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

Security and Privacy Breach Notification

Version	Approval Date	Owner
1.1	May 17, 2017	Privacy Officer

1. Purpose

To ensure that the HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) maintains policies and procedures regarding how to detect and manage the investigation and reporting of a security or privacy incident or breach. In its role as a Business Associate to the Covered Entities that participate in the health information exchange, HSX is responsible for coordinating the evaluation of potential breaches in concert with the HSX Members/Participants.

2. Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX Data are required to comply with this policy.

3. Policy

HSX complies with federal and state law regarding security breach notification requirements applicable to a "Security Breach" of "Protected Health Information" (PHI) or "Personal Information" (PI) as such terms are defined under the applicable laws. Specifically, in the event of a Security Breach of PHI and/or PI, the following applicable standards shall apply:

- The HITECH Act, and specifically §13402 (the "Breach Statute");
- HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule"); and
- Applicable State Breach Notification Laws.

Collectively, these standards shall be referred to in this Policy as the Security Breach Notification Laws.

HSX acts in concert with the requirements outlined in the Participation Agreement (PAR) and Business Associate Agreements (BAA) it has executed with its Members/Participants.

The employees, interns, contractors and third parties of HSX participate in education and training sessions provided by HSX as per the *Privacy and Security Awareness Education and Training* policy. Initial training regarding security breach notification obligations of the employees, interns, agents, contractors and consultants shall have been completed no later than the date by which an end User gains access to PHI.

HSX Members/Participants are required to stay abreast of HSX policies and to comply with them in accordance with the PAR.

Security Incident Examples

The following actions constitute misuse of HSX IS resources and are strictly prohibited. Prohibited actions include but are not limited to:

- Using HSX systems or information for personal financial gain or to solicit others for activities unrelated to HSX business.
- Browsing patient, personnel, financial or other corporate information without authorization (e.g., for the purpose of satisfying personal curiosity or with the intent of improperly disclosing that information).
- Intentionally interfering with the operations of any HSX computer system or using a HSX computer to disrupt or circumvent the security measures of any computing system.
- Altering or deleting information or software, except when performing authorized business functions.
- Creating, installing unapproved, unauthorized or illegally copied software, including games, on a computer and knowingly distributing software.
- Modifying or reconfiguring the software or hardware of any HSX IS resource without proper authorization.
- Attempting to circumvent, assisting someone else in circumventing or requesting that someone else circumvent any security measure or administrative access control that pertains to HSX IS resources.
- Permitting someone to use another person’s User ID, or using someone else’s User ID. This includes permitting IS administrators to use User IDs or passwords.
- Failing to protect a password from unauthorized use.
- Unapproved system cracking (hacking), password cracking (guessing), file decryption, or bootleg.
- Software copying, or similar unauthorized attempts to compromise security measures are unlawful, and will be considered serious violations of HSX policy and will result in disciplinary actions.

Privacy Incident Examples

The following actions constitute inappropriate use, disclosure and request of information assets and are strictly prohibited. Specific examples of privacy incidents or violations are better understood by understanding HSX privacy procedures. However, prohibited actions include but are not limited to:

- Unauthorized Disclosure Outside HSX
- Inappropriate Use Within HSX
- Unauthorized Use or Disclosure by Business Associate
- Failure to use reasonable safeguards when using or disclosing PHI
- Failure to adhere to any HSX privacy procedure

4. Procedures

1. **Detection and Internal Reporting**
   a. In accordance with its Audit and Monitoring Policy, HSX will establish mechanisms for detection of any privacy and/or security breaches. HSX will Implement reasonable and appropriate procedures to detect potential or actual Security Breaches.
   b. Any employee, intern, consultant, agent or vendor/subcontractor who obtains information or has reason to believe that a Security Breach and/or inadvertent data disclosure has or may have potentially occurred and involves PHI or PI created or maintained by HSX, shall be required to promptly report such information to HSX.
   c. As a downstream-Business Associate (BA) of HSX participating organizations, contracted vendors shall report discovery of any Security Breaches as soon as reasonably practicable but in any case within the timeframe specified in its HIPAA BAA with HSX. Such information as required by the HIPAA BAA, and as required by HITECH, shall be provided in order for HSX to appropriately notify all required parties.
   d. HSX Members/Participants are required to report concerns related to any potential misuse of Data including suspected Security Breaches or inadvertent Data disclosures.
   e. HSX shall notify the Covered Entities with whom it has executed BAAs in accordance with the required time frames in the BAA of the discovery of any Security incidents.

f. HSX shall work in concert with the Covered entities to ensure that when required by law, Individual(s) affected, and the Secretary of HHS, are notified.
g. Vendors of HSX's shall require their Sub-Contractor Business Associates to report any Security Breaches as soon as reasonably practicable from the date of constructive or actual discovery of the Security Breach.
h. HSX Privacy and Security Officer will follow the procedures outlined in the Incident Management Plan to conduct the investigation and risk assessment of a security breach.
i. HSX shall use the Privacy and Security Incident Reporting Form (Appendix A) to report the incidents to Covered Entities in accordance with the Business Associate Agreements.

