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

Acceptable Use Policy

Version	Approval Date	Owner
1.1	November 8, 2018	Chief Information Security Officer

1. Purpose

This policy sets standards and expectations for HealthShare Exchange (HSX) employees, interns, contractors, members, participants, users, and third parties with regard to access to HSX information assets.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, and third parties who use HSX information assets and related resources.

This policy applies to information technology administered in individual departments; technology administered centrally; personally-owned computing devices connected by wire or wireless to the HSX network; and to off-site computing devices that connect remotely to HSX's network.

3. Policy

Acceptable Use Policy

- Employees, interns, contractors, members, participants, users, and third parties shall bear the responsibility for knowing and complying with applicable state and federal laws, rules and regulations, and contractual obligations when accessing HSX information assets.
- Employees, interns, contractors, members, participants, users, and third parties shall be informed of their responsibilities for maintaining effective access controls and shall be required to follow HSX policies.
- HSX provides information assets as resources to employees, interns, contractors, members, participants, users, and third parties. Each individual shall be responsible for properly using and protecting those resources.

- Use of information assets owned or operated by HSX imposes certain responsibilities and obligations. HSX considers use of IT resources to be a privilege that is granted on the condition that each individual respects the integrity of IT resources and the rights of other individuals.
- Employee, intern, contractor, member, participant, user and third-party authorized individuals are prohibited from using external information systems unless the appropriate security controls are verified and deemed adequate with an approved connection or processing agreement.
- Chief Information Security Officer (CISO) or designee must approve, control, monitor, and periodically check all maintenance tools.
- Employee, intern, contractor, member, participant, user, and third-party access to HSX information assets (e.g., PHI) shall be restricted to need-to-know and minimum necessary.
- Employees, interns, contractors, members, participants, users, and third parties shall be responsible for the use and protection of HSX information resources by using effective access controls (e.g., passwords) and by safeguarding those access controls.
- Employees, interns, contractors, members, participants, users, and third parties are required to handle, label, and store confidential data in accordance with the *Data Handling, Labeling, and Storage Policy*.
- All employees, interns, contractors, members, participants, users, and third parties must scan all electronic media for potential threats prior to use in accordance with the *Endpoint Protection Policy*.
- Connection to the Internet, or use of a website, is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action.
- Employees, interns, contractors, members, participants, users, and third parties shall be allowed to use HSX information assets:
    - To which they have been granted authorized access.
    - For HSX business and research purposes.
    - For incidental personal use.
- Employees, interns and contractors shall be allowed incidental personal use so long as those activities are legal and do not violate:
    - HSX policies
    - Contractual obligations
    - The safety, security, privacy, reputational and intellectual property rights of others.
    - Applicable restrictions on political or commercial activities.
- Related HSX policies that may apply to acceptable use of HSX information assets include, but are not limited to, HSX's Human Resources personnel policies, Finance

policies, Information Security and Privacy policies, and Administrative policies, all of which are subject to change.

Acceptable Password Use Policy

- Passwords must be kept confidential and must not be written down or recorded electronically.
- Passwords and accounts must not be shared.
- Personal and HSX (business) passwords must be different.
- Passwords must be changed at least every 90 days or whenever there is any indication of possible system or password compromise.
- Employees, interns. contractors, members, participants, users, and third parties shall utilize strong passwords that require at least 8 characters which are a combination of alphabetic, upper- and lower-case characters, numbers, and special characters (combination of any three [3] of the above four [4] listed is acceptable).
- Passwords cannot be reused for at least six (6) generations. At least four changed characters must be used when new passwords are created.
- Temporary passwords shall be changed at the first log-on.

Responsibilities for Unattended Information Assets

- Employees, interns, contractors, members, participants, users, and third parties shall ensure that unattended equipment has appropriate protection.
- Employees, interns and contractors shall log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal) in accordance with the *Clear Desk and Clear Screen Policy*.
- HSX shall safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output.

