

HIPAA Regulations

Clinical Fusion™ has been programmed to meet HIPAA regulations for a clinical database management program that is not considered an electronic medical record. Clinical Fusion™ is not designed to be used as a health center's only way of recording patient registration and medical information. We suggest that health centers keep a paper chart of the patient's information in addition to the data contained in Clinical Fusion™.

The modifications made in Clinical Fusion™ to meet HIPAA regulations are based on a non-electronic medical record and are outlined below:

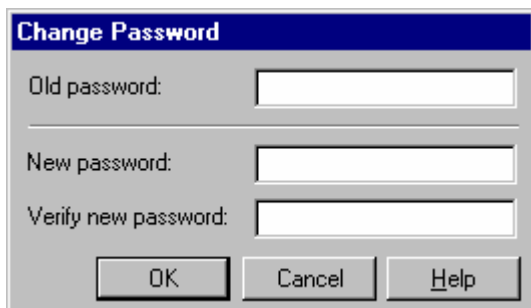
Password Security

The requirements for passwords used in Clinical Fusion™ have been adapted to create a more secure password, thus making the database itself more secure. The clinic administrator is responsible for assigning appropriate access rights to groups of users for the different activities within Clinical Fusion™. The administrator must also assign individual usernames and temporary passwords to each staff member who will have access to the Clinical Fusion™ database. See the topic on "Setting up Security for Users" for detailed instructions on assigning access rights and adding usernames and passwords to the Clinical Fusion™ database.

Once the usernames have been entered, each staff member is responsible for logging into Clinical Fusion™ using their individual username and password and for keeping the password confidential. Clinical Fusion™ will keep an audit of specific data entered by individual users. Each user will need to change the temporary password assigned by the administrator to a password he/she assigns.

To change your password:

1. Log into Clinical Fusion™.
2. Cancel out of the **Search** screen.
3. Click on the **Tools** menu.
4. Click on **Change Password**.
5. Type in your **Old Password**.
6. Next, type in your **New Password**.
7. Last, verify your **New Password**.
8. Click on **OK** to accept the new password. Be sure to tell no other user your password.



The image shows a standard Windows-style dialog box titled "Change Password". It contains three text input fields stacked vertically, labeled "Old password:", "New password:", and "Verify new password:". Below the input fields are three buttons: "OK", "Cancel", and "Help".

The criteria below must be followed when creating a password for Clinical Fusion™. You will receive an error if the password does not follow the criteria outlined for secure passwords.

- Be at least 8 characters in length

- Contain 3 of the following four character types: alpha lowercase (a, b, c, etc.); alpha uppercase (A, B, C, etc.); number (1, 2, 3, etc.); and symbols (!, @, #, \$, etc.)
- Clinical Fusion™ will force you to change your password every 90 days
- Cannot be the same as the password previously used

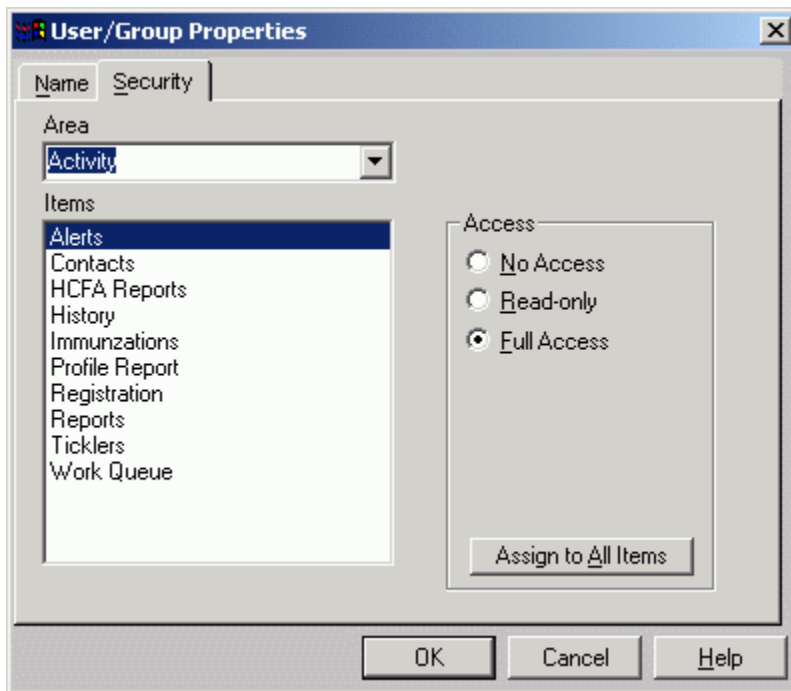
Other suggestions for creating secure passwords:

- Non-dictionary word
- Work passwords are different from home passwords
- Easy for you to remember, hard for anyone else

Report Security

Enhancements have been made to Clinical Fusion™ so that the report writing capabilities are connected to access rights given within the 'Users and Groups' setup screen in the Administration program. For example, if a user is given full access to the registration activity but no access to the contact activity, Report Manager will only allow that user to run reports that contain only registration information. The user will not be able to run any reports containing student contact information.

