Patient Level Data
User Accounts and Security

Requirements

When accessing the *System for Integrated Electronic Reporting and Auditing (*SIERA), each facility is required to have ***a minimum*** of one user whom the facility administrator has approved to act as their User Account Administrator (UAA). Designating multiple UAAs is encouraged.

The UAA is responsible for maintaining current user information for all other users at a facility. For instance:

- Creating user account
- Assigning facility contacts (Primary and Secondary)
- Confirming all user account information is current and accurate
- Confirming the Facility Administrator is current and accurate
- Disassociating users when they are no longer need access or have left the facility

Only the Patient Data Section can grant a user UAA privileges. Whoever will be performing the UAA role must complete and submit a User Account Administrator Agreement form. Please allow 2 business days for processing the request.

For additional information on account requirements, review the UAA Quick Guides series on our Training page.

The following security guidelines follow industry best practices and should be followed when using SIERA to ensure data security and integrity.

Each user must have a SIERA account in order to log into the system. Your password should always be kept private. NEVER SHARE YOUR ACCOUNT INFORMATION.

All actions within the system are logged and tracked for by means of your user account. The person associated with an account is responsible for all actions attributed to that account.

People who will need access to SIERA Patient Level Data will include:

- Individuals who will submit or enter data on behalf of the facility
- Individuals who will perform on-line corrections
- Individuals who need to see status of data submissions on a regular basis

If an employee temporarily needs access to SIERA, the UAA should create a new user account, then disassociate the account when the employee no longer need access. For the security of your confidential data, accounts and passwords should never be shared.

If you need additional assistance, please contact the Patient Data Section at (916)327-1262.