HealthShare Exchange

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

Risk Management Policy

Version	Approval Date	Owner
1.0	October 25, 2017	Chief Information Security Officer

1. Purpose

To develop and implement a Risk Management Program that addresses risk assessments, risk treatment, and risk monitoring and review.

2. Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HealthShare Exchange (HSX) enterprise data are required to comply with this policy.

3. Policy

Risk Management Program Development Policy:

- HSX shall develop and maintain a Risk Management Program to manage risk to an acceptable level.
- HSX shall maintain a formal, comprehensive program to manage the risk associated with the use of information assets.
- Information safeguards shall not be applied unnecessarily (e.g., to de-identified information).
- HSX shall implement a formal methodology for tracking risk assessments and risk treatments.

Risk Assessment Policy:

- Risk assessments shall be performed to identify, quantify and prioritize risks against operational and control objectives and to design, implement and exercise controls that provide reasonable assurance that objectives will be met and that risk will be mitigated and managed to an acceptable level.

- HSX shall perform risk assessments in a consistent way prior to production implementation of new applications or IT systems.
- HSX shall review risk assessment results at least annually, or when there are significant changes to HSX's operational environment.
- HSX shall update the results of a formal, comprehensive risk assessment every two (2) years, or whenever there is a significant change to the operational environment.
- Risk assessments shall include the evaluation of multiple factors that may impact security in addition to the likelihood and impact from a loss of confidentiality, integrity and availability of confidential data and systems.
- Risk assessments must include at a minimum:
    - Identification of the assets that are within scope.
    - Identification of the threats, the type of threats represented and their sources (e.g. hardware, software, network, media/peripherals, business process, etc.).
    - Identification of the vulnerabilities for known threats that may be exploited and which assets could be affected.
    - Identification of the controls and their status, as either existing or planned.
    - Identification of the consequences that losses of confidentiality, integrity and availability may produce.
    - Identification of specific risks, based upon relevant incident scenarios, including the identification of threats, vulnerabilities, affected assets, consequences to assets and business processes.
    - Assessment of the likelihood of occurrence of specific risks, whether qualitative or quantitative.
    - Assessment of the operational impact of specific risks.
    - Assessment of the consequences that each specific risk poses to confidentiality, accessibility, and integrity of HSX sensitive information.
    - Application of a risk estimation methodology (either qualitative or quantitative) to measure risk levels
    - Estimation of the level of risk with appropriate values assigned.
    - Evaluation and prioritization of the risks in relation to incident scenarios and risk levels.
- The likelihood and magnitude of harm (impact) from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the confidential data it processes, stores, or transmits shall be included in the risk assessment process. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).

Risk Management Policy:

- Risks shall be reduced to the lowest acceptable level.
- Risks and non-conformities shall be identified, evaluated, and prioritized.
- A Risk Management Plan shall be developed to identify resources, responsibilities, and priorities for managing information security risks.
- The Risk Management Plan shall be reviewed and updated on an annual basis.
- HSX must apply and document one or more of the following risk response measures to each identified risk:
    - Avoidance: Avoid the risk by eliminating it via alteration of business practice, applying technology, etc.
    - Mitigation: Reduce the level of risk and/or its impact to the organization.
    - Transfer: Transfer the risk to another organization (e.g., vendor or business partner) via contractual agreement or insurance policy.
    - Manage: Choose to accept and manage the risk.
- HSX shall mitigate any harmful effect that is known of a use or disclosure of protected health information (PHI) in violation of its policies and procedures.
- HSX shall implement a process for ensuring that corrective action plans and the remedial information security actions necessary to mitigate risk for the security program and the associated organizational information systems are prioritized, maintained and documented.
- HSX shall review corrective action plans (plans of action and milestones) for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
- HSX shall update existing remediation or corrective action plans quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Risk Monitoring and Review:

- Risks shall be continually evaluated and assessed.
- Risks and their factors (asset value, impacts, threats, vulnerabilities, and likelihood) shall be monitored and reviewed regularly to identify any changes.
- Review incidents of non-compliance and determine whether to waive compliance to the policy and accept the risks.
- HSX shall review and update policies on an annual basis.
- HSX shall review any proposed changes to policies and procedures, non-compliant situations, and exceptions to policies at least annually.

4. Enforcement

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

5. Definitions

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

6. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308 (a)(1)(i), HIPAA § 164.308 (a)(1)(ii)(A), HIPAA § 164.308 (a)(1)(ii)(B), HIPAA § 164.308 (a)(2), HIPAA § 164.308 (a)(7)(ii)(E), HIPAA § 164.316(a), HIPAA § 164.402
- HITRUST Reference: 03.a Risk Management Program Development, 03.b Performing Risk Assessments, 03.c Risk Mitigation, 03.d Risk Evaluation
- PCI Reference: PCI DSS v3 12.2

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org
Approved By	HSX Management	**Approval Date**	October 25 2017
Date Policy In Effect	October 25, 2017	**Version #**	1
Original Issue Date	October 25, 2017	**Last Review Date**	December 1, 2018
Related Documents	Glossary Risk Management Plan Security Gap and Risk Annual Assessment		