This feature works for each of the activities and modules on the Security tab of the 'Users and Groups' screen. Below is a screen shot of activities whose corresponding reports are connected to the access rights assigned by the administrator. The Group Activities module works in the same way.



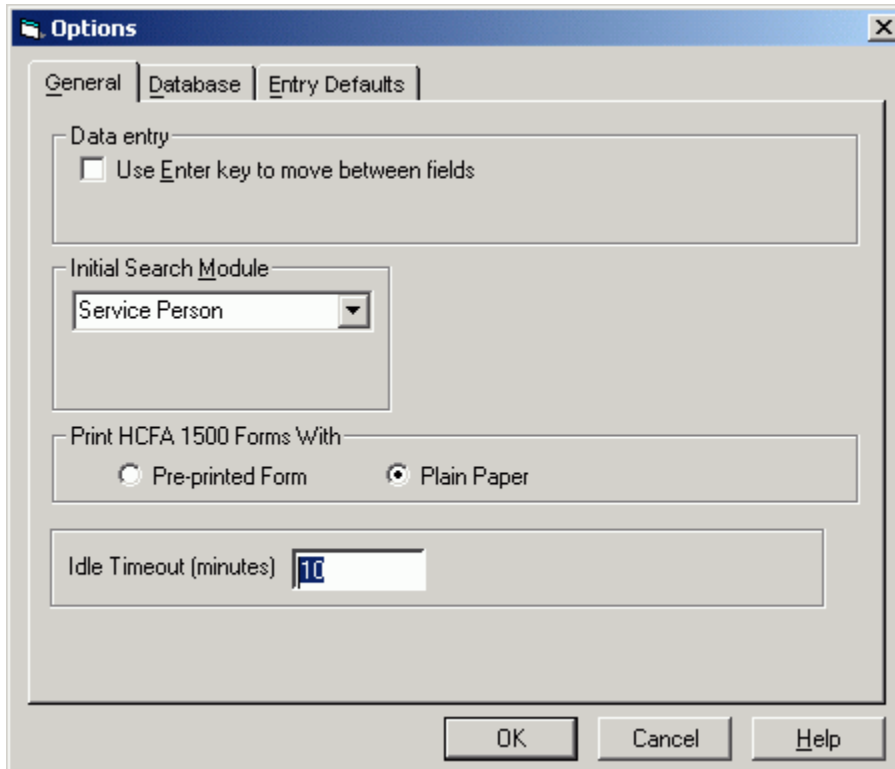
Timeout Feature

An automatic logoff feature has been added to Clinical Fusion™. If a user has stepped away from his/her desk or has stopped using the mouse or keyboard, Clinical Fusion™ will

automatically sit idle after a specified number of minutes set by the administrator. The user must re-enter their username and password to gain access back into Clinical Fusion™.

To set the Idle Timeout feature:

1. Log into Clinical Fusion™.
2. Cancel out of the **Search** screen.
3. Click on the **Tools** menu.
4. Click on **Options**.
5. In the General tab: enter the time in minutes for the **Idle Timeout (minutes)** field.
6. Click on **OK** to save the changes.



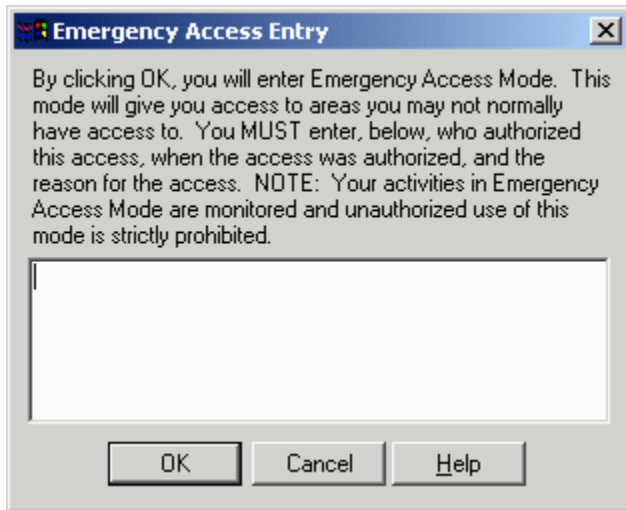
The image shows a screenshot of the 'Options' dialog box in Clinical Fusion™. The dialog has three tabs: 'General', 'Database', and 'Entry Defaults'. The 'General' tab is selected. It contains several sections: 'Data entry' with a checkbox for 'Use Enter key to move between fields' (unchecked); 'Initial Search Module' with a dropdown menu set to 'Service Person'; 'Print HCFA 1500 Forms With' with radio buttons for 'Pre-printed Form' (unchecked) and 'Plain Paper' (checked); and 'Idle Timeout (minutes)' with a text input field containing '10'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Emergency Access

