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

Privacy and Security Awareness Education and Training Policy

Version	Approval Date	Owner
1.2	December 1, 2018	Privacy Officer

1. Purpose

HealthShare Exchange (HSX) is committed to ensuring that employees, interns, consultants and contractors are properly trained and made aware of policies, procedures, potential threats, and security incidents.

The purpose of this policy is to ensure that employees and contractors receive privacy and security training in a timely manner, and that there is appropriate documentation of the training. In addition, this policy ensures that employees and contractors with significant security responsibilities receive in-depth training.

2. Scope

This policy applies to all employees, interns, consultants and contractors regardless of physical location.

Senior leadership shall be responsible for ensuring that employees and contractors are compliant with this policy.

The Chief Information Security Officer (CISO) and the Privacy Officer shall be responsible for:

- Determining the training content and requirements. This shall include the following:
    - A periodic review and update of the training materials.
    - An inspection of the training materials to ensure that the content covers all areas of the HIPAA Privacy and Security Rules.
    - Implementing a process to track training attendance and successful course completion.
- Ensuring compliance with information privacy and security training requirements, which shall include the following:

- Employees, interns, and consultants and contractors completing training within the specified time frame.
- Employees, interns, consultants and contractors signing the Confidentiality Agreement within the specified time frame.
- Evaluating employees, interns, consultants and contractors' understanding of policies and procedures on an annual basis.
- Notifying the appropriate person when these requirements are not met.

Employees, interns, consultants and contractors shall be responsible for:

- Completing training within the specified timeframes.
- Reviewing and understanding policies and procedures.
- Signing the Confidentiality Agreement prior to performing any job functions.
- Completing refresher training on an annual basis.

3. Policy

HSX shall develop and implement training to ensure that all Employees, interns, consultants and contractors are aware of the risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, and procedures.

- HSX must promote strategies for protecting information assets and confidential data.
- HSX must provide specialized training for Employees, interns, consultants and contractors whose job functions require specialized skill or knowledge in information security.
- HSX must conduct an annual review of the training program and materials.

Privacy and Security Awareness and Training:

- All Employees, intern, consultants and contractors shall receive privacy and security awareness training no later than 30 days after hire, when required by system changes, and annually thereafter.
- Security awareness training shall include the recognition and reporting of potential indicators of an insider threat.
- All Employees, interns, consultants and contractors shall receive training prior to being granted access to HSX confidential information.
- All Employees, interns, consultants and contractors shall acknowledge that they have received training and are aware of their responsibilities by signing an acceptance or acknowledgement of their responsibilities.

- All Employees, interns, consultants and contractors shall demonstrate understanding of HSX policies, procedures, and directives through their compliance and an attestation document.
- HSX shall maintain ongoing security awareness by publishing security bulletins and posters, and conducting safety fairs, ad-hoc presentations, and monthly meetings.
- HSX shall update training materials on an annual basis or whenever there is a change in regulatory controls.
- HSX shall provide ongoing training for all employees, interns, consultants, and contractors as needed, but not limited to security and privacy requirements (e.g., objective, scope, roles and responsibilities, coordination, compliance, legal responsibilities and business controls) as well as training in the correct use of information assets and facilities (including, but not limited to, log-on procedures, use of software packages, anti-malware for mobile devices, and information on the disciplinary process).
- A list of applications, application stores, and application extensions and plugins approved for Bring Your Own Device (BYOD) usage will be provided during training. (See HSX Business Document for full list of approved applications).
- All employees, interns, consultants, and contractors will be required to complete a refresher training of HSX's security and privacy education and training program at least every three hundred and sixty-five (365) days. Employees shall be required to acknowledge they have received training and are aware of their responsibilities through signoff.
- HSX shall include security awareness training on recognizing and reporting potential indicators of an insider threat.
- HSX's security personnel, including organizational business unit security points of contact, shall receive specialized security education and training appropriate to their role/responsibilities. Train developers at least annually in up-to-date, secure coding techniques, including how to avoid common coding vulnerabilities. Ensure developers understand how sensitive data is handled in memory.
- Personnel with significant security responsibilities, e.g., system administrators, receive specialized education and training on their roles and responsibilities prior to access the organization's systems and resources, when required by system changes, when entering into a new position that requires additional training, and no less than annually thereafter.
- HSX's awareness program will:
    - Focus on the methods commonly used on intrusions that can be blocked through individual actions;
    - Deliver content in short online modules convenient for employees;

  - Receive frequent updates (at least annually) to address the latest attack techniques; and
  - Include the senior leadership team's personal messaging and involvement.
- HSX will train all employees, interns, consultants, and contractors to ensure covered information is stored in organization-specific locations.
- HSX shall provide incident response and contingency training to information system users consistent with assigned roles and responsibilities
  - within 30 days of assuming an incident response role or responsibility;
  - when required by information system changes; and
  - within every three hundred sixty-five (365) days thereafter.