Employees, interns, contractors, members, participants, users, and third parties of HSX Information Assets agree to ***NOT***:

- Post, use or transmit content that they do not have the right to post or use, for example, under intellectual property, confidentiality, privacy or other applicable laws.
- Post, use or transmit unsolicited or unauthorized content, including:
    - Advertising or promotional materials
    - "Junk mail"
    - "Spam"
    - "Chain letters"
    - "Pyramid schemes"
    - Political campaign promotional material
    - Any other form of unsolicited or unwelcome solicitation or advertising

- Infringe upon copyrighted material of any kind, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of HSX information assets (e.g. network, email system, website, etc.) to access, display, send, transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited.
- Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or otherwise interfere with or disrupt HSX information assets.
- Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false and misleading, incites an illegal act, or is otherwise in breach of one's obligations to any person or contrary to any applicable laws and regulations;
- Intimidate or harass another;
- Use or attempt to use another Employee, intern, contractor, member, participant, user, and third party's account, service, or personal information;
- Remove, circumvent, disable, damage or otherwise interfere with any security-related features;
- Attempt to gain unauthorized access to HSX information assets, other user's accounts, computing devices or networks connected to HSX information technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of HSX information assets or any activities conducted through those information assets;
- Impersonate another person or entity, or falsely state or otherwise misrepresent one's affiliation with a person or entity;
- Conduct any activities with the intention of creating and/or distributing malicious programs using HSX's network (e.g., viruses, worms, Trojan Horses, etc.);
- Install or use unauthorized or malicious software, or obtain data and software from external networks;
- Fail to exercise appropriate caution when opening emails, attachments or accessing external web sites.

Prevention of Misuse of Information Assets

- All employees, interns, contractors, members, participants, users, and third parties shall read and sign the *Acceptable Use Policy* before receiving access to information assets.
- All employees, interns. contractors, members, participants, users, and third parties shall be responsible for appropriately securing their computers and other electronic

devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of HSX information assets.

- HSX shall provide notice that each individual's actions may be monitored, and that the individual consents to such monitoring.
- While HSX desires to maintain privacy and to avoid the unnecessary interruption of activities, HSX reserves the right to investigate unauthorized or improper use of computing devices, which may include the inspection of personal data stored or transmitted on HSX's network. In the event that use is determined to be contrary to HSX policy or applicable law, appropriate measures shall be taken.
- Employees, interns, contractors, members, participants, users, and third parties shall be informed in writing of the *Sanctions Policy* for security violations.
- Use of email must comply with all HSX Code of Ethical Conduct rules as they apply to the working environment. Non-compliance shall result in termination of the email account and subject the employee, contractor, member, participant, user, and third party to any other actions defined in the *Sanctions Policy*.
- Information asset owners shall approve the use of information assets and take appropriate action when unauthorized activity occurs.

4. Procedure

None

5. Enforcement

- As part of HSX orientation, HSX employees, contractors and interns shall be informed about the requirements of the *Acceptable Use Policy* and sign a copy of the policy as documentation of receipt and agreement to comply.
- 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.
- Any employee, intern, contractor, member, participant, user, and third party violating these policies or applicable local, state, or federal laws while using HSX information assets shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate, possibly including termination and criminal and/or civil prosecution in accordance with federal and state law and HSX Human Resources policies and procedures.

HSX reserves the right to review and/or monitor any emails or transmissions sent or received through the HSX Network, at its sole discretion.

Penalties for violating this policy may include restricted access or loss of access to the HSX Network, termination and/or expulsion from HSX and in some cases, civil and/or criminal liability.

HSX reserves the right to update or revise this policy or implement additional policies in the future.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308 (a)(5)(ii)(D), HIPAA § 164.310(a)(1), HIPAA § 164.310(b), HIPAA § 164.310(c), HIPAA §164.312(a)(2)(iii)
- HITRUST Reference: 01.f Password Use, 01.g Unattended User Equipment, 09.j Controls Against Malicious Code
- PCI Reference: PCI DSS v3 8.2.6, PCI DSS v3 8.4, PCI DSS v3 8.2.4, PCI DSS v3 8.2.5

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Management Team	**Approval Date**	November 8, 2018
Date Policy In Effect	May 15, 2017	**Version #**	1.1
Original Issue Date	May 15, 2017	**Last Review Date**	September 17, 2020 November 8, 2018

Related Documents	Clear Desk and Clear Screen Policy Conflict of Interests Policy Data Handling, Labeling, and Storage Policy Employee Human Resources Manual Endpoint Protection Policy Glossary Sanction Policy Social Media Policy