Emergency Access mode provides a user with access to areas of Clinical Fusion™ that they may not normally have access to. You **MUST** enter who authorized the emergency access, when the access was authorized, and the reason for access. **NOTE:** Your activities in Emergency Access mode are monitored and unauthorized use of this mode is strictly prohibited.

To gain Emergency Access:

1. Log into Clinical Fusion™.
2. Cancel out of the **Search** screen.
3. Click on the **Tools** menu.
4. Click on **Emergency Access**.
5. Type in who authorized the emergency access, when the access was authorized, and the reason for access.
6. Click on the **OK** button.



You will be in Emergency Access mode until you exit out of Emergency Access mode.

To exit out of Emergency Access mode:

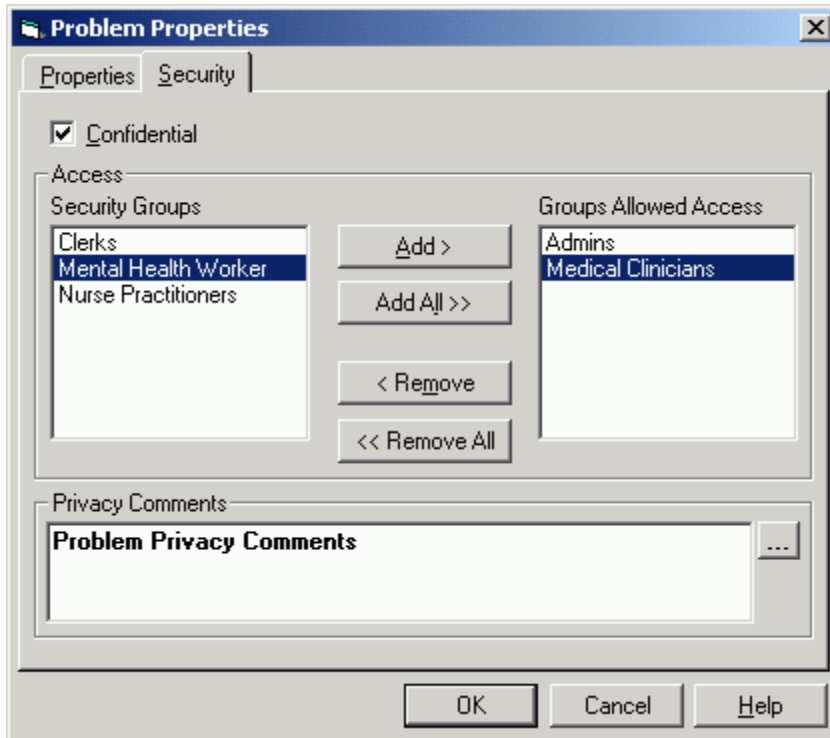
1. Click on the **Tools** menu.
2. Click on **Exit Emergency Access**.

Privacy Comments

You have the ability to enter privacy comments about a problem or a contact for a patient within Clinical Fusion™. These comments can only be reported on by a user who has access to the Problem and Contact information.

