HealthShare Exchange
OF SOUTHEASTERN PENNSYLVANIA, INC.

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

Audit Logging and Monitoring Procedure (V1.1)

Procedure

HSX will perform the following activities each month looking for suspected misuse of protected health information. This procedure applies to all employees, interns, contractors, and users accessing HSX's data and systems. All users are notified of monitoring and consent to having their activity monitored. Monitoring includes privileged operations, authorized access, unauthorized access attempts, and system alerts or failures. Separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems. Separation of duties is maintained and accomplished in HSX by segregating the duties of individual. User who request access is never the user who authorize/provide access.
Access to system audit tools and audit trails is protected and controlled to prevent unauthorized access and use. Administrators are the only users allowed to access system audit tools and audit trails.

90 Day Inactivity

HSX will lock accounts that have been inactive for more than 90 Days. Except for specific accounts that are used for specific Use Cases that require them to be activated upon and are already locked until needed.

Audit Records

A secure audit log record is created for all activities on the system (create, read, update, delete) involving covered information. Authorized access and unauthorized access attempts to the audit systems and audit trails is logged and protected from modification in line with HSX's Audit Logging and Monitoring Policy. Event logs are not to be kept on the same server as the application.

Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e.g., A/V and IDS), and identification and authentication mechanisms, and creation and deletion of system-level objects.

Audit logs are maintained for management activities, system and application startup/ shutdown/errors, file changes, and security policy changes.

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

Auditing and monitoring systems employed by HSX support audit reduction and report generation.

The organization's system clocks are synchronized to an agreed, authoritative real-time standard (e.g., daylight savings time) and synchronize daily and at system boot. The agreed, authoritative real-time standard is in compliance with The Official NIST US time. Time data is protected and controlled from unauthorized access. No single person is able to access, modify, or use information systems without authorization or detection. No single person is able to access or modify the time zone settings. Any changes, including deletions from the event log are tracked in the event log.

Laptops are synchronized from time zones automatically based on current location (eastern daylight, closest city being Philadelphia), date and tie set automatically time.apple.com (every hour).

Mirth applications are synchronized from the west coast but they are translated to the east coast. Translated to the current time zone of your location.

[REDACTED] instances are synchronized from UTC/GMT time, everything is programmed in UTC time.

- All audit information is stored and archived in the Mirth application forever. Access to the audit logs are restricted to administrators only. Individuals responsible for administering access is limited to the minimum necessary based upon each users' role and responsibilities and these individuals cannot access audit functions related to these controls.
- The information system is able to automatically process audit records for events of interest based on selectable criteria.
    1. Log into the specific Mirth application that is being monitored (e.g. Mirth Results, Mirth Match, Mirth Mail, Mirth SSO)
    2. Click on the "Administration" tab
    3. Under the "Auditing" section, click on "Event log". The Event Log lists events in chronological order
    4. Events can also be found by conducting an "Advanced Search"
        a. Search by user name or Participant ID
        b. Filter by event outcomes (success/failure)
        c. Search by words or phrases
        d. Search by date/time range

All audit log records include but are not limited to the following:

- the unique user ID
- unique data subject ID,
- function performed
- date/time the event was performed.
- activities of privileged users (administrators, operators, etc.) including the success/ failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event.

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

- Messages sent and received including the date, time, origin, and destination of the message
- management activities,
- system and application startup/shutdown/errors,
- file changes,
- security policy changes,
- file integrity monitoring,
- time data

Extract of Covered Information

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.

Automated Systems

Automated systems deployed throughout HSX are used to monitor key events and analyze system logs, the results of which are reviewed at least annually by the CISO. Automated systems support near real-time analysis and alerting of events (e.g., malicious code, potential intrusions) and integrate intrusion detection into access and flow control mechanisms.
HSX uses [Redacted] to monitor for privacy and security breaches surrounding covered information.

- All event logs are sent daily to [Redacted] for monitoring purposes.
- [Redacted] runs algorithms and metrics against HSX's event logs daily and monitors users in search for suspicious activity
- Any and all suspicious activity to reported to HSX as potential privacy and security breaches each day as such suspicious activity may be found.
- HSX's Technical Operations team and CISO review alerts whenever received and decide whether or not to proceed with investigations as may be required
- Once an investigation is launched, all information on the user in question is reviewed. If needed, the CISO will conduct an interview with the user in question
- HSX's Technical Operations team and CISO will decide if the reported suspicious activity is indeed a breach or not.

