

# Complete Consent - Rapid Release User Management Job Aid

This document provides guidance on how to perform key User Management tasks as it relates to Complete Consent Rapid Release for Enabled Partners.

This Job Aid will guide you through:

- What it means to be an Enabled Partner using Complete Consent - Rapid Release
- Learning about the user roles of Complete Consent
- The workflow of user management and site creation for Complete Consent

Contents

[What is Complete Consent - Rapid Release?](#).....3

[What does it mean to be an Enabled Partner using CC-RR?](#).....3

[Summary of all roles](#).....5

[Summary of Study Configuration roles](#).....5

[Summary of Data Management roles](#).....11

[Who can see what? \(Data visibility\)](#).....14

[Understanding the relationship between roles created in Study Constructor & Consent Director](#).....15

[Common workflows for creating specific roles: instructions and videos](#).....17

[Personas](#).....21

[Best practices](#).....25



## What is Complete Consent Rapid Release?

Complete Consent is Clintech's consent management solution for better participant access and experience.

Complete Consent - Rapid Release is a version of Complete Consent where study build activities can be completed by an enabled partner.

## What does it mean to be an Enabled Partner using Complete Consent - Rapid Release?

As an enabled partner of Complete Consent Rapid Release, you will learn how to configure studies, manage users, and build electronic Informed Consent Forms (electronic consents), using Clintech's Consent Advisor tool. Let's begin with roles.

The roles that can be assigned to users in Study Constructor fall into three categories:

**Account role category:** Affects access to the entire org / study and, in some cases, to multiple Clintech applications (for instance, Complete Consent uses the Consent Advisor, Study Constructor, Participant Study Application, and Study Administrator Apps). Also referred to as **Study-Level** or **Gyrus-level** roles. Divided into the Study Configuration and Data Management sub-categories.

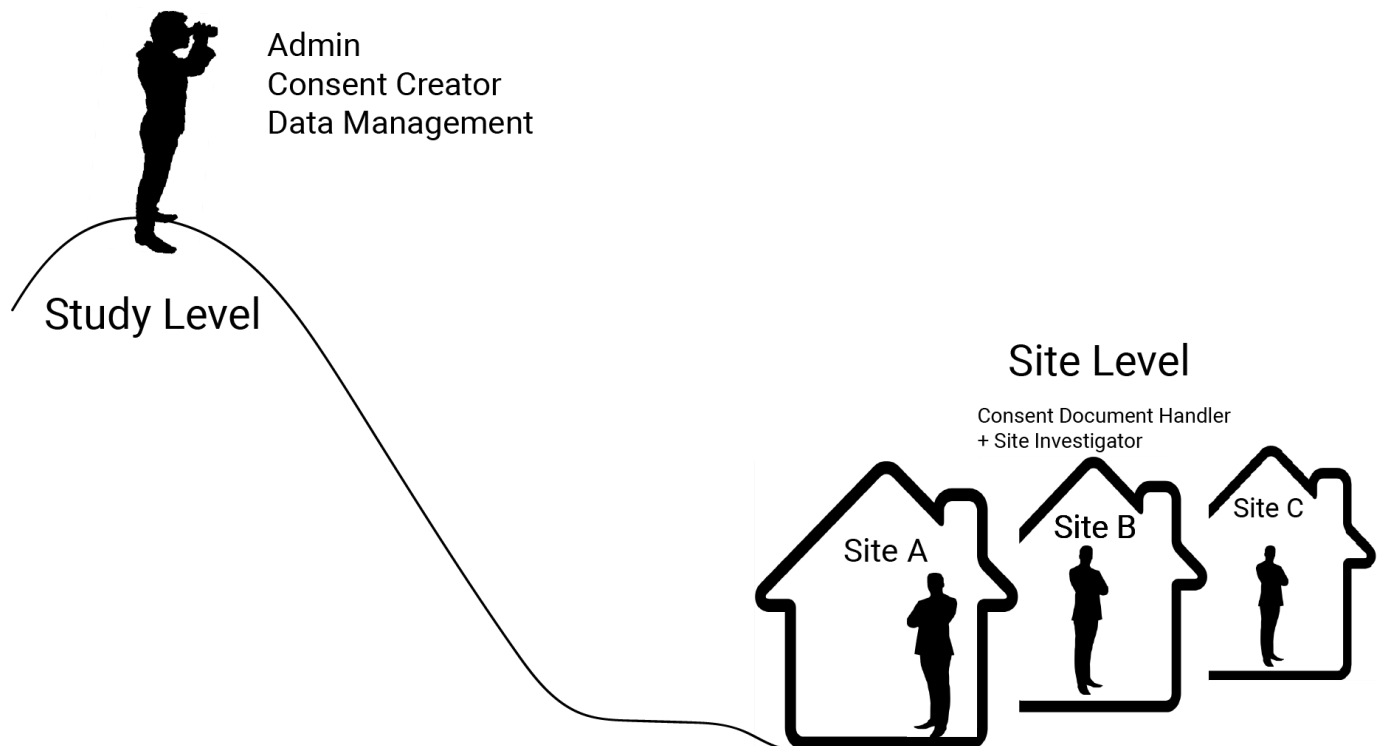
**Site role category:** Allows user to log in to Site User Express/ Site User Web applications and see / capture / edit data for participants associated with a specific Site. Referred to as **Site Level** or **Neuron - level**.

