Audit Log Review
Guidelines
Integrated Assessment Record (IAR)

Version 4.0
June 2015

Table of Contents

Introduction

The IAR audit log is a record of the software events occurring within the IAR system so each participating organization can review the events that are pertaining to their organization. The IAR audit log is composed of log entries, where each entry contains information related to a specific event that has occurred within IAR, such as a user login failure, a client search, a search for assessments, a viewing of an assessment, an assessment upload error, printing of an assessment, etc.

The IAR audit log is only accessible to privacy officers. The privacy officer of the participating organization can access the audit log file from their privacy officer account, where they can review the audit log of their respective organization. The global privacy officer (the privacy officer at the Health Integration Network Provider (HINP)), has access to the audit log of all the IAR users.

The Audit Log Review Basic Guidelines described below establish the minimum efforts for the local privacy officers to conduct audit log review activities in their respective operational environments.

The Audit Log Review Additional Guidelines included in this document are helpful examples and scenarios designed to assist the local privacy officers when conducting reviews and investigations using the audit log information.

To support the privacy officer's audit log review efforts, pre-defined audit log reports of key events have been developed to assist the monitoring and review of user activities in the privacy officer's organization.

Basic Guidelines

1. The privacy officer must review the IAR audit log frequently to look for abnormal activities and events. This should be done at minimum on a monthly basis.
2. Any suspicious or unusual event found during the audit log review must be investigated further. If applicable, an incident report should be completed, and appropriate parties should be alerted for further investigation and resolution of the incident.
3. In the event of inquiries or complaints by a client or staff member, audit logs or audit log reports must be reviewed in order to determine if an unauthorized event has occurred. As above, if applicable an incident report should be completed and appropriate parties alerted for further investigation and resolution of the incident.
4. Special attention must be paid to any events in the audit log or audit log reports that may identify potential disclosures of personal health information (PHI), such as unusually high volumes of printing, viewing, and other access events.

Additional Guidelines

The following are additional guidelines designed to help privacy officers review the IAR audit log.

1. Review Frequency

1.1 Initial reviewing frequency — For the initial three months of implementation, it is recommended that the privacy officer review the IAR audit log as often as possible or at a minimum of no less than once a week in order to:

- Familiarize themselves with the use of the audit log review user interface,
- Establish a baseline of user activities in the organization, and
- Establish a log review routine.

1.2 Ongoing reviewing frequency — Depending on the baseline established within the initial implementation period log review, the privacy officer can adjust the frequency of log review after the first 3 months.

2. Integration with Incident Management Process

2.1 As a result of conducting the review of the audit log and audit reports and any associated investigation, the privacy officer may need to alert other participating organizations (or the HINP) if the privacy officer uncovers an incident that affects these parties. Refer to the *Integrated Incident Management process* for details of how to escalate and communicate with the HINP and other participating organizations.

3. Log Review Techniques

3.1 Use of the CSV export function — All audit log reports displayed on the screen can be downloaded as a CSV file, which can be opened and accessed by Excel. Once the report is opened in Excel, data sorting, data filtering, and other Excel functionalities can be used to present the data in a way that will assist the investigation activities by the privacy officers.

4. Possible Incident Patterns

The following are recommended patterns to look for when reviewing the IAR audit log. For more details on establishing usage baselines and investigating incidents, refer to the investigation scenarios below.

4.1 Review Inactive Users

When reviewing the audit log, the privacy officer should pay attention to inactive users. If a user is inactive for an extended period of time, the privacy officer should investigate and determine if the user still has a legitimate reason to maintain an IAR user account.

Once a month, the privacy officer should list users that have not logged in to IAR for the last 30 days. For each inactive user account record on the list, the privacy officer should:

- Confirm with the user's manager or the Human Resources department that the user is still working in the organization.
- Confirm with the user's manager if the user is on vacation, or on any long term absence from his/her position; then consider disabling the user account temporarily, and only re-enable the user account upon the user's return.
- Confirm with the user's manager that the user still performs the functions that require IAR access; otherwise, the privacy officer should initiate the removal of the user account.

4.2 Review User Login Failures

Multiple sequential user login failures or user login authentication errors may indicate attempted unauthorized access (i.e., someone trying to login using someone else's credentials by guessing the passwords).