HSX also uses [Redacted] to analyze and correlate audit records across different repositories and correlates this information with input from non-technical sources. HSX copies all events and sends them to [Redacted] for analysis.

- [Redacted] combines HSX's data repository and SSO with supplemental information from [Redacted]. The combination of this information is tied out to algorithms to conduct audits and monitoring.

HSX uses TrendMicro for IPS monitoring

- All event logs are sent to TrendMicro for monitoring purposes.
- TrendMicro runs algorithms and metrics against HSX's event logs and monitors users in search for suspicious activity
- Any and all suspicious activity to reported to HSX as potential privacy and security breaches.
- HSX's Technical Operations team and CISO review alerts and decide to proceed with investigations
- Once an investigation is launched, all information on the user in question is reviewed. If needed, the CISO will conduct an interview with the user in question
- HSX's Technical Operations team and CISO will decide if the reported suspicious activity is indeed a breach or not.

Monitoring Communications

- All outbound email messages are scanned for PHI and automatically encrypted if detected
- All outbound but internal emails are on a TLS (encrypted) connection
- All inbound emails comply with HSX's [Redacted] policies which block any non-standard document types
    - HSX allowed document types are: Word, PDF, PPT, Excel, and JPEG.

Development Functions and Procedure

- The Enterprise Architect (EA) is responsible for developing patterns between systems and applications.
- The patterns developed by the EA is passed down to a Solutions Architect (SA) who is responsible for creating the actual solution or application's architecture.
- The Development Team is tasked with delivering the final deliverable. The Development Team is ran by a Project Manager (PM).
- During the Project Review Meeting, the Development Team reviews and approves the project's scope and specifications
- After the development phase, the testing plan is developed.
- After the testing plan is implemented and approved, the solution is ready to go to production given the PM's approval.
- A change request is submitted for the Change Management Team to review. The change request documents all technical details, affected systems, data handling specifications, and impact on privacy and security.
- After the Change Management Team approves the change request, the solution/ application is ready to go to production.

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

- During production, the Implementation Team monitors for changes, outliers, and system performance effects.
- After the defined monitoring period, if there are no potential bugs identified, the solution/application is sent to the Operations Team.
- The Operations Team assumes responsibility for monitoring, supporting, and updating the solution/application.

Use Cases

Direct Secure Messaging (DSM)

The following HSX Systems are used for Direct Secure Messaging: Mirth Single Sign On and Mirth Mail.

Auditing Activities

- User Login and Logout
- User Password Resets
- Direct Secure Messaging Sent and Received
- User Account Delegates
- User Account Management
- Security Role Management

Encounter Notification Service (ENS)

The following HSX Systems are used for Encounter Notification Service: Ai ENS, Mirth Connect, Mirth Match, and Mirth Results.

Auditing Activities

- Patient or Member Panel Validation
- User Login and Logout (Mirth Mail)
- User Password Resets (Mirth Mail)
- Direct Secure Messaging Sent and Received
- User Account Delegates (Mirth Mail)
- User Account Management (Mirth Mail, SSO)
- Security Role Management (Mirth Mail, SSO)
- Subscribed Types of Encounter Notifications Validation

Clinical Activity History

The following HSX Systems are used for Direct Secure Messaging: Mirth Single Sign On, Mirth Mail, Mirth Match, and Mirth Results.

Auditing Activities

- User Login and Logout
- User Password Resets

Automated Care Team Finder

The following HSX Systems are used for Direct Secure Messaging: Mirth Single Sign On, Mirth Mail, Mirth Match, and Mirth Results.

Auditing Activities

- User Login and Logout
- User Password Resets

Clinical Data Repository (CDR) for Treatment

The following HSX Systems are used for Direct Secure Messaging: Mirth Single Sign On, Mirth Mail, Mirth Match, and Mirth Results.

Auditing Activities

- User Login and Logout
- User Password Resets
- User Account Management
- Security Roles Management
- CDR PHI View and Management
- Consent Management
- Concepts Management
- External Networks PHI View and Management

Health Plan Quality Reporting

The following HSX Systems are used for Health Plan Quality Reporting: Mirth Single Sign On, Mirth Match, and Mirth Results.

