

Auditing Access for EMR Users

When accessing the EMR to view or access patient information, users must have a provider/service relationship with the client (circle of care) or require access as part of their assigned duties. Review or access of patient information outside of one's authorized duties is not permitted. Examples of unauthorized access include, but are not limited to:


- One's own personal health information;
- Information of any of the user's direct/indirect family members
- Information relating to user's neighbours, friends, co-workers, acquaintances or public figures;
- Information of any other individual where the user is not included in the "circle of care" or does not require access for other assigned duties.

Audit Responsibilities

- The EMR auditing function is valuable for supporting the custodian's responsibility to restrict access to personal health information. This is helpful when making a patient's EMR record of activity available to them and when investigating a breach.
- Auditing of EMR access should be performed by an individual who can validate whether access is appropriate based on assigned duties and/or circle of care.








Audit Log Access

The audit log captures all EMR activity. Reports can be generated based on user activity, patient information, or a combination of both criteria. Site level access is required to access the audit log.

The audit log is available under **Profile**  -> **Audit Log**:

med access		Audit Log Viewer		Look Back:	Event Type:	User:	Internal ID:	Reports:	Refresh
		None	ALL				0	Frequent Failed Login	
TimeStamp	Event Type	Data	Patient	User	Source	Tx ID			
10:56:03	Access audit log		n/a	ksmith		9994			
10:56:01	Access audit log		n/a	ksmith		9993			
10:55:53	Login		n/a	ksmith		9992			
10:55:45	Logout		n/a	dattenborough		9991			
10:55:31	Chart updated	INSERTED Lab	Jonathan Test	dattenborough		9989			
10:55:09	Chart accessed		Jonathan Test	dattenborough		9988			
10:54:41	Login		n/a	dattenborough		9987			
10:54:31	Login failure	principal=clocke	n/a	clocke		9986			
10:54:22	Login failure	principal=clocke	n/a	clocke		9985			
10:54:17	Logout		n/a	ksmith		9984			
10:54:14	Patient created/updated	Demographics updated	Miriam Test	ksmith		9983			

Icons

Filters	Purpose
Look Back  None 	Determines how many days to look back when retrieving data. Click the calendar icon to input a date range instead.
Event Type: ALL 	Determines what event type you wish to see. For more details, see the chart below.
User: 	Determines which user to retrieve information about.
Internal ID: 0 	Determines which patient's chart to use. Click to search for a patient.
Reports: Frequent Failed Login  	Select a security report type and then click on the printer icon to print that report.
Refresh	Refreshes the Audit Log and displays results based on other filter's criteria.

Reports

The following EMR reports reflect current audit industry standards and requirements identified by legislation and PHIA and should be included as part of regular audits:

REPORTS	DESCRIPTION
Frequently Accessed Record Audit	Returns a list of patients that have been accessed most often.
Same User Same Patient Last Name Search Audit	Provides a list of who is unmasking what and why.
User Activity Audit	Returns all activity for users of the EMR.
User Name Search Audit	A report of all searches for charts with the same name as a user of the EMR.
User Activity Audit (off hours)	Returns all user activity during off hours.

Reports can also be customized using the following criteria/filters under **Event Types**:

EVENT TYPE	DESCRIPTION
All	All event types.
Access Audit Log	Each time a query is run on the audit log.
Chart Assessed	Select a user to view all of the charts they accessed.
Chart Updated	Select a user or patient to see the chart updates.
Attachment Detached	See when and from where attachments were detached.
Group Favorite Enabled	See when and who enabled a favorite for the group.
Confidential Data Disclosed	Choosing to run a report on confidential charts.
Email Sent	Shows email sent.
Group Favorite Disabled	See when and who disabled a favorite for the group.
Record Exported	Apply a service in the reporting window or run an export service in reports.
eReferral Received	If clinic is on the Referral Network a list of all referrals received.
eReferral Sent	If clinic is on the Referral Network a list of all referrals sent.

Lab/DI Manual Download Request	Shows requests for annual download of labs.
Record Imported	(showing import agent) Chart imports, patient merges, care plan imports.
Login	The list of users that have logged into the EMR.
Logout	The list of users that have logged out of the EMR.
Mask Applied	A list of tasks marked confidential (masked).
Mask Overridden	A list of confidential tasks / charts accessed.
Patient Merge Completed	List of all merged patients.
Referral Patient Merge Completed	List of all Referral patients merged (referral network only).
Patient Search	List of patient searches.
Patient Merge Started	List of all merges started.
Password Changed	List of who and when a password change was made.
Password Change Failure	List of who and when a password change was attempted but failed.
Patient Created/Updated	List of all patients created or updated.
Print	List of printing actions (print preview).
Provider Modified	Changes made to the provider list.
Session Timed Out	List of all sessions that timed out.
User Modified	List of all changes to users.
User Group Modified	List of all changes to the user groups.

Auditing Frequency

Regular audits should be conducted to search for potential unauthorized access and to adhere to privacy and security standards. Reports can be run for a defined period: daily, weekly, bi-weekly or monthly intervals.

Audit Cues and Pattern Uses To Guide In Determining Appropriate Access

- Audit cues are events that stand out on an audit that are possible signals that inappropriate access has taken place.
- Each user accesses the system in different ways. How people perform their duties even in the same position can be very different. Everyone has their own way of accessing the system that makes up a visible Pattern of Use.
- Audit cues may deviate or contain practices not consistent with that user's regular pattern of use.

Examples that may present an **Audit Cue** include:

Same Name	Time of Access
Repeated Lookups	Patient Age
Staff Location	Frequency Lookups
Duration of Lookup	

To ensure that cues are not misinterpreted it is recommended to cross reference other sources of information. Consultation with the user's Manager/Director may also be required. The goal is to find information to validate the access.

- Access may have changed.
- Position may have changed.
- Employee may be working in one or more areas.
- Special circumstances may exist for the access for the employee or the client accessed.