2. HIPAA Presumption of Breach and Risk Assessment

It shall be presumed that an impermissible use or disclosure of PHI is a reportable Breach for purposes of HIPAA and HITECH unless HSX demonstrates that there is a low probability that the PHI was compromised. Notwithstanding the foregoing, HSX shall conduct a Risk Assessment to determine whether the impermissible use or disclosure resulted in a "low probability that the PHI was compromised". If HSX determines that there is a low probability that the PHI was compromised as a result of the impermissible use or disclosure, HSX may conclude that a Breach did not occur. Nonetheless, the ultimate decision regarding whether or not a Breach occurred remains with the Covered Entities.

At a minimum, HSX shall consider and assess the following factors when conducting a Risk Assessment:

a. **The Nature and Extent of the PHI.** For this factor, HSX shall consider the type of PHI involved, such as if the PHI was of a more "sensitive" nature. An example is if credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud are involved, then this would cut against finding that there is "low probability" that the PHI was compromised. With respect to clinical information, consider things like the nature of the services, as well as the amount of information and details involved. "Sensitive" information is not just information such as STDS, mental health or substance abuse.
b. **The Unauthorized Person who Disclosed/Used the PHI.** For this factor, HSX shall consider who the unauthorized recipient is or might be. For example, if the recipient person is someone at another participating organizations or HISP, then

this may support a finding that there is a lower probability that the PHI has been compromised since Covered Entities and Business Associates are obligated to protect the privacy and security of PHI in a similar manner as the Covered Entity or Business Associate from where the breached PHI originated. Another example given is if PHI containing dates of healthcare service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the PHI has been compromised.

c. **Whether the PHI was actually Acquired/Viewed.** For this factor, HSX must investigate and determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. One example given here is where a HSX mails information to the wrong individual who opens the envelope and calls the HSX to say that he/she received the information in error. In contrast, a lost or stolen laptop is recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, the HSX could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

d. **Mitigation.** For the fourth and final factor, HSX must consider the extent to which, and what steps need to be taken to mitigate, and once taken, how effective the mitigation was. For example, HSX may be able to obtain and rely on the assurances of an employee, affiliated entity, another HSX, or a HSX that the entity or person destroyed PHI it received in error, while such assurances from certain third parties may not be sufficient.

3. **Response Procedures for Breaches.** If it has been determined that there has been a Security Breach of PHI or PI as set forth, HSX shall be notified. Steps shall be taken to Mitigate any harm as best as reasonably possible. Corrective actions shall be taken, which shall be documented and retained by the Privacy or Security Officer for a period of seven (7) years. Reasonable and appropriate sanctions shall be assessed against violating employees in accordance with HSX's Sanctions Policy and Procedures.

   a. For Breaches of PHI ONLY (HIPAA HITECH):

      1. **Breaches Affecting 500 or More Patients:** If a Security Breach affects 500 or more individuals, HSX will provide Covered Entity participating

organizations with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach so that they may report such Breach to the Secretary of HHS as required by HIPAA.

2. **Breaches Affecting Fewer than 500 Patients:** If a Security Breach affects less than 500 individuals, HSX shall required the incident to be logged in a Security Breach Log (maintained by the Privacy and/or Security Officer) and HSX will notify covered entity participating organizations as required under the applicable HIPAA BAA.

5. Enforcement

- 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.
- 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 §§ 164.400-414, HIPAA § 164.308(a), HIPAA § 164.314(a), HIPAA § 164.530(e)
- HITRUST Reference: 11.a Reporting Information Security Events, 11.c Responsibilities and Procedures, 02.f Disciplinary Process

Policy Owner	Privacy and Security Officers	**Contact**	Brian.Wells@healthshareexchange.org Don.Reed@healthshareexchange.org

Approved By	HSX Management Team	**Approval Date**	May 17, 2017
Date Policy In Effect	December 23, 2013	**Version #**	1.1
Original Issue Date	December 23, 2013	**Last Review Date**	September 16, 2020
Related Documents	Glossary Incident Management Plan Information Security Management Program Policy Business Associate Agreement Participation Agreement Business Associate Policy		

Appendix A

Privacy and Security Incident Reporting Form

Date and Time of Incident	
Location of Incident (department, workstation, etc)	
Nature/description of Incident (include information system involved, hardware, software, data, physical threat or equipment, etc)	
Persons involved (include names of all parties involved)	
Person(s) immediately notified	
Immediate action taken	
Completed by Submitted to (check one)	□ Privacy/Security Official or designee □ Special Investigations Unit (check here ONLY if you wish to report incident anonymously)
Submission Date/Time	

Privacy and Security Incident Reporting Form Administrative Use

Results of investigation (include statements made by parties involved and harm or potential harm to HSX or individuals)	
Corrective action immediately taken if any	
Recommendations for improvement, if any	
Completed By	

Date and Time	