The privacy officer should use the event type and status filters to display user login failure events by entering date ranges, such as the last 7 days, 14 days, 30 days, etc.

When reviewing the failure login list, the privacy officer should look for unusually high volumes of unsuccessful login events on a single or on multiple user accounts. This may indicate an intruder is trying to gain access to the IAR system by using various user accounts and guessing the respective passwords.

During investigation the privacy officer should look for the physical IP address from which potential intrusion attempts originate, and work with the organization's physical security personnel to conduct further investigations (e.g., reviewing surveillance video footage of the physical location where the IP address is originated from, etc.).

4.3 Review for Unusual User Names

The privacy officer should review the audit log to look for any unusual usernames (usernames that are not of the same username convention). For example, if all usernames take the form "firstname.lastname" and user "mcc0004" logs in, this may indicate unauthorized access. The privacy officer should contact the HINP privacy officer to investigate the creation of this unusual user account name, as well as the authorization of such a request. The HINP manages new user account creation and keeps records of all user account request forms authorized by the organizations. Contacting the HINP will determine whether the unusual username is a legitimate user of the organization.

4.4 Review for Out-of-Ordinary User Access to IAR

Once a user behavior baseline is established in the organization, it is much easier for the privacy officer to spot unusual or out-of-norm user access to IAR. The privacy officer should look for the following user access activities:

- Login frequency – By displaying only the successful login and logout events, the privacy officer can determine how often the users are logging in to IAR. Filtering the display down to 24-hour segments may make this particular review more manageable depending on the size of the organization and the number of IAR users in the organization.
- When a particular user logs in to IAR significantly more frequently than usual, (e.g., 10 times a day versus once a day), further investigation may be warranted. The privacy officer may consult with the user's immediate manager to determine if there has been a possible shift of the user's job responsibility. Out-of-norm login frequency may also indicate unauthorized use.
- Login duration – From the display of successful user login and logout events, the privacy officer can also determine if login duration for a particular user that is out-of-norm (e.g., between 6 am to 11 pm versus 9 am to 5 pm, etc. The increase of login frequency should also trigger the privacy officer to review the login duration for the same user to determine if there is legitimate business explanation for the increased login frequency and extended login duration in IAR.
- Login interval – From the same successful user login and logout event display, the privacy officer can also determine the interval between login sessions from the users. Again this is used to compare against normal user behavior, if the baseline is established that users login to IAR from Monday to Friday as a norm, and seldom login over the weekend. Then for example, any login sessions over the weekend are worth further examination. Together with the reviews regarding login frequency and login duration, the privacy officer should investigate if the login interval between user access events is out-of-norm when compared to the login frequency and login duration mentioned previously.
- In all of the above mentioned situations regarding access activities, the event by itself may not be a cause for concern (e.g. a user is shown logging in IAR over the weekends for two consecutive weeks and his/her usual usage pattern is always Monday to Friday). While this would be a good starting point for the privacy officer to conduct some preliminary investigation, there are many legitimate business explanations to such behavior, such as a project deadline or new organizational

schedule. Therefore it is important to view these user activities variations with the broad understanding of business requirements and changes in the organization in mind.

4.5 Review for Unusually High Volume Client Search

Out-of-norm volumes of client searches from one single user warrant further investigation. The privacy officer should display daily or weekly user activities to determine if client search activities are of higher than normal volume. If the search events are higher than average, use filters to identify if these high search/view activities are from a single user. If that is the case, that particular user may be conducting client information surfing, or there is legitimate clinical reason for the high volume of searching of clients from that user.

The privacy officer may use local sources such as verbal interviews with the user's managers, the users themselves and possibly the user's peers to determine either the rationale for the increased in client search activities or if suspicious circumstances were observed.

4.6 Review for Unusually High Volume Assessment Search

Unusually high volumes of assessment searches from one single user on one or more clients warrant further investigation. The privacy officer should investigate and determine if the particular user has a legitimate reason for examining these client(s) in detail based on his/her job functions.

The privacy officer can use local sources such as verbal interviews with the user's managers, the users themselves and possibly the user's peers to determine rationale for the increased in client search activities or if suspicious circumstances were observed.