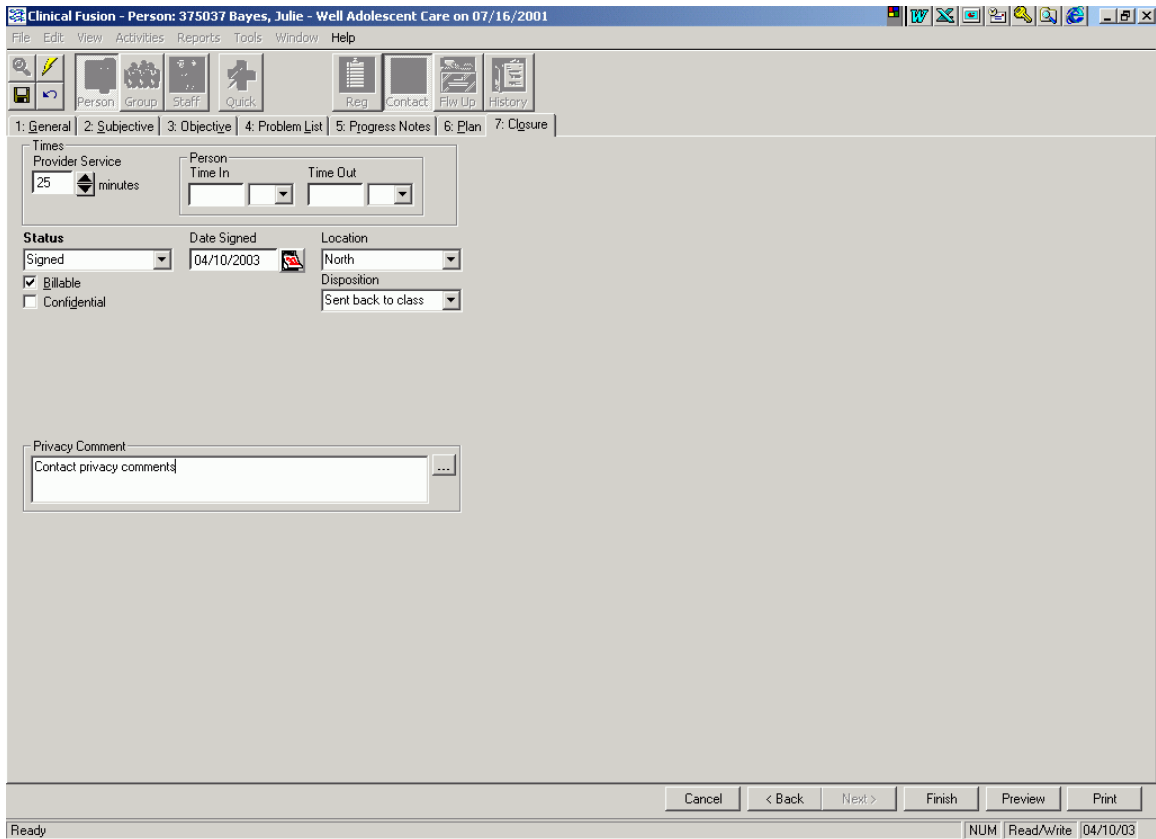
To enter Privacy Comments for a problem:

1. Log into Clinical Fusion™.
2. Search for the person you want to enter a privacy comment for.
3. Click on **Open Existing**, then click on **History**.
4. Click on the **Problems** tab.
5. Highlight an existing problem or add a new problem and click on the **Properties** button.
6. Click on the **Security** tab.
7. Type in the privacy comments needed.
8. Click **OK** to save the changes.



To enter Privacy Comments for a contact:

1. Log into Clinical Fusion™.
2. Search for the person you want to enter a contact for.
3. Click on **Create New**, then **Contact**.
4. Enter all of the contact information needed.
5. On the **Closure** tab at the bottom of the screen you can type in any privacy comments needed.
6. Click on **Finish** to save the contact.



Audit Database

HIPAA requires that all data entered into a database management program must be recorded so that the information can be easily audited if necessary. Clinical Fusion™ keeps track of this audit information in a separate database called 'Accesslog.mdb'. Placing the audit data in a separate file helps to maintain a higher speed of data entry in the actual Clinical Fusion™ database file. The 'Accesslog.mdb' file is located in the same folder that the Clinical Fusion™ database is found. **Be sure not to delete the 'Accesslog.mdb' file. If you are audited you will need the information contained in the file.**