**Application / functional access role category** – Allows users to login to a specific application or access a particular function. For Electronic Consent Experts, this will apply mainly to the Study Administrator App role.

One way to think about it is with a visual metaphor:

A role with a **Study-Level** view is like a person standing on a mountain, looking over a group of houses. Each house is like a site and all the houses together make up the study.

- **Study-Level** Users inside each house can only see what's going on inside their house (Site), including the personally identifiable information (PII) for participants assigned to that house (site). They cannot see inside the other houses (sites).
- If a person has a **Study-Level** role, they have a view of all the houses (sites) from the mountain top, but they are unable to see inside them, so no PII is visible to them.



## Summary of all roles

Enabled partner users will assume at least one of these **Study - Level** roles:

- Administrator
- Consent Creator
- Consent Document Manager

**Application / functional access** roles include the Data Management roles:

- Data Evaluator
- Data Processor
- Lead Data Processor

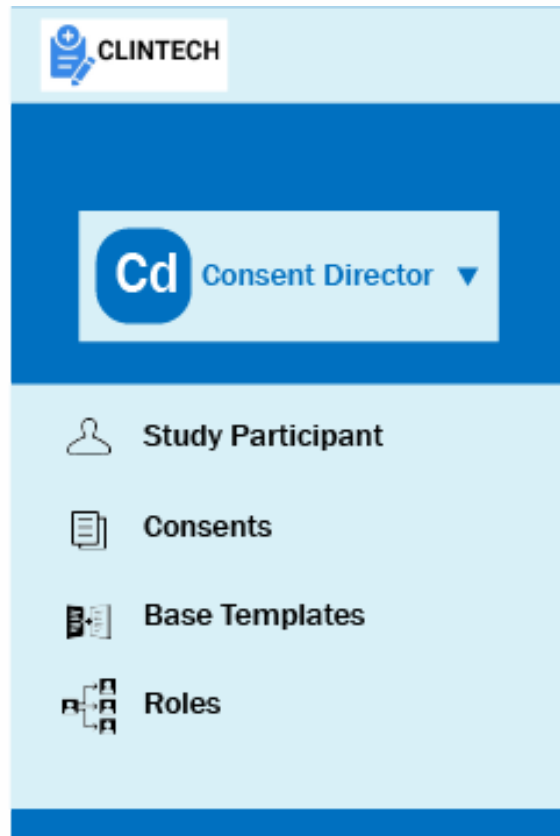
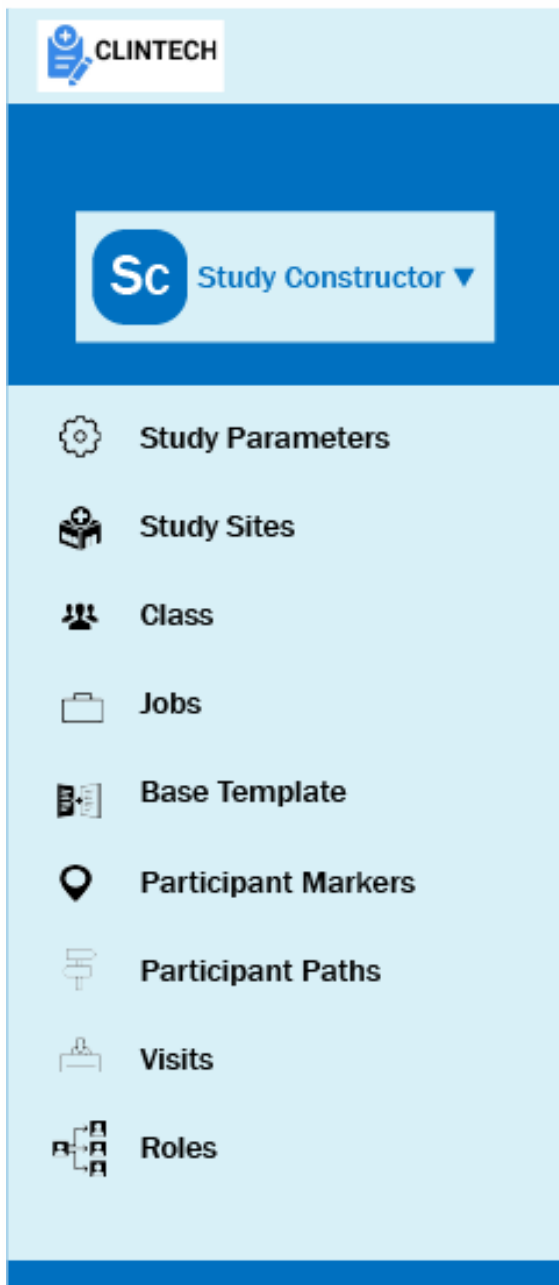
## Summary of Study Configuration roles

