HealthShare Exchange

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareexchange.org

# Information Security Management Program Procedures

| Version | Approval Date | Owner |
|---|---|---|
| 1.4 | December 14, 2021 | Chief Informaiton Security Officer |

## 1. Purpose of Procedure

HealthShare Exchange's (HSX) Information Security Management Program (ISMP) procedures aims to reduce risks to HSX by protecting and supporting the confidentiality, availability, and integrity of information assets by outlining the process for implementing the ISMP policy.

HSX is committed to conducting business in keeping with its core organizational values and established policies and in compliance with all industry standards and applicable laws and regulations. In particular, HSX is committed to compliance with the regulatory requirements established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of electronic protected health information ("ePHI"), also known as the "Security Rule" and all subsequent Security Rule updates, as well as all state-level regulatory compliance requirements that apply to its area of operations.

## 2. Procedure Scope

This procedure covers all HSX information security practices across all departments and business units. All HSX employees, interns, contractors and third parties are required to comply with this procedure.

## 3. Procedures

**Information Security Management Program Approval and Update Procedure**

The organization's information protection and risk management programs, including the risk assessment process, are formally approved and are reviewed for effectiveness and updated annually.

- The Privacy and Security Officers review the HSX Information Security Management Program during the annual policy and procedure review, update and proceed through the HSX Governance Process if any changes are deemed necessary.
- If changes occur, the communications procedure below is followed.
- The HSX CISO and Privacy Officer shall assign risk designations for all positions within the organization as appropriate, with commensurate screening criteria and shall review such designations annually.
- HSX shall formally appoint in writing non-professional or professional security contacts by name in each major organizational area or business unit within its members and participants.
- HSX CISO shall report in writing on HSX's cybersecurity program and material cybersecurity risks at least annually to the HSX board of directors, equivalent governing body, or suitable committee.

The Technical Operations Team, CISO, and/or Reporting Manager shall ensure that employees, contractors and third-party users:

1. are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
2. are provided with guidelines to state security expectations of their role within the organization;
3. are motivated and comply with the security policies of the organization;
4. achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
5. conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and
6. continue to have the appropriate skills and qualifications.

All HSX employees, interns, contractors and third parties will be responsible for signing an attestation acknowledging the ISMP policy. This attestation will either be signed during a lunch and learn, or during a one-on-one meeting with the Reporting Manager. Should any changes be made to ISMP policy, all HSX employees, interns, contractors and third parties will be responsible for signing a new attestation acknowledging the new changes. The Technical Operations Team will be responsible for reviewing testing, training, and monitoring plans for consistency with the organization risk management strategy and organization-wide priorities for risk response actions. All HSX employees, interns, contractors and third parties will be directed to the HSX website to review all policies to ensure compliance. An attestation document will be signed to capture acknowledgement.

**Communicating Community Security Objectives**

To ensure transparency, all HSX approved policies are publicly accessible and can be found

online at hsxsepa.org.

All HSX policies and procedures are required to follow the HSX governance process. For device security, see HSX's Patch Management Policy, New Employee Setup policy and Annual Laptop Check procedure.

HSX creates and communicates its security goals, objectives and importance via the Privacy and Security Workgroup. Follow-up meetings with vendors are scheduled after any security analysis takes place. These changes are reviewed by the Privacy and Security Workgroup for approval.

HSX Senior management formally appoints and or engages security specialists for various related assessments. Such assessments are reviewed and remediated as may be required and coordinates and communicates results of the specialists' advice at appropriate levels within HSX.

The HSX CISO shall maintain appropriate security certifications and provide HSX leadership with copies of such certification. HX leadership shall ensure such certifications are maintained.

## 4. References

Regulatory References:

- HITRUST References: 02.d; CSF Control Reference, 02.d Management Responsibilities

| | | | |
|---|---|---|---|
| **Responsible Owner:** | Chief Information Security Officer | **Contact: email** | Brian.Wells@healthshareexchange.org |
| **Approved By:** | Board<br>HSX Management Team<br>Privacy and Security Workgroup | **Version #** | 1.4 |
| **Current Approval Date:** | December 14, 2021 | **Review Dates:** | December 12, 2021<br>October 5, 2021 |

| | | | |
|---|---|---|---|
| | | | October 19, 2020<br>March 19, 2019<br>April 1, 2017 |
| **Date Procedure to go into Effect:** | December 19, 2019 | | |
| **Related Documents:** | Glossary<br>Information Security Management Program | | |