Auditing Activities

- Patient or Member Panel Validation
- User Login and Logout
- User Password Resets
- User Account Management
- Security Roles Management
- CDR PHI View and Management
- Consent Management
- Concepts Management
- Self Pay Information
- Participation Organizations

Urgent Patient Activity Liaison (UPAL)

The following HSX Systems are used for Urgent Patient Activity Liaison: Mirth Single Sign On, Mirth Match, and Mirth Results.

Auditing Activities

- User Login and Logout
- User Password Resets
- User Account Management

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

- Security Roles Management
- CDR PHI View and Management
- Consent Management

Clinical Data Repository (CDR) for External Networks

The following HSX Systems are used for Clinical Data Repository for External Networks: Mirth Connect and Mirth Results.

Auditing Activities

- User Login and Logout
- User Account Management
- Security Roles Management
- CDR PHI View and Management
- Consent Management
- External Networks PHI View and Management

Customer Relationship Management (CRM)

The following HSX System are used for Customer Relationship Management: [Redacted]

Auditing Activities

- User Account Management

Mirth Single Sign On

User Access Monitoring

User Monitoring

These are the Audit Event Types that HSX will be reviewing for individual Users.

- Forgotten Password
- Forgotten Username
- Login Attempt
- Logout
- Password Change

Administrative Monitoring

These are the Audit Event Types that HSX will be reviewing for administrative Users.

- Application Created
- Application Deleted
- Application Updated
- Delegate Created
- Delegate Removed
- Delegate Updated
- SecurityRole Created
- SecurityRole Updated

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

- SecurityRole Deleted
- Template Created
- Template Deleted
- Template Updated
- User Created
- User Deleted
- User Locked
- User Unlocked
- User Updated
- User Viewed

Audit Logging Event Type

These are the relevant Audit Event Types that are available in the HSX System.

- Application Created
- Application Deleted
- Application Updated
- Delegate Created
- Delegate Removed
- Delegate Updated
- Forgotten Password
- Forgotten Username
- Login Attempt
- Logout
- Password Changed
- SecurityRole Created
- SecurityRole Updated
- SecurityRole Deleted
- Template Created
- Template Deleted
- Template Updated
- User Created
- User Deleted
- User Locked
- User Unlocked
- User Updated
- User Viewed

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

Mirth Results

User Access Monitoring

User Monitoring

These are the Audit Event Types that HSX will be reviewing for individual Users.

- Bypass User Access Control
- Forgotten Password
- Forgotten Username
- Login Attempt
- Logout
- Password Changed
- View PHI

External Networks

These are the Audit Event Types that HSX will be reviewing for external network Users.

- InboundDocumentQuery:NwHIN
- InboundDocumentRetrieve:NwHIN
- OutboundDocumentQuery:NwHIN
- OutboundDocumentRetrieve:NwHIN

Consent Management

These are the Audit Event Types that HSX will be reviewing for consent Users.

- Consent Added
- Consent Deleted
- Consent Edit
- Create Consent
- Create or Update Consent
- Update Consent

Administrative Monitoring

These are the Audit Event Types that HSX will be reviewing for administrative Users.

- Audit Access
- Clinical Item Removed
- Coded Element and Concept Auto-Mapper
- Coded Element and Concept Mapped
- Coded Element and Concept Unmapped
- Create or Update Concept
- Create or Update Patient
- Create or Update Patients
- Create or Update User
- Delete User
- Event View

- SecurityRole Created
- SecurityRole Deleted
- SecurityRole Updated
- SecurityRole View
- User Created
- User Deleted
- User Locked
- User Unlocked
- User Updated by SSO

Reports

Clinical Items Access Individual Details

Individual Details with User Name, Event Date and Time, Type of Event, Source Facility, HSX ID, First Name, Last Name, Date of Birth

Parameters

Report Start Date
Report End Date

Clinical Items Access

Summary Graph with Type of Data Accessed

Parameters

Graph Friendly: Yes, No
Aggregation Type: Weekly, Monthly

Mirth Results Activity Report

Summary of Activity Report

Patient Searches

Summary with Week Starting, Week Ending, Successful Patient Searches, Unsuccessful Patient Searches, Running Total Successful Patient Searches, Running Total Unsuccessful Patient Searches

Parameters

Report Type: Exclude Administrators, Include Administrators
Aggregation Type: Weekly, Monthly

Patient Searches Individual Details

Individual Details with User Name, Event Date, Search Criteria, Result Rows, IP Address

Parameters

Report Start Date
Report End Date
Report Type: Exclude Administrators, Include Administrators

Audit Logging Event Type

These are the relevant Audit Event Types that are available in the HSX System.