4.7 General Failure Events

As a general rule, the privacy officer should investigate any failure activities to determine if there is any logical explanation. For instance, a high surge in login failure activities across multiple users on a Monday morning after the March break holiday can be explained by the fact that the some users have forgotten their passwords due to the extended absence from normal IAR usage. A high volume of user login failure for a brand new user can also be attributed to the user's lack of familiarity with the IAR system. Failure events can be filtered by selecting the "Fail" button under Results.

4.8 Establishing a User Behavior Baseline (look for PS1 and…)

In addition to identifying possible incidents by matching the log with the pattern, privacy officers can establish a baseline of your user behaviors in order to conduct more comprehensive log reviews.

The privacy officer should review user activities from the IAR log on a regular basis and document the following:

- Number of search or view events
- Number of print events
- Time period of high user activity

- Time period of low user activity
- Number of user logins on week days
- Number of user logins on weekends
- Average duration of user login sessions
- Number of failed and successful event statuses

Calculating the averages from the data collected over a period of time will assist the privacy officer to establish baselines of user behaviors.

5. IAR Reports for Privacy Officers

There are two kinds of audit log reports in IAR: privacy and security reports and IAR operations.

5.1 Privacy and Security Reports

Report Names	Report Descriptions
PS1 - IAR User Activities Report	The report presents a list of logged audit events on a user-by-user basis for a specified time period
PS2 - IAR Event Type Report	This report provides summary details of all login events (successful and failed logins) for all users of the organization for a given date range
PS3 – IAR Consent Directives History Report	This report displays a list of both IAR-level and HSP-level consent directive changes for a client in a specified time period. This report shows all consent directives requested by this client and updated in the IAR system during the specified period of time
PS4 – IAR Current Consent Directive Report	This report displays a list of both IAR-level and HSP-level consent directives currently registered for a particular client. If the client has never requested or changed his/her IAR-level consent directive, the default IAR-level consent directive is “GRANTED” and is not presented in this report.
PS5 - IAR User PHI Access Report	This report presents a list of all the assessments accessed by a specific IAR user. Based on the selected User ID and date/time range, the report shows which patient/client and which assessments that user has reviewed or accessed. This report is focused on access related events (i.e. events where either the PHI and/or the assessments were viewed).
PS6 - IAR PHI Disclosure Report	This report, based on the selected client ID and date/time range, will present which user from which organization has accessed this selected client’s assessment .
PS7 - Assessment Disclosure Report	This report displays users from outside of the current organization who have accessed a person’s assessments belonging to (i.e., uploaded from) the current HSP.
PS8 – Inactive Users Accounts Report	This report displays user’s Last successful login, and the days of inactivity. The privacy officer should ensure that any user who has not logged in for more than 90 days has a valid reason or should be disabled in the system

5.2 Operational Reports

Report Names	Report Descriptions
OP1 – List of IAR Users	This report provides a list of all IAR users, primarily sorted by their organizational affiliations and secondarily by their roles
OP2A – List of IAR Locations	The OP2A report shows all of the IAR Locations, Location ID, and associated IP-Address
OP2B – List of IAR Organizations	The OP2B shows all of the IAR organizations, their Organization name, Organization ID, as well as when they joined this particular cluster

5.3 IAR Logs

Log Names	Log Descriptions
LOG1 – Current Activity Log	The Log contains information about all sessions currently active. The organizational privacy officer can view the current activity of all currently logged in users from their organization
LOG2 – Privacy Log	Contains Information relevant to access of PHI by any user.
LOG3 – Clinical Log	Clinical Log contains detail information about user activities, including login time, log off time, search performed, upload, change or open any assessments etc. Privacy officers of the organization can use the log to build a history of user activities
LOG4 – System Log	System log Contains Information about the system activities, and is usually used to check the start up and shutdown time of the system and to check if the database was exported or imported.

