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

Sanctions Policy

Version	Approval Date	Owner
1.1	December 16, 2015	Privacy Officer

1. Purpose

HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) employees, interns, contractors, members, participants, users, and third parties must comply with HSX information security policies and procedures, federal regulations (e.g., HIPAA, HITECH), state regulations (e.g., data breach notification laws, health codes), and accreditation standards related to information security (e.g., Joint Commission).

The purpose of this policy is to ensure that violations of information security and privacy policies, procedures, regulations, and standards including terms of use are addressed through a sanctions process. Any sanctions that are taken would be done under the direction of the HSX Executive Committee and in coordination with the HSX member when applicable. HSX would not be involved in applying any direct sanctions to workforce members who are HSX users. However, HSX could revoke access to the HSX Network for any HSX user of a participating member as appropriate.

2. Scope

This policy applies to all employees, contractors, members, participants, users including HSX members' workforce, interns, and third parties regardless of physical location.

3. Policy

HSX shall ensure that HSX information privacy and security policies/procedures, Federal and State regulations, and accreditation standards are followed and that appropriate sanctions are taken against employees, contractors, members, participants, users, and third parties who violate them.

- All HSX employees, interns, third parties, members, participants, users and contractors shall be responsible for complying with regulations, accreditation standards, HSX policies, federal regulations (e.g., HIPAA, HITECH), state regulations

(e.g., data breach notification laws, health codes), and relevant accreditation standards.

Employee and Contractor Disciplinary Process:

- The HSX Sanctions policy is consistently applied to all HSX employees, interns, co-ops, fellows, and contractors.
- Failure to comply with policies and procedures shall result in disciplinary action.
- HSX shall develop and employ a formal disciplinary process for employees, interns and contractors who fail to comply.
- The following categories will be used to define the significance and impact of the privacy or security incident to help guide appropriate corrective action and remediation steps as outlined in the Code of Conduct and Disciplinary Employee Performance policies.
- Category 1: Accidental or inadvertent violation. This is an unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error. Examples of this type of incident include directing PHI via mail, e-mail, or fax to a wrong party or incorrectly identifying a patient record.

  Category 2: Failure to follow established privacy and security policies and procedures. This is a violation due to poor job performance or lack of performance improvement. Examples of this type of incident include release of PHI without proper patient authorization; leaving detailed PHI on an answering machine; failure to report privacy and security violations; improper disposal of PHI; failure to properly sign off from or lock computer when leaving a work station; failure to properly safeguard password; failure to safeguard portable device from loss or theft; or transmission of PHI using an unsecured method.
  Category 3: Deliberate or purposeful violation without harmful intent. This is an intentional violation due to curiosity or desire to gain information, for personal use. Examples of this type of incident include accessing the information of high-profile people or celebrities or accessing or using PHI without a legitimate need.
  Category 4: Willful and malicious violation with harmful intent. This is an intentional violation causing patient or organizational harm. Examples of this type of incident include disclosing PHI to an unauthorized individual or entity for illegal purposes (i.e., identity theft); posting PHI to social media websites; or disclosing an individual's PHI for malicious purposes.

- Potential sanctions resulting from the disciplinary process shall include but are not limited to:

  - Remedial training
  - Informal counseling
  - Formal counseling
  - Suspension or removal of access rights to HSX information assets
  - Performance evaluation impacts and documentation
  - Suspension or rescinding of promotion.
  - Transfer from current job position
  - Termination of employment with HSX.
  - Termination of Contracts with Vendors
- HSX shall appoint a contact in Human Resources to support the discipline of employees and/or contractors involved in security incidents.
- HSX shall maintain a list of employees and contractors involved in security incidents including the outcome of the investigation.
- If a failure to comply has been alleged to have occurred but prior to the result of the disciplinary process, in cases where the Chief Information Security Officer (CISO) determines that allowing employees and contractors to retain access rights to HSX information assets presents an unacceptable risk to HSX, access rights to HSX information assets may temporarily be suspended.
- In cases where civil or criminal charges are involved, the CISO shall work together with Human Resources and HSX Legal Counsel where appropriate to determine and take appropriate legal action.
- The Sanctions policy is aligned with HSX's Anti Retaliatory and Whistleblower policies to ensure that there is no intimidation, threat, coercion or discrimination.
- No employee contractor, intern, co-op student or fellow shall be discharged, demoted, suspended, threatened, harassed, coerced, or retaliated against in any way as a result of reporting an actual or apparent violation in good faith. However, an employee who knowingly makes a false allegation or provides false or misleading information during an investigation will be subject to disciplinary action, up to and including termination of employment.

