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

Third Party Risk Management Policy

Version	Approval Date	Owner
1.3	December 16, 2019	Chief Information Security Officer

1. Purpose

The purpose of this policy is to establish the methods by which HealthShare Exchange (HSX) will manage security risks that are introduced by third parties, including contracted vendor service providers and members/participants. The intent is to ensure that the security of HSX's information and information assets are not reduced when sharing information with third parties or by the introduction of third-party products or services into the HSX environment.

This policy also describes what processes must be in place before protected health information (PHI) can be released to Business Associates, and the mechanism for developing and maintaining contractual agreements with business associates regarding their responsibilities under HIPAA regulations.

2. Scope

This policy applies to all third-party arrangements, including those with Business Associates.

3. Policy

HSX shall establish third party risk management functions with the purpose of governing security risks of third-party organizations that have access to enterprise data or provide products/services for HSX.

- Responsibilities for the third-party risk management function shall include:
    - Identifying all HSX Business Associates, according to the HIPAA Security and Privacy rules.

- Vetting the security controls (e.g. policies and procedures) of third parties before establishing a third-party contract relationship.
- Ensuring an approved and up-to-date HSX Business Associate Agreement (BAA) is in place and has been signed by every third party.
- Maintaining a current and accurate listing of all HSX business associates.
- Monitoring third parties for adherence to provisions within BAAs (where applicable), Service Level Agreements (SLAs), and contractual security requirements.
- Performing on-going or continuous reviews of security measures implemented by third party service providers.
- Annually reviewing all partners'/third party-providers' information supply chain mechanisms implemented by third party service providers and establishing reasonable information security exists
- Ensuring the adherence to all other provisions within this policy.

Third Party Risk Identification:

- The potential risks to HSX information assets from business processes involving third parties shall be identified, and appropriate controls shall be implemented to mitigate these risks before granting access.
- Third parties shall only be granted access to HSX's information assets after due diligence has been conducted, appropriate controls have been implemented, and a written contract defining the terms of access has been signed.
- Due diligence by HSX to determine risk shall include interviews, and reviews of documents, checklists, and certifications.

Third Party Security Requirements:

- If appropriate, a risk assessment shall be conducted of the third party to determine the specific security requirements necessary to secure their systems to a level of risk acceptable to HSX.
- All identified third party security requirements shall be addressed and validated before granting third party access to HSX's information or information assets.
- HSX shall designate personnel security requirements including security roles and responsibilities for third-party providers in alignment with the *Access Control and Acceptable Use Policies.*

Third Party Agreements:

- Agreements with third parties involving accessing, processing, communicating or managing HSX's information assets, or adding products or services to information assets must cover all relevant security requirements and shall include all required security and privacy controls in accordance with HSX's security and privacy policies.

- The specific limitations of access or access roles, arrangements for compliance auditing, penalties, and the requirement for notification with respect to relevant third-party personnel transfers and terminations shall be identified in the third-party agreements.
- A standard BAA shall be defined. The standard BAA shall be found on the HSX intranet.
- The BAA shall include provisions for breach notification and termination upon breach.
- The BAA shall define the disposition of PHI on termination of the agreement.
- Agreements shall require and designate that it is the sole responsibility of the third party to appropriately restrict access in accordance with federal and state requirements (e.g. Super Protected Data).
- Third Party agreements shall include code/application ownership, security of the code/application, requirements to address the information security risk associated with information and communications technology services (e.g. cloud computing services) and product supply chain, and indemnification considerations.

Third Party Access Control Requirements:

- HSX shall only allow third parties to create, receive, maintain, or transmit PHI on its behalf after the organization obtains satisfactory written assurance that the third party will appropriately maintain and enforce the privacy and security of the enterprise data, including, where relevant, protecting PHI via the standard BAA.
- Third-party access shall be based on the principles of need-to-know and least privilege.
- Third-party access shall be granted only for the duration required and limited to the minimum access necessary.
- Remote access connections between HSX and third parties must be encrypted.
- Remote access connections with third parties shall be monitored on an ongoing basis.

