| Priority | ID | Description | Comment |
|---|---|---|---|
| Audit logs are defined as tracking mechanisms for tracing the history of who used an application/system, when they used it and what information was accessed. The audit trail includes a history of any actions taken to create, update, view, archive and/or delete data. An audit trail is mandated by HIPAA regulations for protecting a patients' medical information. There are four primary categories of reasons for auditing the HIeHR utility: accountability, reconstruction of an event, intrusion detection and problem detection. | | | |
| | **F.1** | **Viewer Audit Log Overview** | |
| | F.1.1 | An audit log is created for all system login/viewing activity, regardless of the HIeHR application used. | Viewer, Viewer Admin, HIE Admin |
| | F.1.1.1 | Log in | |
| | F.1.1.2 | Log out | Note: This is possible only if the User clicks on a logout link. The Event will not be captured if the browser window was closed (user clicks on "x"). |
| | F.1.1.3 | Session Time Out (server side) | |
| | F.1.1.4 | System Lockout due to exceeding allowed # of failed Login attempts | |
| | F.1.1.5 | Password Create/Change | |
| | F.1.2 | An audit log is created for all User Management activities: | Viewer Admin |
| | F.1.2.1 | Create a User | |
| | F.1.2.2 | Edit a User | |
| | F.1.2.3 | Inactivate a User | |
| | F.1.2.4 | Activate a User | |
| | F.1.3 | An audit log is created for all Viewer Configuration Management activities: | Viewer Admin |
| | F.1.3.1 | Create configuration data | |
| | F.1.3.2 | Update configuration data | |
| | F.1.3.3 | Inactivate configuration data | |
| | F.1.3.4 | Delete configuration data | |
| | F.1.4 | An audit log is created for all HIE Configuration Management activities: | |
| | F.1.4.1 | Create configuration data | |
| | F.1.4.2 | Update configuration data | |
| | F.1.4.3 | Inactivate configuration data | |
| | F.1.4.4 | Delete configuration data | |
| | F.1.5 | An audit log is created for the following Viewer activities: | Viewer |
| | F.1.5.1 | Search a Patient | |
| | F.1.5.2 | View Record List | |
| | F.1.5.3 | Access/View Record Detail | |
| | F.1.5.4 | Print Record Detail (Printer-Friendly View) | |
| | **F.2** | **Audit Log Detail** | |
| | F.2.1 | The following data is captured as part of every logging record, regardless of system/activity audited. | |
| | F.2.1.1 | Date/Time of Event | |
| | F.2.1.2 | Module/Component of System where Event occurred | Ex: Viewer Search, Viewer Patient Records, Viewer Record List, Viewer Admin, HIE Admin |

| Priority | ID | Description | Comment |
|---|---|---|---|
| | F.2.1.3 | Event Type | Ex: Login, Logout, Record Access, User Create |
| | F.2.1.4 | Status | Success, Failure, Canceled by User |
| | F.2.1.4.1 | If Status=Failure, Reason | Invalid User Name, Invalid Password, Password Expiration, Session Timeout |
| | F.2.1.5 | User ID | |
| | F.2.1.6 | User Name | |
| | F.2.2 | For the Viewer, the following actions/events are logged in addition to the above: | |
| | F.2.2.1 | Search Function | |
| | F.2.2.1.1 | Log the Search Criteria Entered for each Search initiated. | |
| | F.2.2.2 | Select Patient Function | |
| | F.2.2.2.1 | Log the Patient Identifier (AHCCCS Search Index) selected by the User in order to View the list of associated Records. | |
| | F.2.2.3 | Select Record to View - Log the following details for each record accessed. | |
| | F.2.2.3.1 | Patient Identifier | |
| | F.2.2.3.2 | Record Source System ID | |
| | F.2.2.3.3 | Record Type Selected for Viewing | This is the descriptor, such as "Discharge Summary," or "Lab Result." |
| | F.2.2.3.4 | Record ID Selected for Viewing | |
| ~~1~~ | ~~F.2.2.3.5~~ | ~~Access Time Elapsed~~ | At this time, there appears to be no reliable way to determine length of time a record is viewed. Access time will be limited to the user's session. We are lowering the priority, but not removing the requirement, in the hopes a solution can be developed at a later date. |
| | F.2.2.4 | Print Functions | |
| 4 | F.2.2.4.1 | Launch of the Printer-Friendly Version of a Record | |
| 1 | F.2.2.4.2 | Print of the Printer-Friendly Version of a Record | At this time, there appears to be no reliable way to determine the actual print of a record. Rather, the launch of the Printer-Friendly version must be assumed to be performed with the intention to print. We recognize this has flaws, but this is the statistic we will report, noting the distinction. We are lowering the priority, but not removing the requirement, in the hopes a solution can be developed at a later date. |
| | F.2.3 | For the Viewer Admin, the following audit detail is logged in addition to the data elements noted above (F.2.1): | |
| | F.2.3.1 | User Management | |
| | F.2.3.1.1 | User Record ID | |
| | F.2.3.1.2 | Data Element | |
| | F.2.3.1.3 | Old Value | |
| | F.2.3.1.4 | New Value | |
| | F.2.3.2 | Audit Data | |

| Priority | ID | Description | Comment |
|---|---|---|---|
| | F.2.3.2.1 | Access to the Audit Record Detail | |
| | | Accessing audit log data is logged regardless of where the log is stored, noting the following: | |
| | F.2.3.2.1.1 | Access Type | |
| | F.2.3.2.1.1.1 | Currently only Viewing audit detail is supported through the Viewer. | |
| | ~~F.2.3.2.1.1.2~~ | ~~Archive~~ | Archive activities will be performed by the DBAs at the database level. |
| | ~~F.2.3.2.1.1.2.1~~ | ~~Date Range~~ | |
| | ~~F.2.3.2.1.1.2.2~~ | ~~Criteria for Archive (Record Type)~~ | |
| | ~~F.2.3.2.1.1.2.3~~ | ~~No. of records archived~~ | |
| | ~~F.2.3.2.1.1.3~~ | ~~Restore~~ | |
| | F.2.3.3 | Reporting | |
| | F.2.3.3.1 | Report ID Initiated | |
| | F.2.3.3.2 | Report Title Initiated | |
| | ~~F.2.3~~ | ~~For the Viewer Admin, the following audit detail is logged in addition to the data elements noted above:~~ | |
| | F.2.3.4 | Configuration Management | |
| | F.2.3.4.1 | Configuration Type | |
| | F.2.3.4.2 | Data Element | |
| | F.2.3.4.3 | Old Value | |
| | F.2.3.4.4 | New Value | |
| | F.2.3.4.5 | User Making Change | |
| | F.2.3.4.6 | When deletion of a configuration record is supported, the deletion activity is logged. | Note: Deletion can only be logged if performed via the Viewer. |
| | **F.3** | **Security** | |
| | F.3.1 | Access to the Audit Log is security-controlled. | Role-based; system admin |
| | F.3.1.1 | Users with Account Management functions do not have access to the Audit Logs. | Prevents creation of an account for fraudulent purposes and then removing the audit log of that account's activity. |
| | F.3.2 | Audit Data is able to be archived to a secure location, requiring special permissions to access, view, restore archived records. | Note: Archive of the audit log is a DBA function, and will be performed and managed outside the Viewer Admin Tool. |
| | **F.4** | **Reporting** | |
| | F.4.1 | The system supports the ability to report on audit data. | |