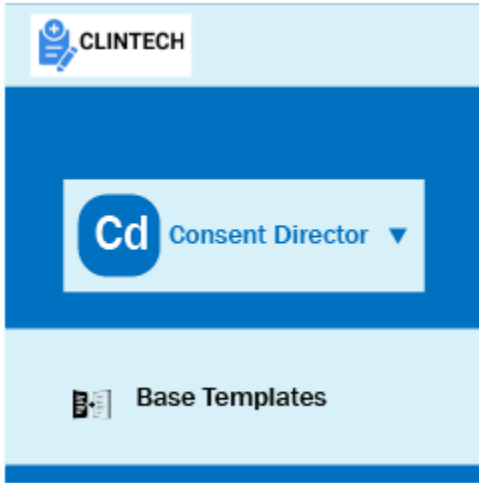
### Administrator

An Administrator can essentially do anything. They have permissions to manage users and assign them to sites, create documents and templates, view all documents, etc. This includes any of the permissions for other roles. This role is a **Study-Level** role and can access all the applications used in Complete Consent: Study Constructor, Consent Director, and Study Director.

It is important to mention that care should be taken when assigning this role. Even users who do not intend to do so can inadvertently change key study settings, modify the permissions of other users, change captured data in Site Director, or launch invalid queries in Study Director if given this "overpowered" role.

Appearance of Study Builder & Consent Manager menus to an Administrator:

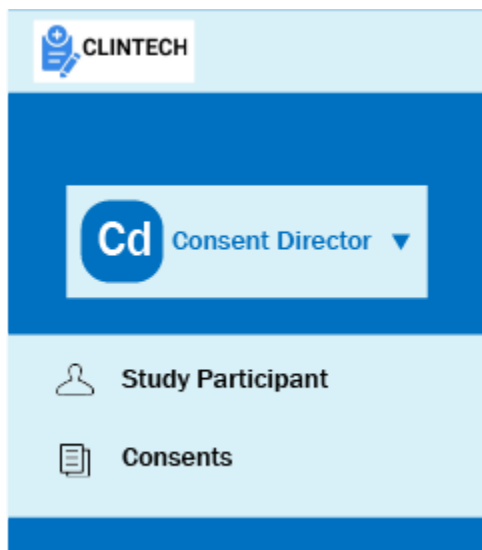




### Consent Creator

A Consent Creator controls consent base templates. They can create signature document templates and assign or publish those templates so that the site Consent Document Handler can create Signature documents for participants. They have the ability to change sites and access the Base Templates screen, but cannot access the Study Participants, Consents or Roles screens within Consent Creator. This role is also a **Study-Level** role but will likely not utilize Study Constructor or Study Director.

Appearance of Consent Constructor to an Consent Creator at left. Notice how there is no Study Participant tab, indicating that this role **cannot** see PII.