Third Party Service Delivery:

- HSX shall require that third parties meet industry best practices and regulatory requirements for security and privacy controls and that they are implemented, operated and enforced.
- SLAs, or contracts with an agreed service arrangement, shall address liability, service definitions, security controls, and other aspects of services management.
- HSX shall develop, disseminate and update at least annually a list of current service providers.

- HSX shall address information security and other business considerations when acquiring systems or services including maintaining security during transitions and business continuity following a failure or disaster.

Third Party Service Providers Monitoring and Review:

- The services, reports and records provided by the third-party Service Provider shall be monitored and reviewed on an annual basis, and audits shall be carried out to ensure compliance with the third-party Service Provider agreements is maintained.
- The results of monitoring activities of third-party Service Provider services shall be compared against the SLA or contracts at least annually.
- Regular progress meetings shall be conducted as required by the SLA or contract to review reports, audit trails, security events, operational issues, failures and disruptions, and ensure identified issues are investigated and resolved accordingly.
- Network connections with third party Service Providers shall be periodically audited to ensure that they have implemented any required security features and meet all requirements agreed to with HSX.

Third Party Member and Participant Monitoring and Review:

- HSX shall require Members and Participants to respond to a Privacy and Security Statement prior to contract execution and eligibility to exchange information or access the exchange.
- HSX shall review each privacy and security statement for compliance with HSX requirements
- HSX shall deny membership or participation unless Member or Participant has resubmitted their privacy and security statement reflecting remediation of all identified gaps
- Members and Participants are required to notify HSX in the event that they have identified any area of non-compliance with this policy.
- HSX will conduct an annual Privacy and Security survey for a subset of the Members/Participants and review for compliance and take appropriate actions, if any, deemed necessary.
- HSX shall ensure that all Participants are aware of their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating or managing the organizations information and information assets.

Third Party Change Management:

- HSX shall only allow for source code to be developed inhouse and nothing within this policy shall constitute approval for source code development to be outsourced

- Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, considering the criticality of business systems and processes involved and re-assessment of risks.
- Third parties shall be required to coordinate, manage and communicate changes that will have an impact to HSX information, systems or processes.
- Third party changes shall be evaluated to identify the potential impacts before implementation.

4. Procedures

The following procedures apply to HSX internal operations only:

- Change Management Procedure
- Incidence Response Plan
- Third Party Vendor Selection Process
- Vulnerability Management Plan

5. Enforcement

- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
- The Member or Participant shall be responsible for enforcing compliance with this policy at minimum within their organization.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.308(a)(4)(ii)(B), HIPAA §164.308(b)(1), HIPAA §164.308(b)(3), HIPAA §164.314(a)(1), HIPAA §164.314(a)(2)(i), HIPAA §164.314(a)(2)(ii), HIPAA

§164.314(b)(1), HIPAA §164.314(b)(2)(i), HIPAA §164.314(b)(2)(ii), HIPAA §164.314(b)(2)(iii), HIPAA §164.314(b)(2)(iv), HIPAA §164.404(b), 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 §164.414(b)

- HITRUST Reference: 05.i Identification of Risks Related to External Parties, 05.j Addressing Security When Dealing with Customers, 05.k Addressing Security in Third Party Agreements, 09.e Service Delivery, 09.f Monitoring and Review of Third Party Services, 09.g Managing Changes to Third Party Services
- PCI Regulatory Reference: PCI DSS v3 2.6, PCI DSS v3 12.8, PCI DSS v3 12.8.1, PCI DSS v3 12.8.2, PCI DSS v3 12.8.3, PCI DSS v3 12.8.4, PCI DSS v3 12.8.5, PCI DSS v3 12.9
- PA eHealth Reference: 9.0. Patient Auditing and Accounting of Disclosures

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

Policy Owner	Chief Information Security Officer	**Contact**	Brian.Wells@healthshareexhange.org
Approved By	Brian Wells	**Approval Date**	December 16, 2019
Date Policy In Effect	May 13, 2015	**Version #**	1.3
Original Issue Date	May 13, 2015	**Last Review Date**	December 16, 2019 September 15, 2019 September 20, 2017
Related Documents	Access Control Policy Acceptable Use Policy Business Associate Agreement Template (BAA) Glossary Service Level Agreement Template (SLA)		