Audit Logging and Monitoring Policy

1. Purpose
To address the regulatory requirements for safeguarding the confidentiality, integrity, and availability of HealthShare Exchange (HSX) information assets through auditing, logging, and monitoring activities.

To verify compliance with access controls and administrative and other safeguards developed and implemented to prevent/limit inappropriate access to data.

To ensure that routine and random audits are utilized as oversight tools for recording and examining access to information through HSX (e.g., who accessed what data and when).

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 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
Audit Policy
- To ensure that appropriate safeguards are in place and effective, HSX shall audit, log, and monitor access and events to detect, report, and guard against:
  - Network vulnerabilities and intrusions
- HSX is committed to conducting business in compliance with all applicable laws, regulations and HSX policies. In particular, HSX is committed to compliance with the HIPAA Security Rule requiring security activity reviews for systems processing enterprise data.
- The planning activities for the annual audit that is required to comply with the Information Security Management Program Policy shall give consideration to risk, involvement of technical and business staff, other ongoing projects, and business endeavors that may impact the effectiveness of the audit.
- Business Associate Agreements (BAAs) with third parties shall define auditing and logging requirements and shall require monitoring of access to detect unauthorized activity and access to HSX confidential data in accordance with the Third Party Risk Management Policy.

Auditable Events
- HSX shall develop and implement an Audit Event Plan to identify which systems, applications, and processes carry out auditing activities.
- The Audit Event Plan shall define what types of events are subject to auditing. At a minimum, the following events may be audited:
  - Normal system events (e.g., startup, shutdown, login attempts, errors, security policy changes, software installations, etc.).
  - Information changes (e.g., create, read, update, delete) including confidential data.
  - Unauthorized access to confidential data for non-permitted purposes this includes accessing records for self, family member, VIP, or neighbor.
  - System management activities including execution of privileged functions.
  - Information exchanges containing confidential data.
- The Audit Event Plan shall provide a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.
- The Chief Information Security Officer (CISO) shall periodically review and update the Audit Event Plan. This review shall include consideration of events that require auditing on a continuous basis, and events that require auditing in response to
specific situations based upon an assessment of risk. Note: The specifics of the Audit Event Plan are not outlined in this policy but would be covered in the HSX procedures to allow greater flexibility because the auditable event process could change with time.

- HSX shall coordinate the security audit function with Third Party Service Providers requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

**Content of Audit Records**

- HSX shall define the content for each type of audit record in the Audit Event Plan. Audit record content shall provide sufficient detail to determine whether a given individual took a particular action.
- Audit records of information exchanges containing confidential data shall include the date, time, origin and destination of the message, but not its contents.
- All disclosures of confidential data within or outside of the HSX HIE shall be logged including type of disclosure, date and time of the event, recipient, and sender.
- Perimeter devices additionally log packet denials.

**Audit Record Retention**

- Audit Records shall be retained and archived for a minimum of ten (10) years in accordance with the Compliance Policy to meet regulatory and organizational record retention requirements. An exception to this is that audit logs for newborns shall be retained for twenty-one (21) years.

**Audit Record Storage Capacity**

- HSX shall allocate sufficient audit record storage capacity to reduce the likelihood of such capacity being exceeded.
- HSX shall configure auditing processes to reduce the likelihood of the audit record storage capacity being exceeded.
- Systems shall alert System Administrators when the allocated audit record storage reaches 80% of its capacity.

**Audit Record Generation**

- Audit records recording user activities including access to protected health information (PHI), exceptions, and events shall be generated and retained for ten (10) years to assist in future investigations and access control monitoring.
- Systems shall provide audit record generation capability as defined in the Audit Event Plan.
- Systems shall allow System Administrators to select which auditable events are audited by specific components of the system.
• Systems shall generate audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Audit record content shall also provide sufficient detail to determine whether a given individual took a particular action associated with an event.
• Systems shall generate audit records that contain the activities of privileged users as defined in the Audit Event Plan.

**Protection of Audit Records**

• Access to audit logging systems and system audit tools shall be limited to those with a job-related need according to the *Access Control Policy* to protect against possible misuse of the tools or compromise to the audit records.
• Access to audit records shall be limited to those with a job-related need according to the Access Control Policy to prevent misuse or compromise of audit records.
• Audit records shall be immutable and shall be protected against modification and deletion by anyone regardless of access privilege according to the Access Control Policy.
• Attempts to access the audit logging systems and audit records shall be logged and the audit records shall be protected from modification and deletion.
• HSX shall implement file-integrity monitoring (or change detection software) to ensure that modifications to existing audit records generate an alert to the System Administrator. Note that the creation of new audit records should not trigger an alert.
• Audit records for external-facing technologies (e.g., wireless, firewalls, DNS, etc.) shall be stored on a server located on the internal network.