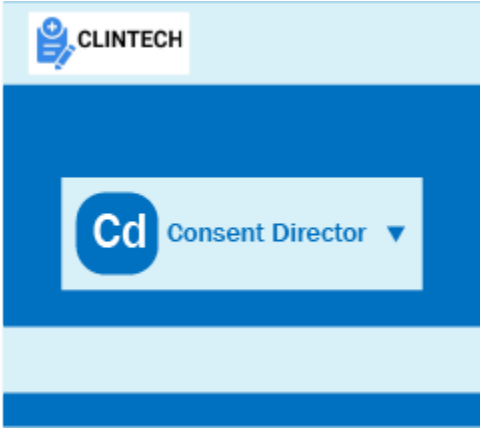


### Consent Document Handler

This role, always used in combination with the Site Director role, can access the Documents and Participants screens, but cannot access the Study Participant or Documents screens. A Consent Document Handler can use published templates to create signature documents and send them to participants. This role is **a Study-Level** role and can only access the Consent Director application. In other words, they are assigned to a specific site within a study and can only work with data for participants associated with that site.

Appearance of Consent Director to a Site Director with an Consent Document Handler role (Consent Document Handler + Site Director). Notice how there is a Study Participant tab, indicating that this role **can** see PII.





Site Director

While this role is often combined with other roles, Site Director can stand on its own as a role. The purpose of this role is as a signer that has been added to specific documents by the Consent Document Handler, and they only have access to those documents. This means that they are able to see some PII of the participants within these documents. This role is a **Site-Level** role and can only access the Consent Director Application. Again, they only have access to those documents to which they have

been assigned.





Below, you will find a table that outlines the specific permissions of each of the above Study Creation roles.

## Consent Roles and Permissions

### Study Configuration Roles

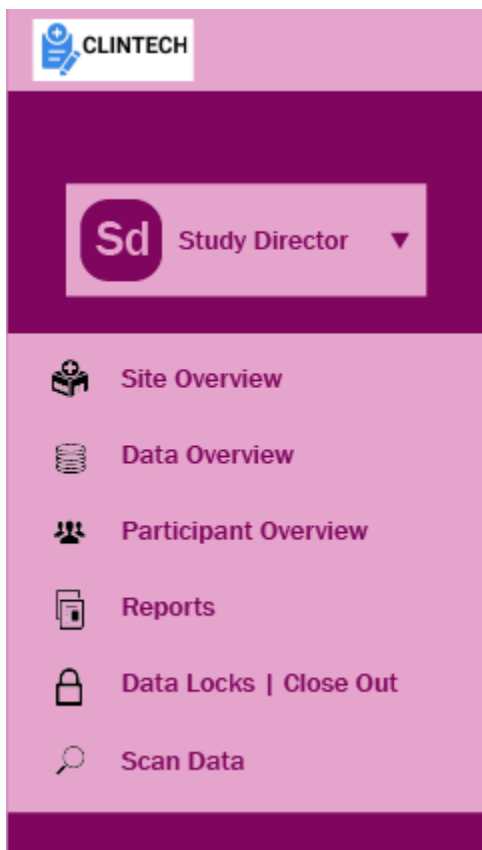
For secure control, Clitech has permission-based roles and responsibilities within Consent Director. Review the table below to learn more.

#### Legend:

-  Select for instructions on how to perform this task
-  Yes
-  No
-  Only if a user, in that role, is assigned to that site

Permissions	Role		
	Administrator	Consent Creator	Consent Document Handler
Create/edit participants 			
Create, publish, archive, and clone document templates			
View document template list			
View Participant Document List			
Download and print signature document			
Assign / send document to signers and resend email invites			
Void document workflow			
View and download documents			
View participants list			
View unsigned documents			
Schedule and initiate Televisit			
Manage users			
Assign users to Sites in the Consent Manager application			

## Summary of Data Management roles



All these roles below allow users to work with de-identified data collected for all the sites in an operational study through the Study Director app, placing them into the **Application / functional access role category**. **Note: These roles cannot access Study Constructor.**

### Data Evaluator

Provides read-only, de-identified access to all of the data collected in the study. They can see consent data, audit trails, locks, and are able to export reports.

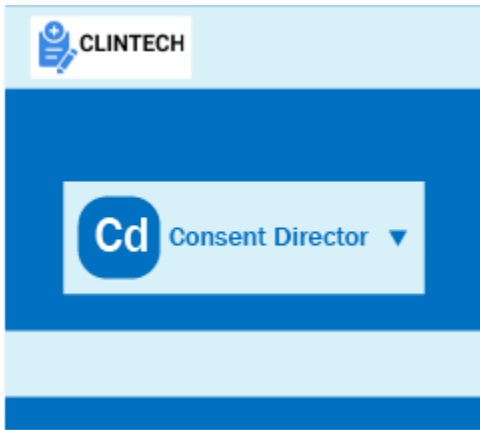
### Data Processor

Provides read-only, de-identified access to all of the data collected in the study and is for data managers who typically work in a remote capacity. They can see consent data, audit trails, and locks. They are able to export reports and create soft & snapshot

locks.