Appendix A — IAR Report Review and Investigation Scenarios

Scenario 1: Cleaning Up Inactive User Accounts

Trigger: Monthly, bi-monthly scheduled or user-requested report indicates that some user accounts have been inactive for 90 days.
Pre-condition: Local privacy officers can only see local user accounts.
Starting Report: OP8, where AVG login=0
Pattern: If AVG login=0 and last login date/time is >90 days, then investigate further.
Investigation:
Verify why user is inactive. Use OP8 to determine User details such as the user's name. The privacy officer can then check with the user's manager, HR or other personnel within the organization to determine if:

i. The user is on extended holiday or maternity leave
ii. The user has been transferred to another department or have left the organization
iii. The use has another reason for not using IAR

Depending on why user is inactive, determine if user account should be disabled. IAR queries or reports are not necessary for this step.
Post-Condition: Follow the IAR User Account Management process to disable accounts where appropriate.

Scenario 2: Developing a Usage Pattern

Trigger: Privacy officer wants to get a clearer picture of IAR user activities across the organization.
Pre-condition: Users must be local.
Starting Report: PS1
Pattern: Look for a pattern of user activities: most common events, average number of print events per week, etc. Use this pattern to establish a baseline and then run this report at pre-determined intervals to see if patterns change according to predictable behaviour, or if there is a deviation.
Post-Condition: *See scenario 4: Routine Log review for next steps after a baseline is established.*

Scenario 3: Routine Log Review

Trigger: As part of weekly, bi-weekly or monthly routinely scheduled log review, the local or HINP (global) privacy officer would call up PS1 to look at user activity and compare it with the established baseline usage pattern in an attempt to detect unauthorized or unusual activity as early as possible.
Pre-condition: Local privacy officer can only review usage patterns of users local to their organization. HINP (global) privacy officer can review usage patterns of all users across organizations.
Starting Report: PS1

Pattern: Viewing of an unusually large number of assessments or person records, unusually large number of search, view or print events as compared to average usage.

Investigation:

1. Determine if user has a valid business reason for this surge in activity. (Privacy officer would use local sources such as verbal interviews with the user's manager, the users themselves or possibly their peers to determine unusual events and if suspicious circumstances were observed.)
2. If there is a stated valid business reason to justify the change in usage pattern, verify if the frequency of events (e.g. views, prints, etc.) match anticipated clinical/business events such as "client/person was present for an appointment, client/person's case was under review for care planning, etc". Use report PS5 in correlation with clinical logs viewer.
3. If frequency seems appropriate, and no other suspicious activity was reported, document the investigation.
4. However, if there is no valid reason for this change in activity, the privacy officer should investigate further to get a clearer picture of the user's usage of IAR, including running:
    i. PS5 to determine which person records were accessed by this user and if the person had restricted consent directives
    ii. PS5 to get a clear picture of which assessments were accessed
5. If the user's activity extends to assessments from other organizations, the local privacy officer should document which assessments, which persons and which organizations are affected and provide this information to the HINP (global) privacy officer for further investigation.

Post-Condition: Document breach details using breach/incident investigation policy and templates, take corrective actions and notify affected clients/persons and other applicable parties as per policy.

Scenario 4: Failed logins

Trigger: As part of weekly, bi-weekly or monthly routinely scheduled log review, the local or HINP (global) privacy officer would call up PS2 where EventType=Login and EventStatus=Failed.

Pre-conditions:

- Local privacy officer can only see local users and events.
- User interface should allow this report to be run without requiring the privacy officer to enter any information besides a date and time range – i.e. There should be a "button" or clickable option called "Failed login reports" so the privacy officer doesn't have to choose "event type = login, status =failure".

Starting Report: PS2

Pattern: If there is a higher than average number of failed logins (e.g. more than 10 in 10 minutes, depending on the number of users/established usage patterns) then the privacy officer should investigate further.

Investigation:

1. The local privacy officer should contact the HINP (global) privacy officer to determine if there is a system-wide problem causing users to be unable to log in. If yes, document the reason for the failed logins and continue with other routine log review activities. (If the system-wide failure is a result of a security incident, the HINP Privacy officer will

manage the incident and provide a report to affected HSPs as per the IAR Integrated Incident Management Process.)

