access, misuse, corruption, or destruction during transportation outside of HSX's physical boundaries.
- Controls shall be established to protect confidential data residing on physical media from unauthorized disclosure or modification while in transit.

Electronic Messaging, Texting, and Paging

- Information involved in electronic messaging, texting, and textual paging shall be appropriately protected in accordance with HSX information security policies, and federal and state laws and regulations.
- Approval shall be obtained from the Chief Information Security Officer (CISO) prior to using external public services (e.g., instant messaging, file sharing, etc.) that are not approved by or managed by HSX.
- Electronic messages shall be encrypted throughout the duration of their end-to-end transport path according to the *Encryption Policy*.
- Employees, contractors, members, participants, users, and third parties shall never send unencrypted HSX Health Information Exchange (HIE) confidential data via messaging technologies (e.g., email, instant messaging, textual paging, SMS texting, chat, etc.).

Interconnected Information Systems

- Policies and procedures shall be developed and implemented to protect confidential data associated with the interconnection of information systems.
- Security and business implications shall be addressed for interconnecting information assets including:
    - Policy and appropriate security controls to manage information sharing.
    - Excluding confidential data if the system does not provide an appropriate level of protection.
    - Categories of employees, contractors, members, participants, users, and third parties allowed to use the system and the locations from which it may be accessed.
    - Restricting selected systems and facilities to specific categories of employees, contractors, members, participants, users, and third parties.
    - Identifying the status of employees, contractors, members, participants, users, and third parties.

4. Procedures

None

5. Enforcement

- 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 and Privacy Officer 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(b)(1), HIPAA § 164.308(b)(3), HIPAA § 164.310(b), HIPAA § 164.310(d)(1), HIPAA § 164.310(d)(2)(iii), HIPAA § 164.312(c)(1), HIPAA § 164.312(c)(2), HIPAA § 164.312(e)(1), HIPAA § 164.312(e)(2)(i), HIPAA § 164.312(e)(2)(ii)
- HITRUST Reference: 09.s Information Exchange Policies and Procedures, 09.t Exchange Agreements, 09.u Physical Media in Transit, 09.v Electronic Messaging, 09.w Interconnected Business Information Systems
- PCI Reference: PCI DSS v3 4.1, PCI DSS v3 4.1.1, PCI DSS v3 4.2, PCI DSS v3 9.6.2

Policy Owner	Chief Information Security Officer	**Contact**	brian.wells@healthshareexchange.org
Approved By	HSX Management Team Board	**Approval Date**	September 15, 2019
Date Policy In Effect	April 29, 2015	**Version #**	1.1
Original Issue Date	April 29, 2015	**Last Review Date**	September 16, 2020 September 15, 2019 January 19, 2017

Related Documents	Acceptable Use Policy Business Associate Agreement (BAA) Compliance Policy Data and Media Sanitization Policy Direct Secure Messaging Data Exchange Policy Direct Secure Messaging Operations Policy Encryption Policy Glossary Privacy and Security Awareness, Education and Training Policy Remote Access Policy Third Party Risk Management Policy Virus and Malware Protection Policy Wireless Network Security Policy