### Lead Data Processor

Provides read-only, de-identified access to all of the data collected in the study and is for data managers who typically work in a remote capacity. They can see consent data, audit trails, and locks. They are able to export reports and create soft & snapshot and hard locks.



Appearance of Consent Director to all three Data Management roles mentioned above. Notice that,

because these roles are **Study-Level**, no PII is visible:

Below, you will find a table that outlines the specific permissions of each of the above Data Management roles.

## Consent Roles and Permissions

### Data Management Roles

For secure control, Clintech has permission-based roles and responsibilities within Consent Director. Review the table below to learn more.

#### Legend:



Select for instructions on how to perform this task



Yes



No

Permissions	Role		
	Lead Data Processor	Data Processor	Data Evaluator
View response data and audit trail	✓	✓	✓
View Consent (Classic) Status	✓	✓	✓
Apply Review Types associated to your role	✓	✓	✓
Export reports	✓	✓	✓
View locks	✓	✓	✓
Create Soft or Snapshot lock	✓	✓	✗
Create Hard Lock	✓	✗	✗

## Who can see what?

As all consent data is protected information, only certain roles have access to Personally Identifiable Information (PII). Below is a chart that summarizes information viewing permissions:

**Legend:**

yes



no

Category	Role	Can See Participant Information?
Study Configuration	Administrator	✓
	Consent Creator	✗
	Consent Document Manager	✓
Site	Site Director(Signing Role)	✓
Data Management	Data Evaluator	✗
	Data Processor	✗
	Lead Document Processor	✗

## Understanding the relationship between roles created in Study Creator and Consent Director

The interplay of roles within different applications may seem confusing at first. This is because the procedures creating roles at the **Study-Level** differ somewhat from creating them at the **Site-Level**. For instance, as you've seen, these roles are created at the **Study-Level** in the Study Constructor application:

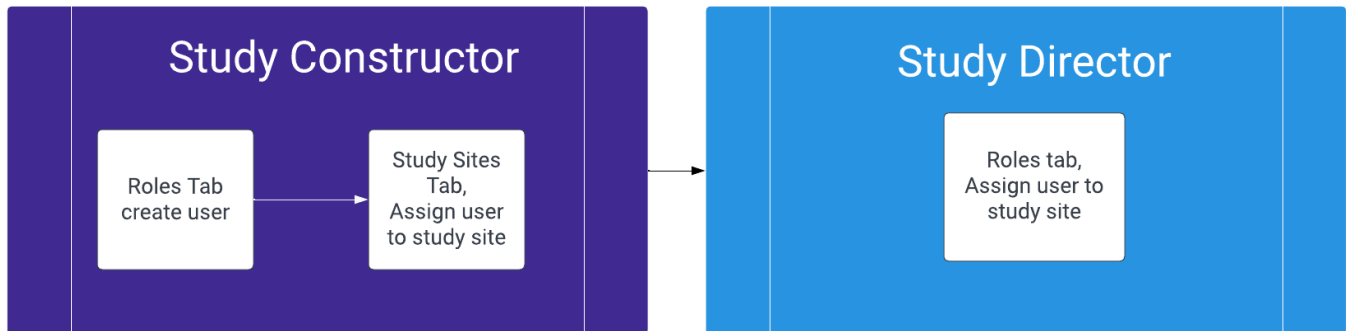
- Administrator
- Consent Creator

Roles can be created and assigned in Study Constructor by those with **Study-Level** access in two different tabs. Those created in the Roles tab will have **Study-Level** access. Those created in the Site Roles section of the Study Sites Tab will have Study-Level Access.

Roles can also be created by those with **Study-Level** access at the **Study-Level** ( Administrator ) Let's look at the larger workflow role creation workflows to get an idea.