Members' Responsibilities:

- With guidance from HSX, each HSX Health Information Exchange (HIE) Member designates authorized users for the HSX network. The Member must ensure that such Member's users and all other workforce, agents and contractors shall comply with HSX privacy and security policies when accessing and using the HSX HIE.
- If a Member learns of or suspects a violation of an HSX Privacy or Security policy and/or evidence of unauthorized use of the HSX network, the Member shall report such violation as soon as is reasonably possible to the HSX CISO or the HSX Privacy Officer. This reporting does not relieve the Member from its own continuing duty to take appropriate action against its workforce for violations of its internal policies

and/or federal or state law governing the use and disclosure of a patient's data obtained through HSX.

- A Member shall require its own respective users to report violations to that Member, and shall adopt appropriate action for failure to do so.

HSX Member Investigatory Period and Administrative Suspension:

- The HSX Executive Committee shall authorize the CISO and Privacy Officer to establish operational procedures for auditing compliance with HSX policies and for conducting investigations upon discovery of potential non-compliant events and upon receipt of a complaint.
- HSX CISO and Privacy Officer will coordinate its investigation of a user with the Member who authorized the user.
- During any investigation, HSX may temporarily suspend access to the HSX HIE until the investigation is completed.
- Based on the findings of the audits and discovery activities (Findings), the CISO in collaboration with the HSX Privacy Officer shall present such Findings to the HSX Executive Committee, legal counsel, and/or HSX Board in a timely manner for its review and determination to impose sanctions, if any.

HSX Executive Committee Determination and Sanctions:

- Upon receiving the Findings, the HSX Executive Committee shall make a determination with regard to whether sanctions should be imposed upon a Member. In addition, the HSX Executive Committee could determine whether or not access to the HSX Network should be revoked for an HSX user of a participating member organization.
- Based on the Findings, the HSX Executive Committee shall render a determination whether or not to impose a sanction in accordance with the following:
    - Based on its interpretation of the Findings and the severity of the violation, the HSX Executive Committee may issue a sanction against the Member or the user.
    - In its discretion, the HSX Executive Committee may issue a sanction against a Member and its entire staff, or to selected users.
    - Any sanctions imposed by the HSX Executive Committee against a user or a Member will affect rights with regard to the HSX HIE under the Member Agreement. All specific "employment" and/or other "disciplinary" actions that may be taken against any user or member of a Member's workforce are reserved to the respective Member.
    - The HSX Executive Director on behalf of the HSX Executive Committee shall transmit its determination to the affected Member and applicable user by letter via the U.S. Postal Service or a commercial delivery service.

The determination letter shall specify whether a Sanction has been imposed or not.

- If the HSX Executive Committee determines not to impose any sanctions, then the suspension shall immediately end and the ability to access and use the HSX HIE shall be reinstated in full.
- HSX shall follow all federal and state laws regarding reporting of legal violations to state and federal authorities and shall cooperate with state and federal authorities for any investigation that such authorities may initiate.
- The Executive Committee shall report significant incidents requiring sanctions to the Board.

Appeal:

- A Member or user whose access to the HSX HIE has been terminated shall be afforded an opportunity to make an appeal to the HSX Executive Committee. Any such request for an appeal must be submitted by written letter within seven (7) calendar days and state the specific reasons and information supporting why the HSX Executive Committee's sanction should be overturned. A letter sent via the U.S. Postal Service or a commercial delivery service, with confirmed, signed delivery, shall be the only acceptable means of delivering such a letter.
- HSX may request written statements from any other parties involved in the matter that could have an impact on the decision made with regard to the sanction.
- All determinations made by the HSX Executive Committee shall be on the record only. There will be no personal appearances afforded to any party.
- The sanction previously imposed by the HSX Executive Committee shall continue in full force and effect until a final decision has been made.
- The HSX Executive Committee shall render a final decision to uphold or overturn the sanction. The final decision shall be transmitted by letter via the U.S. Postal Service or a commercial delivery service. The determination by the HSX Executive Committee upon appeal shall be FINAL, and there will be no further administrative rights afforded to a recipient of a sanction.

4. Procedure

The CISO and Privacy Officer are responsible for initiating an annual review of the Sanctions Policy to ensure current information and consistent policy enforcement and sanction application for privacy and security noncompliance.

5. Enforcement

The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

Participants and members are responsible for ensuring compliance with this policy for their own entities.

6. Definitions

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

7. References

Regulatory References

- HIPAA Regulatory Reference: HIPAA §164.308(a)(1)(ii)(C), HIPAA §164.414(a), HIPAA §164.530(e)
- HITRUST Reference: 02.f Disciplinary Process

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	HSX Senior Management Team HSX Privacy and Security Workgroup	**Approval Date**	December 16, 2016
Date Policy In Effect	December 16, 2015	**Version #**	1.1
Original Issue Date	December 16, 2015	**Last Review Date**	April 6, 2021 September 17, 2020 December 22, 2016

Related Documents	Anti Retaliation Policy Code of Conduct Disciplinary Employee Performance Policy GlossaryParticipation Agreement Termination Policy Whistleblower Policy