- Audit Access
- Bypass User Access Control
- Clinical Item Removed
- Coded Element and Concept Auto-Mapper
- Coded Element and Concept Mapped
- Coded Element and Concept Unmapped
- Consent Added
- Consent Deleted
- Consent Edit
- Create Consent
- Create or Update Concept
- Create or Update Consent
- Create or Update Patient
- Create or Update Patients
- Create or Update User
- Delete User
- Event View
- Forgotten Password
- Forgotten Username
- Login Attempt
- Logout
- Password Changed
- SecurityRole Created
- SecurityRole Deleted
- SecurityRole Updated
- SecurityRole View
- Update Consent
- User Created
- User Deleted
- User Locked
- User Unlocked
- User Updated by SSO
- View PHI

Audit Logging Event Type PA eHealth P3N

These are the relevant Audit Event Types that are available in the HSX System.

- InboundDocumentQuery:IHE
- InboundDocumentRetrieve:IHE
- InboundDocumentQuery:NwHIN
- InboundDocumentRetrieve:NwHIN

- OutboundDocumentQuery:IHE
- OutboundDocumentRetrieve:IHE
- OutboundDocumentQuery:NwHIN
- OutboundDocumentRetrieve:NwHIN

Mirth Match

User Access Monitoring

Administrative Monitoring

These are the Audit Event Types that HSX will be reviewing for administrative Users.

- Approved Workitem
- Delete Entity
- Entity Query
- Entity View
- Forgotten Passsword
- Forgotten Username
- Login Attempt
- Logout
- Password Change
- Reject Workitem
- SecurityRole Created
- SecurityRole Deleted
- SecurityRole Updated
- User Created
- User Deleted
- User Updated
- User Viewed
- Workitem Query
- Workitem View

Audit Logging Event Type

These are the relevant Audit Event Types that are available in the HSX System.

- Approved Workitem
- Delete Entity
- Entity Query
- Entity View
- Forgotten Passsword
- Forgotten Username
- Login Attempt
- Logout
- Password Change

1801 Market Street | Suite 750 | Philadelphia PA 19103 | 215.391.4905 | www.healthshareecxchange.org

- Reject Workitem
- SecurityRole Created
- SecurityRole Deleted
- SecurityRole Updated
- User Created
- User Deleted
- User Updated
- User Viewed
- Workitem Query
- Workitem View

Mirth Mail

User Access Monitoring

User Monitoring

These are the Audit Event Types that HSX will be reviewing for individual Users.

- Delegate Created
- Delegate Removed
- Delegate Updated
- Forgotten Password
- Forgotten Username
- Login Attempted
- Login Failed
- Login
- Logout Attempt
- Logout
- Password Changed
- Password Change Notification
- PasswordReset Attempt

Administrative Monitoring

These are the Audit Event Types that HSX will be reviewing for administrative Users.

- Delegate Created
- Delegate Removed
- Delegate Updated
- Entity Created
- EntityRemoved
- Entity Updated
- EntityView
- SecurityRole Created
- SecurityRole Deleted

