

# EMR Auditing

## The Audit Log Functionality

The auditing function in the EMR is valuable for supporting the custodian's responsibility to restrict access to personal health information to those who need to know, making available to patients a record of activity associated with their electronic record, and when investigating a breach. The custodian is responsible for the proper management and use of the auditing information. These responsibilities include, but are not limited to:

- Ensuring at least one person within the clinic is trained on how to use the auditing function;
- Restricting access to the audit logs and reports to those who need to know;
- Ensuring employees, other health professionals, and medical students and residents are aware that all actions within the EMR are audited;
- Determining what information will be collected in the audit log;
- Developing a standard report for audit logs, one by user and another by patient and an understanding of how to run ad hoc reports;
- Establishing a regular schedule for reviewing audit logs.

Further guidance on auditing and other privacy considerations can be found at:

<https://edocsnl.ca/privacy-and-security/>

## The Audit Log

Every change that users make a Med Access EMR is recorded in the audit log. The log records everything that is done in a patient's chart, such as viewing a patient, entering notes, editing or deleting any information, and sending messages.

The log also records some non-clinical changes, such as password changes, who accessed the audit log, and who printed information. It includes which user did the work, when, and from which computer (IP address).

You can view a user's activity, a patient's activity, all activity of a certain type, or a combination of all those criteria. You can also view and print pre-configured security reports that enable you to view information about your users. Use these reports to perform random audits of the users on the system, and to check for suspicious activity.

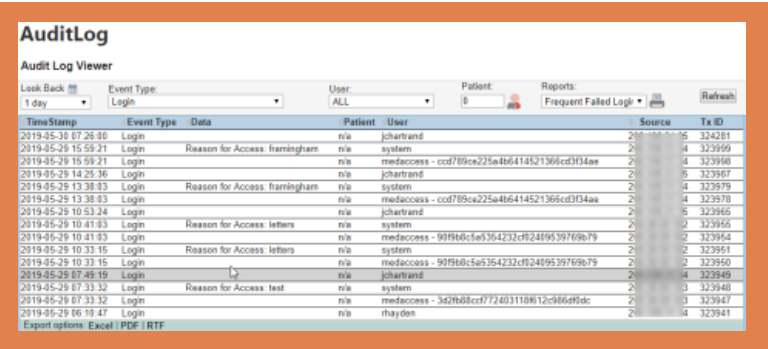
Only users with Site level access can use the audit log.

# EMR Auditing

## The Audit Log Functionality

### Viewing the Audit Log: Steps

1. From the main EMR window, click **Profile** in the upper right corner of your dashboard.
2. Under **Site Administration** on the left side of the screen, click **Audit Log**. The log for logins in the last day appears by default.
3. From the **Look Back** list, select for how many days to retrieve data.
4. From the **Event Type** list, select what event type to see. For more information, see the attached document "EMR Auditing."
5. From the **User List**, choose for which user to audit activity, if required for the selected report type.
6. In the **Patient** field, type the patient chart number or click to search for a patient, if required for your selected report type.
7. From the **Reports** list, choose a type of security report to run. For more information, click here to review the "EMR Auditing" file.
8. Click **Refresh** to return new results based on your filter criteria.
9. To generate a spreadsheet report, click **Print**.



**AuditLog**  
Audit Log Viewer

Look Back: 1 day | Event Type: Login | User: ALL | Patient: 0 | Reports: Frequent Failed Login | Refresh

TimeStamp	Event Type	Data	Patient	User	Source	Tx ID
2019-05-30 07:26:30	Login		n/a	jchartrand	2019-05-30 07:26:30	3234281
2019-05-29 15:59:21	Login	Reason for Access: framingham	n/a	system	2019-05-29 15:59:21	3239999
2019-05-29 15:59:21	Login		n/a	medaccess - ccd769ce225e4b6414521366cd3f34ae	2019-05-29 15:59:21	3239990
2019-05-29 14:25:36	Login		n/a	jchartrand	2019-05-29 14:25:36	3239987
2019-05-29 13:38:53	Login		n/a	system	2019-05-29 13:38:53	3239979
2019-05-29 13:38:53	Login	Reason for Access: framingham	n/a	medaccess - ccd769ce225e4b6414521366cd3f34ae	2019-05-29 13:38:53	3239978
2019-05-29 10:53:24	Login		n/a	jchartrand	2019-05-29 10:53:24	3239965
2019-05-29 10:41:53	Login	Reason for Access: letters	n/a	system	2019-05-29 10:41:53	3239965
2019-05-29 10:41:53	Login		n/a	medaccess - 90f8b6c5a5354232c0f2409539769b79	2019-05-29 10:41:53	3239954
2019-05-29 10:33:15	Login	Reason for Access: letters	n/a	system	2019-05-29 10:33:15	3239961
2019-05-29 10:33:15	Login		n/a	medaccess - 90f8b6c5a5354232c0f2409539769b79	2019-05-29 10:33:15	3239960
2019-05-29 07:49:19	Login		n/a	jchartrand	2019-05-29 07:49:19	3239949
2019-05-29 07:33:32	Login	Reason for Access: test	n/a	system	2019-05-29 07:33:32	3239948
2019-05-29 07:33:32	Login		n/a	medaccess - 342f6b8ccf772403110612c0b6d9dc	2019-05-29 07:33:32	3239947
2019-05-29 06:19:47	Login		n/a	rhayden	2019-05-29 06:19:47	3239941

Export options: Excel PDF RTF

### Example 1: Auditing all Activity by a Given User

1. Select the date range for which you wish to report on the user activity.
2. Select **All** as the **Event Type**.
3. Select the required **User** (this is the user activity is being audited).
4. Do not specify a **Patient**.
5. Click **User Activity Audit** under **Report Type**.
6. Click **Refresh**.
7. The report generated will show all activity for the selected user over the selected date range.



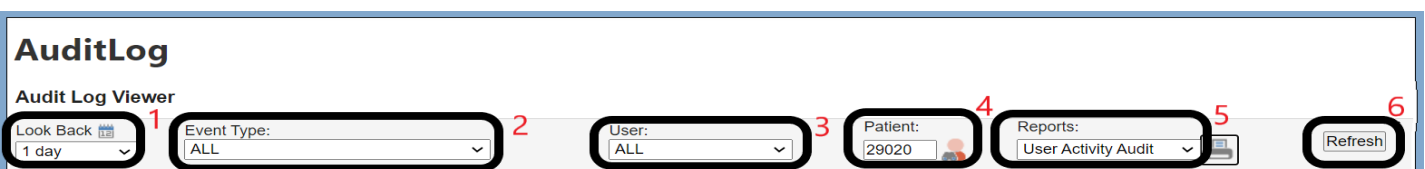
**AuditLog**  
Audit Log Viewer

Look Back: 1 day | Event Type: ALL | User: TEST - Training | Patient: 0 | Reports: User Activity Audit | Refresh

Nothing found to display

### Example 2: Auditing all Activity on a Patient's Chart

1. Select the date range for which you wish to report on the user activity.
2. Select **All** as the **Event Type**.
3. Select the required **User** (this is the user whose activity is being audited).
4. Specify a **Patient** (process outlined above) (this is the patient record on whose chart you are auditing all activity).
5. Select **User Activity Audit** under **Report Type**.
6. Click **Refresh**.
7. The report generated will show all activity for the selected user over the selected date range.



**AuditLog**  
Audit Log Viewer

Look Back: 1 day | Event Type: ALL | User: ALL | Patient: 29020 | Reports: User Activity Audit | Refresh