2. If there is no system-wide reason for login failures, the Local Privacy Officer should validate if the login failures are actual login attempts by the user, or if there are suspicious circumstances involved. (Manual investigation – contact the user directly and get a list of when the users recall using the IAR system and what activities were performed at this time.)
3. If the user(s) do not recall attempting to login and having difficulty logging in during the time range identified in the report, the Privacy Officer should use the IP Address located under "Event Location" in PS2 and work with the operational/IT team to identify if this IP address is onsite, or at a remote location.
4. Additionally, the Privacy Officer should note any other activities by the users with the unexpected failed logins within the same time range to determine if these user accounts have been compromised and what has been viewed/downloaded/printed by these compromised accounts. (use PS5 with the approximate date/time range of the failed logins). If PHI has been compromised, determine which clients were affected,
5. Regardless of location, the Privacy Officer should work with the IT or security team to kick off a security incident investigation to determine what is going on at that node. If the IP address is local, physical security measures (eg cameras and access card readers, etc) may provide additional information as to how to contain the incident.
6. Based on the persons affected and the results of the security investigation, the Privacy officer should follow the IAR Integrated Incident Management Process to resolve the incident.

Post-Condition: Document incident details using breach/incident investigation policy and templates, and take corrective actions and notify affected clients/persons and other applicable parties as per policy.

Scenario 5: VIP or Victim of Violence

Trigger: A newspaper article is published containing a significant amount of a hockey player's PHI and it becomes clear that the PHI may have been leaked by a user at Organization A where the hockey player received services.

Pre-condition: Local privacy officer can see any users from any organizations that have accessed assessments that their HSP uploaded for this person.

Starting Report: PS6

Pattern: List of users that have access the hockey player's assessment information

Investigation:

1. The privacy officer should use the list of users that accessed the hockey player's assessment information and compare it with the organization's list of which clinicians and case workers had valid business reasons to access the hockey player's assessments. If there are user names that do not appear in the valid list, the privacy officer should investigate further manually through interviews with the user's manager and colleagues and other means as per scenario 10 (the nosy neighbour) below.
2. If all users had a valid reason to access the client's assessment, the privacy officer should still investigate with managers and within the care team to determine if it is

possible that one of the clinicians used the assessment in an inappropriate manner. This is out of scope for the IAR processes.

3. If the users that accessed the hockey player's PHI did so from another organization, the local privacy officer should work with the HINP (global) privacy officer to coordinate the investigation of valid business reasons for access.

Post-Condition: The incident should be documented according to IAR Integrated Incident Management Process and corrective actions taken as appropriate.

Scenario 6: The Nosy Neighbour

Trigger: Client, user Y, third party, or global (HINP) privacy officer complains that User X is "surfing" persons or assessments, or "spying on" persons.
Pre-condition: If user is local, run report PS5. If user is not local, run report PS7 and then contact HINP privacy officer to continue investigation.
Starting Report: PS5, search by user X or PS7, search by date range when unauthorized disclosures are suspected.
Pattern: If user X has an unusually high number of persons viewed (according to your organization's established user patterns) and/or persons viewed have restricted consent directives, then investigate further.
Please note that when using PS7, you can use OP2 to identify the organizations listed in PS7. For complaints involving users from other organizations, contact the HINP privacy officer to continue your investigation.
Investigation using PS5:

1. Does User X have a valid business reason to view persons? (Privacy officer would use local sources such as: asking User X's manager, checking a roster of user roles to see if User X has a role that works with this type of person, or User X's client list, or potentially speaking with the person/client who raised the concern if applicable.)
2. If yes, there is a valid business reason: Verify if the frequency of access events (e.g. views, prints, etc.) match anticipated clinical/business events such as "client/person was present for an appointment, client/person's case was under review for care planning, etc".
   - Use report PS5 in correlation with other administrative logs

   If yes, the frequency of access correlates with valid clinical or business events, end the investigation and document the incident as cleared according to breach/incident investigation policy and templates.
3. If the answer to either 2 or 2.a is no:
   i. Identify which persons are affected.
   ii. Identify breach details:
      - Using PS5 identify if the actions performed on the persons and their assessments were "view person" or "view assessment" or "view assessment detail" or "print".
      - Depending on the event type, determine the likely nature of User X's activities: personal/curiosity (view type events) or possibly an external facing breach (print type events).
      - Use any other investigative means (interviews with User X's colleagues, affected client/persons, etc) to determine as many details as possible about User X's activities.

Post-condition: Document breach details using breach/incident investigation policy and templates, and take corrective actions and notify affected clients/persons and other applicable parties as per policy.