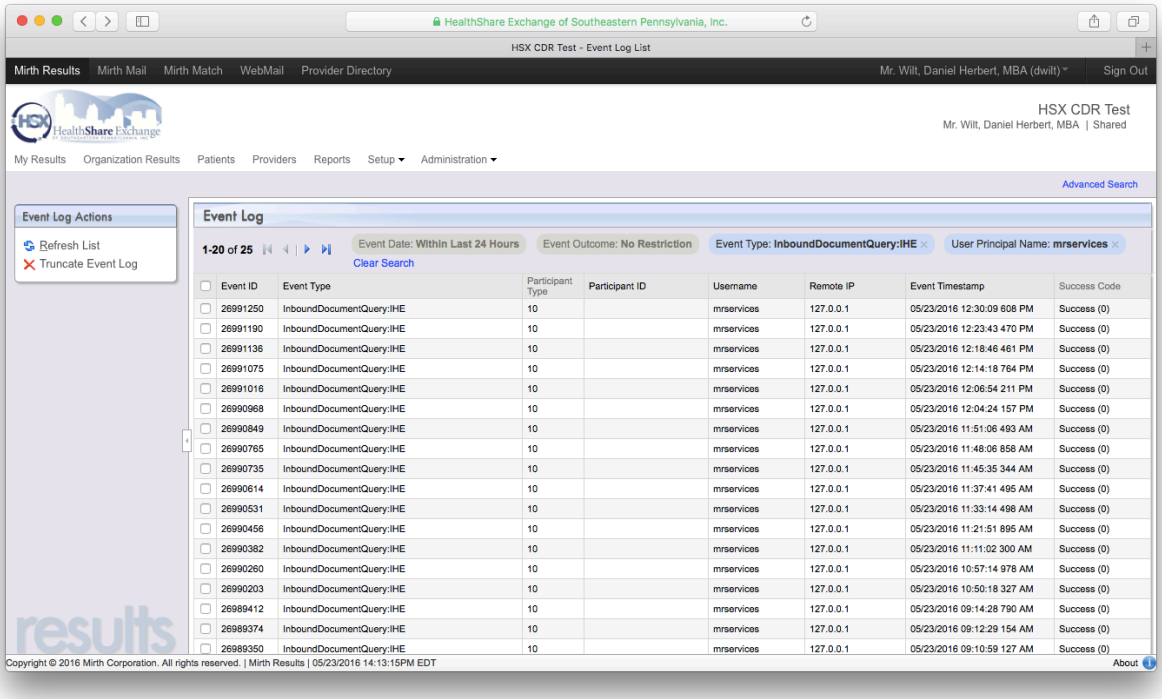
- Securityrole Updated
- User Created
- User Deleted
- User Updated
- User Viewed

Audit Logging Event Type

These are the relevant Audit Event Types that are available in the HSX System.

- Delegate Created
- Delegate Removed
- Delegate Updated
- Entity Created
- EntityRemoved
- Entity Updated
- EntityView
- Forgotten Password
- Forgotten Username
- Login Attempted
- Login Failed
- Login
- Logout Attempt
- Logout
- Password Changed
- Password Change Notification
- PasswordReset Attempt
- SecurityRole Created
- SecurityRole Deleted
- Securityrole Updated
- User Created
- User Deleted
- User Updated
- User Viewed

Audit Log Screen Shots



HSX monitors its information system to identify irregularities or anomalies which are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state.

- HSX uses [Redacted] as its main communication tool for alerts and uses [REDACTED] [Redacted] as its monitoring tool to trend resources and statistics of HSX services over a 12-hour time. The combination of these two assist HSX to identify irregularities or anomalies in the systems.
- HSX has created specific rules to check the health of its servicers and services and will send those alerts to [Redacted], notifying the Technical Operations team if one of those rules are triggered.
- HSX also has monitoring in its command center, whereby members of the Technical Operations Team monitor the screens to identify faults or issues in processing in real time.
- When alerts are sent to [Redacted], they are reviewed by the Technical Operations Team and determined if there is a risk fault or irregularity in system. If there is a risk fault or irregularity in the system, a support ticket within HSX opened up to track case from start to finish
- The case is escalated depending on responsible vendor (Mirth, AI, [Redacted], [REDACTED]) for support to resolve the observed issue.

- At this point the support process is handed off to the HSX Support Team and the standard support process is followed.
- Job descriptions and duties are defined when an employee is hired and a description is provided to all members of HSX including the hire.
- Job descriptions are reviewed on annual basis, and, if necessary, changes are communicated to the HSX Team with the redefined duties.
- If an employee has any description including typical operations, their duties will be involved in auditing, monitoring, supporting the infrastructure of HSX and all of its services
- Amon the HSX Team, there are subject matter experts for specific HSX services which are used as an escalation point. Those resources are identified within support procedures.

Responsible Owner:	Security Officer	**Contact: email**	Brian.Wells@healthshareexchange.org
Approved By:	Brian Wells	**Version #**	1.1
Current Approval Date:	December 3, 2019	**Review Dates:**	September 17, 2020 December 3, 2019 May 14, 2017
Date Procedure to go into Effect:	May 14, 2017, Approved by Daniel Wilt, CISO		
Related Documents:	Audit Logging and Monitoring Policy		