HealthShare Exchange
OF SOUTHEASTERN PENNSYLVANIA, INC.

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

Incident Management Policy

Version	Approval Date	Owner
1.0	November 29, 2018	Chief Information Security Officer

1. Purpose

This policy governs the actions required for reporting and responding to security incidents (including breaches) involving HealthShare Exchange (HSX) information assets. The policy is provided to ensure effective and consistent handling of such events to limit any potential impact to the confidentiality, availability and integrity of HealthShare Exchange information assets.

2. Scope

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

IT resources include all HSX owned, licensed, leased, or managed hardware and software, and use of the HSX network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

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

Incident Management Policy

- It is the policy of HSX to acknowledge the responsibility to mitigate, to the extent practicable, any harmful effect that is known to HSX of a use or disclosure of protected health information (PHI) in violation of its policies and procedures or the requirements of HSX or its Business Associates by federal or state law. This may include, but is not limited to, the following:

- Taking operational and procedural corrective measures to remedy violations.
- Taking employment actions to re-train, reprimand, or discipline employees and contractors as necessary, up to and including termination according to the *Sanctions Policy*.
- Addressing problems with Business Associates and Covered Entities and HSX Participants once HSX is aware of a breach of privacy.
- Incorporating mitigation solutions into other HSX policies as appropriate.
- Maintaining cyber insurance coverage at a level that is appropriate for the services offered as well as compliance with any federal or state required insurance levels.

Information Security Incident Response Capability

- HSX shall establish a formal Information Security Incident Response Capability (ISIRC) to respond, report (without fear of repercussion), escalate and treat breaches and reported security incidents.
- The ISIRC shall be documented in the Incident Response Plan which shall include the following at a minimum:
    - Incident Response Team (IRT) roles and responsibilities
    - Incident Response Procedures
    - Incident Response Communications Plan
- The Incident Response Plan shall be communicated to the appropriate individuals in HSX.
- HSX shall implement an insider threat program that includes a cross-discipline insider threat IRT.
- All employees, contractors, members, Participants, users, and third parties shall be informed of HSX's incident response policy and procedures (e.g., awareness communication, training, etc.).
- HSX shall adhere to the HITECH Act requirements for responding to a data breach of protected health information (PHI) and reporting the breach to affected covered entities in accordance with federal and state laws and regulations.

Reporting Security Incidents

- Security Incidents must be reported immediately to the Chief Information Security Officer (CISO). All employees, contractors, members, participants, users, and third parties shall be made aware of their responsibility to report any security incidents as quickly as possible.
- Employees and contractors who report security incidents in good faith shall be protected against retaliation.

- All employees, contractors, members, participants, users, and third parties of information assets and services shall report any observed or suspected security weaknesses in information assets or services to the CISO.
- Security Incidents involving civil or criminal charges shall be promptly reported to law enforcement (e.g., FBI, district attorney, state and local law enforcement, etc.) and incident reporting organizations (e.g., US-CERT) by the CISO and by legal counsel.
- Security incidents involving a breach of PHI shall be promptly reported to the appropriate regulatory agencies by the CISO as required.
- Reports and communications shall be made without unreasonable delay and no later than after the discovery of a security incident, unless otherwise stated by law enforcement orally or in writing, according to the Incident Response Communication Plan in accordance with the HSX agreements.
- Intrusion Detection/Intrusion Protection System (IDS/IPS) alerts shall be utilized for reporting security incidents.
- A log shall be maintained of unauthorized disclosures of PHI.

Responding to Security Incidents

- Management responsibilities and Incident Response Procedures shall be established to ensure a quick, effective, and orderly response to security incidents.
- The CISO shall be the point of contact for coordinating security incident responses.
- An incident response support resource shall be available to offer advice and assistance in regards to the handling and reporting of security incidents in a timely manner.
- Following a security incident, audit trails and evidence shall be secured in accordance with reasonable chain of custody procedures, system and data access controlled, emergency actions documented, actions reported to senior leadership, and system and control integrity confirmed.
- Change management requests shall be opened for events that require permanent fixes.
- Where action against a person or organization after a security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdictions.

Reviewing Security Incidents

- HSX shall put mechanisms in place to quantify and monitor the types, volumes, and costs of security incidents.
- The information gained from the evaluation of security incidents shall be used to identify recurring or high impact security incidents.

- Security incidents (or a sample of security incidents) shall be reviewed on a periodic basis to identify necessary improvements to security controls.
- Incident response testing exercises shall be planned at least annually. The results of the exercises must be documented and must be used to update the Incident Response Plan and Incident Response Procedures.

4. Enforcement

- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- Employees, contractors, members, participants, users, and third parties shall cooperate with security incident investigations (e.g., federal and state investigations, disciplinary proceedings, etc.).
- HSX shall employ any necessary audits of employee devices as per the End User Computing Device Security Policy.
- HSX shall take appropriate action against employees, contractors, members, participants, users, and third parties that fail to cooperate with security incident investigations in accordance with the *Sanctions Policy*.

5. Definitions

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

6. References

Regulatory References

- HIPAA Regulatory Reference: HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(6)(i), HIPAA §164.308(a)(6)(ii), HIPAA §164.314(a)(2)(i), HIPAA §164.402, HIPAA §164.404(a)(1), HIPAA §164.404(a)(2), HIPAA §164.404(b), HIPAA §164.404(c)(1), HIPAA §164.404(c)(2), HIPAA §164.404(d)(1), HIPAA §164.404(d)(2), HIPAA §164.404(d)(3), HIPAA §164.406(a), HIPAA §164.406(b), HIPAA §164.406(c), HIPAA §164.408(a), HIPAA §164.408(b), HIPAA §164.408(c), HIPAA §164.410(a)(1), HIPAA §164.410(a)(2), HIPAA §164.410(b), HIPAA §164.410(c)(1), HIPAA §164.410(c)(2), HIPAA §164.412, HIPAA §164.414(b), 164.530(f)
- Health Information Technology for Economic and Clinical Health ("HITECH") Act § 13402

- HITRUST Reference: 11.a Reporting Information Security Events, 11.b Reporting Security Weaknesses, 11.c Responsibilities and Procedures, 11.d Learning from Information Security Incidents, 11.e Collection of Evidence
- PCI Reference: PCI DSS v3 11.1.2, PCI DSS v3 12.10, PCI DSS v3 12.10.1, PCI DSS v3 12.10.2, PCI DSS v3 12.10.3, PCI DSS v3 12.10.4, PCI DSS v3 12.10.5
- PA eHealth Reference: 8.0. Data and Privacy Breaches, 8.1. Breach Notification and Reporting, 8.2. Privacy Violations, Breach Report Handling, and Possible Consequences, 8.3. Reconsiderations
- Pennsylvania Breach of Personal Information Notification Act 73 P.S. § 2301 – 2329

Policy Owner	Daniel Wilt	**Contact**	Daniel.Wilt@healthshareexchange.org
Approved By	HSX Leadership	**Approval Date**	November 29, 2018
Date Policy In Effect	November 29, 2018	**Version #**	1.0
Original Issue Date	November 29, 2018	**Last Review Date**	November 29, 2018
Related Documents	Breach of Privacy Complaint Form End User Computing Device Security Policy Glossary Incident Response Plan Privacy and Security Incident Reporting Form Sanctions Policy Business Associate Agreement Template		