**Audit Monitoring, Review, Analysis and Reporting**

• HSX shall review and analyze audit records for evidence of suspicious, unusual, and inappropriate activity on an ongoing basis.
• HSX shall report anomalous auditable events and related security incidents to the CISO, who shall be responsible for reporting security and compliance issues to senior leadership as appropriate.
• HSX shall adjust the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations based on law enforcement information, intelligence information, or other credible sources of information.
• HSX shall establish procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities shall be reviewed on a regular basis.
• HSX shall review any unauthorized access to the network and information systems at least once every quarter, with appropriate action being taken upon discovery of unauthorized access.
• Monitoring activities shall include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.
• HSX shall meet all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.
• HSX shall ensure that Third Party Service Providers employ automated Intrusion Detection (IDS) and/or Intrusion Prevention Systems (IPS) according to the Network Protection Policy to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to unauthorized access and unexpected traffic.
• Monitoring shall include inbound and outbound information exchanges and file integrity monitoring.
• HSX shall analyze and correlate audit records across different repositories and correlate this information with input from non-technical sources.
• HSX will conduct analyses to detect trends and/or patterns of use.
• System Administrator activities shall be logged and reviewed on a regular basis.
• Audit logs shall not be considered part of the designated record set, and patients shall not have the right to access audit logs. However, audit logs may be used to respond to a patient’s request for an accounting of disclosures.
• In the event of an extract of covered information, the CISO shall verify every ninety (90) days for each extract of covered information recorded that the data is erased, or its use is still required. If use of covered information is still required, then access will be granted for another ninety (90) days. Any extract of covered information shall require the CISO’s permission. Upon permission being granted, the CISO shall maintain a record and update as needed.
• HSX monitors the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state.

Audit Reduction and Report Generation

• HSX shall utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered.
• Systems shall provide audit reduction and report generation capability.
• Auditing and monitoring systems shall have the capability to automatically process audit records for events of interest based upon selectable event criteria.
Response to Alerts

- Systems shall alert System Administrators in the event of an audit processing failure and System Administrators shall take remediation action.
- Systems shall generate alerts for suspicious activity and security alerts. System Administrators shall analyze the alerts and investigate suspicious activity or suspected violations.
- Automated Systems (e.g., IDS, IPS) shall support near real-time analysis and alerting of adverse events (e.g., malicious code, potential intrusions, etc.) and integrate intrusion detection into access and flow control mechanisms. The events that trigger real-time alerts shall be defined in the Audit Event Plan.
- System faults shall be logged and analyzed, and System Administrators shall take appropriate remediation action.

Clock Synchronization

- HSX shall synchronize system clocks with a real-time clock set to Coordinated Universal Time (UTC) to support tracing and reconstitution of activity timelines.
- System clocks shall be synchronized daily and at system boot.
- HSX shall restrict authorization to change system time settings to those with a job-related need.
- Changes to system clocks on critical systems shall be logged, monitored and reviewed.

4. Procedure

The following procedures apply to HSX internal operations only:

- Audit Logging and Monitoring Procedure
- Continuous Monitoring Procedure
- Incident Response Plan

5. Enforcement

- The CISO shall be responsible for enforcing compliance with this policy under the direction of the President.

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)(B), HIPAA §164.308(a)(1)(ii)(C), HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.308(a)(4)(i), HIPAA §164.308(a)(4)(ii)(B), HIPAA §164.308(a)(5)(ii)(C), HIPAA §164.310(a)(2)(ii), HIPAA §164.312(b), HIPAA §164.316(a), HIPAA §164.316(b)(1), HIPAA §164.316(b)(2)(iii)
- HITRUST Reference: 06.i Information Systems Audit Controls, 06.j Protection of Information Systems Audit Tools, 09.aa Audit Logging, 09.ab Monitoring System Use, 09.ac Protection of Log Information, 09.ad Administrator and Operator Logs, 09.af Clock Synchronization
- PCI Reference: PCI DSS v3 10.1, PCI DSS v3 10.2, PCI DSS v3 10.2.1, PCI DSS v3 10.2.2, PCI DSS v3 10.2.3, PCI DSS v3 10.2.4, PCI DSS v3 10.2.5, PCI DSS v3 10.2.6, PCI DSS v3 10.2.7, PCI DSS v3 10.3, PCI DSS v3 10.3.1, PCI DSS v3 10.3.2, PCI DSS v3 10.3.3, PCI DSS v3 10.3.4, PCI DSS v3 10.3.5, PCI DSS v3 10.3.6, PCI DSS v3 10.4, PCI DSS v3 10.4.1, PCI DSS v3 10.4.2, PCI DSS v3 10.4.3, PCI DSS v3 10.5, PCI DSS v3 10.5.1, PCI DSS v3 10.5.2, PCI DSS v3 10.5.3, PCI DSS v3 10.5.4, PCI DSS v3 10.5.5, PCI DSS v3 10.5.6, PCI DSS v3 10.6, PCI DSS v3 10.6.1, PCI DSS v3 10.6.2, PCI DSS v3 10.6.3, PCI DSS v3 10.7, PCI DSS v3 11.5, PCI DSS v3 11.5.1, PCI DSS v3 A.1.3
- PA eHealth Reference: 4.0. Authority Auditing

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Daniel Wilt</th>
<th>Contact</th>
<th><a href="mailto:Dani/e.wilt@healthshareexchange.org">Daniel.wilt@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By</td>
<td>Board</td>
<td>Approval Date</td>
<td>November 8, 2018</td>
</tr>
<tr>
<td></td>
<td>HSX Management Team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSX Privacy and Security Workgroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Policy In Effect</td>
<td>June 4, 2015</td>
<td>Version #</td>
<td>1.4</td>
</tr>
<tr>
<td>Original Issue Date</td>
<td>June 4, 2015</td>
<td>Last Review Date</td>
<td>November 8, 2018</td>
</tr>
<tr>
<td>Related Documents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Event Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach Notification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Associate Agreement Template (BAA)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Glossary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Management Program Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Protection Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Termination Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Risk Management Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>