Acceptable Use Training

- Employees and contractors shall receive training on the acceptable uses of HSX information assets in accordance with the *Acceptable Use Policy* prior to being granted access to HSX information assets.
- At a minimum, Employees and contractors shall receive training and periodical reminders:
  - To not leave confidential data on system output devices (e.g., copiers, printers, and facsimile machines) according to the *Acceptable Use Policy*.
  - That facsimile machines and photocopiers have page caches that will store pages in case of a paper or transmission fault. The pages may be printed later once the fault is cleared.
  - Regarding using facsimile machines securely, namely to avoid:
    - Sending documents and messages to the wrong number either by misdialing or using the wrong stored number.
    - Unauthorized access to built-in message stores while retrieving messages.
    - Deliberate or accidental programming fax machines to send messages to specific numbers.
  - Not to register or add demographic data, such as their email address or other personal information, in any software to avoid collection for unauthorized use.
  - HSX prohibits users from installing unauthorized software, including data and software from external network, and ensures users are made aware and trained on these requirements. See Access Controls Policy and HSX Business Applications document for more details regarding acceptable software.
  - Leading practices in information exchange (oral, paper, electronic).

Training for Information Security Employees and Contractors

- All information security Employees and contractors shall receive specialized training regarding their roles and responsibilities as part of their initial training, when required by system changes, and annually thereafter.
- HSX must provide or coordinate training for Employees and contractors whose job functions require special knowledge of security threats, risks, vulnerabilities, techniques, and safeguards. This training must focus on expanding knowledge, skills, and abilities for workforce members who are assigned information security roles and/or responsibilities.
- All information security Employees and contractors shall receive specialized training and awareness prior to accessing information assets.
- All information security Employees and contractors shall receive regular updates regarding policies and procedures relevant to their job function.

Training Records

- Dedicated security and privacy awareness training developed as a part of HSX's onboarding program will be documented and tracked and will the recognition and reporting of potential indicators of an insider threat.
- HSX must retain records of all training activities and attestation documents through the Human Resource Department.

4. Procedure

- All Employees, interns, consultants and contractors shall receive privacy and security awareness training no later than 30 days after hire, when required by system changes, and annually thereafter.
- HSX shall provide ongoing training for all employees, interns, consultants, and contractors as needed, but not limited to security and privacy requirements (e.g., objective, scope, roles and responsibilities, coordination, compliance, legal responsibilities and business controls) as well as training in the correct use of information assets and facilities (including, but not limited to, log-on procedures, use of software packages, anti-malware for mobile devices, and information on the disciplinary process).
- All employees, interns, consultants and contractors will be required to sign an attestation document at the completion of every training acknowledging training completion, compliance with HSX policies, and acceptance of security and privacy responsibilities.
- Dedicated security and privacy awareness training developed as a part of HSX's onboarding program will be documented and tracked, and will the recognition and reporting of potential indicators of an insider threat.

- HSX must retain records of all training activities and attestation documents through the Human Resource Department, including a documented list of each individual who completes the on-boarding process and trainings, for at least 5 years.
- All HSX Employees, interns, consultants, and contractors will be informed in writing, (e.g., when they sign HIPAA Privacy and Security Training Attestation document which indicates the rules of behavior or an acceptable use) that violations of the security policies will result in sanctions or disciplinary action.

5. Enforcement

- The HSX Human Resource representative shall ensure that all employees, interns, consultants and contractors receive education and training according to 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 §160.103, HIPAA §164.308 (a)(5)(i), HIPAA §164.308 (a)(5)(ii)(A), HIPAA §164.308 (a)(5)(ii)(B), HIPAA §164.308 (a)(6)(i), HIPAA §164.308 (a)(7)(ii)(D), HIPAA §164.310(b), HIPAA §164.414(a), HIPAA §164.530(b)
- HITRUST Reference: 02.e Information Security Awareness, Education and Training, 09.s Information Exchange Policies and Procedures
- PCI Reference: PCI DSS v3 4.1, PCI DSS v3 4.1.1, PCI DSS v3 6.5, PCI DSS v3 9.9, PCI DSS v3 9.9.3, PCI DSS v3 12.6, PCI DSS v3 12.6.1, PCI DSS v3 12.6.2

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

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	Board HSX Management Team HSX Privacy and Security Workgroup	**Approval Date**	December 1, 2018
Date Policy In Effect	June 4, 2015	**Version #**	1.2
Original Issue Date	June 4, 2015	**Last Review Date**	December 4, 2022 September 30, 2021 September 17, 2020 September 15, 2019 December 1, 2018
Related Documents	Acceptable Use Policy Confidentiality Agreement Glossary HSX Privacy and Security Training August 2014 Privacy and Security Compliance Agreement		