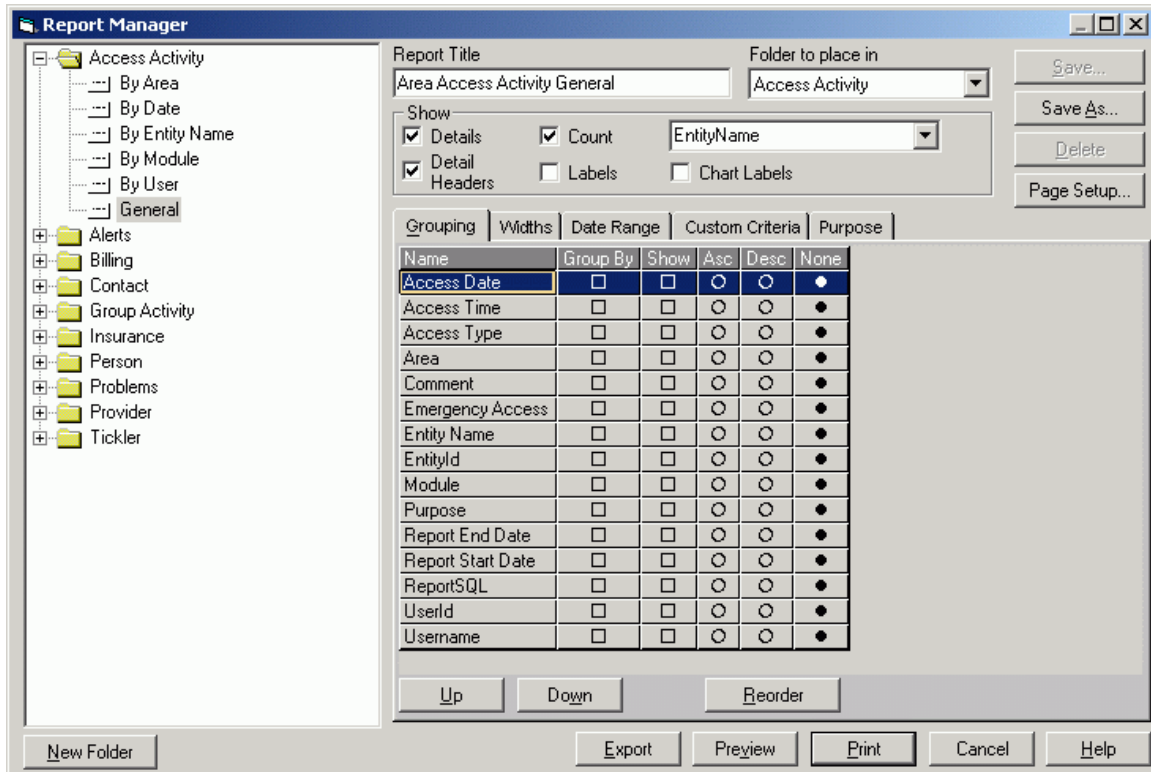
The following audit information can be reported on the 'Accesslog.mdb' file from within Report Manager:

Field Name	Definition
Access Date	The system date that the data was viewed, modified (entered), printed, or exported.
Access Time	The system time that the data was viewed, modified (entered), printed, or exported.
Access Type	The method used to work with the Clinical Fusion™ data. The options are viewed, modified, printed, or exported.
Area	The area of Clinical Fusion™ that a user has gained access to. This could be specific tabs within registration, contacts, history, or ticklers. It can also be report titles of reports that a user has previewed, printed or

	exported.
Comment	A memo field allowing the user to explain the purpose of a report run within Report Manager and who the report is for.
Emergency Access	True/False value stating if a user was under 'Emergency Access' mode while working with the specified data. 'True' signifies emergency access, and 'False' signifies regular access.
Entity Name	The person or provider whose data is being viewed, modified, printed, or exported. A value of <Empty> signifies group activities or reports since no one specific entity is accessed.
EntityId	A unique ID number generated automatically by Clinical Fusion™ for the entity name.
Module	The modules include 'Person', 'Staff', 'Group', or 'Reports'.
Purpose	The purpose of the report being generated. This is controlled by a drop-down list box and is entered on the Purpose tab in Report Manager. You can modify this list in Administration within the 'Report Purpose' element table.
Report End Date	The end date specified in the Date Range tab for any report generated in Report Manager.
Report Start Date	The start date specified in the Date Range tab for any report generated in Report Manager.
ReportSQL	The SQL statement generated by Microsoft Access identifying the exact information generated on a report in Report Manager.
UserId	A unique ID number generated automatically by Clinical Fusion™ for the username.
Username	The user who has viewed, modified, printed, or exported data from within Clinical Fusion™.

To run reports on the Clinical Fusion™ Audit database:

1. Log into Clinical Fusion™.
2. Cancel out of the **Search** screen.
3. Click on **Reports**, then **Report Manager**.
4. Click on the '+' next to the **Access Activity** folder.
5. You can choose any one of the standard reports. The **Access Activity** reports function in a similar method to all other **Report Manager** reports. You have complete control over what fields you want to report on the **Grouping** tab.



6. You can then adjust the widths of the columns on the **Widths** tab.
7. You can enter the 'Access Date' date range on the **Date Range** tab. This is not the actual contact date or registration date. It is the date the data was accessed or entered.
8. You can enter any specific criteria on the **Custom Criteria** tab.
9. The **Purpose** tab enables you to state your reasons for running the report. This tab is found on all of the Report Manager reports.