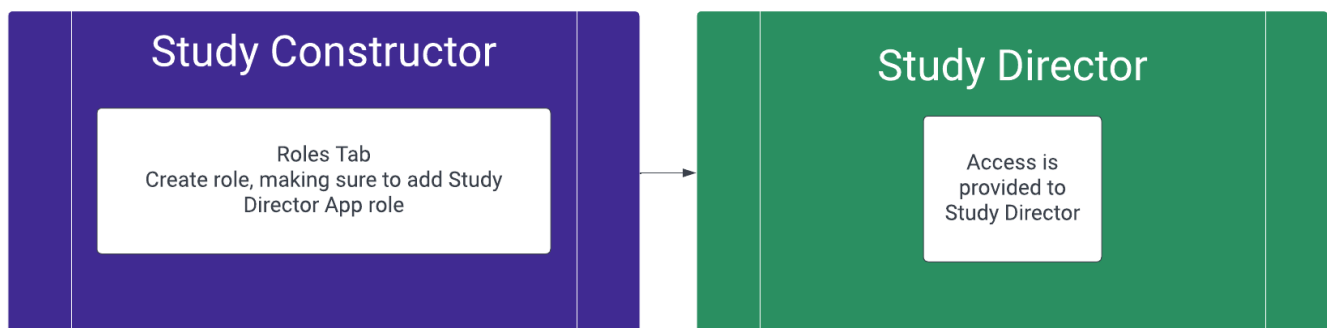
- Study Constructor and Consent Director

In Study Constructor, an Administrator creates **Study-Level** roles in the Roles tab. The Administrator then assigns them to Sites via the Sites tab, selecting a **Site-Level** role there. The Administrator must then switch to Consent Director and find the user they've just assigned in Study Constructor and assign that individual to a specific site.



- Study Constructor and Study Director

In Study Constructor an Administrator creates **Study-Level** roles in the Users tab. For a user to access Study Director, the same individual must also have an additional role: Study Director App.





## Common workflows for creating specific roles

Now, let's look at the steps necessary for an Administrator to create key users.

- Consent Creator



[Scan the code or click this link to see a video that shows this process](#) (note, link is inactive to protect brand)

1. Log in to Study Constructor
2. Select the **Roles** tab in the left menu
3. Click the “**+Create**” button
4. Fill in the desired information (Only an email address is required)
5. Select the role Consent Creator from the dropdown
6. Click the “**Create Account**” button in the upper right
7. Log in to Consent Director
8. Click on the **Roles** tab in the left menu
9. Find the user you created previously in Study Builder
10. Scroll down to the Assign Sites tile
11. Click the **+ Assign** button
12. Select your desired site (you can choose multiple sites), and then click the **Assign** button

- Consent Document Handler



[Scan the code or click this link to see a video that shows this process](#) (note, link is inactive to protect brand)

1. Log in to Study Constructor
2. Select the **Roles** tab in the left menu
3. Click the “**+Create**” button
4. Fill in the desired information (Only an email address is required)
5. Select the role Consent Document Handler from the dropdown
6. Click the “**Create Account**” button in the upper right
7. Click the **Study Sites** tab in the left menu
8. Click on your desired site.
9. Scroll down to the Site Users tile and click on the “**Assign Site User**” button
10. Search for the user you previously created.
11. Select the role Site Director
12. Click the “**Add Site Users**” Button
13. Log in to Consent Director
14. Click on the **Roles** tab in the left menu
15. Find the user you created previously in Study Constructor
16. Scroll down to the Assign To Sites tile
17. Click the **+ Assign** button
18. Select your desired site (you can choose multiple sites), and then click the “**Assign**” button

- Site Director (Signing Role)



[Scan the code or click this link to see a video that shows this process](#)

1. Log in to Study Constructor
2. Select the **Roles** tab in the left menu
3. Click the “**+Create**” button
4. Fill in the desired information (Only an email address is required)
- 5. Do not select a role.**
6. Click the “**Create Account**” button in the upper right
7. Click the **SStudy Sites** tab in the left menu
8. Click on your desired site.
9. Scroll down to the Site Users tile and click on the “**Assign Site User**” button
10. Search for the user you previously created.
11. Select the role Site Director
12. Click the “**Add Site User**” Button
13. Log in to Consent Director
14. Click on the roles tab in the left menu
15. Find the user you created previously in Study Constructor
16. Scroll down to the Assign To Sites tile
17. Click the **+ Assign** button
18. Select your desired site (you can choose multiple sites), and then click the “**Assign**” button

- Data Management Roles



[Scan the code or click this link to see a video that shows this process](#)

1. Log in to Study Constructor
2. Select the **Roles** tab in the left menu
3. Click the “**+Create**” button
4. Fill in the desired information (Only an email address is required)
5. Select either the role Data Evaluator Data Processor, or Lead Data Processor from the dropdown. **Do not combine these roles with each other.**
6. Also assign the Study Director App role to whatever role you selected in the previous step
7. Click the “**Create Account**” button in the upper right

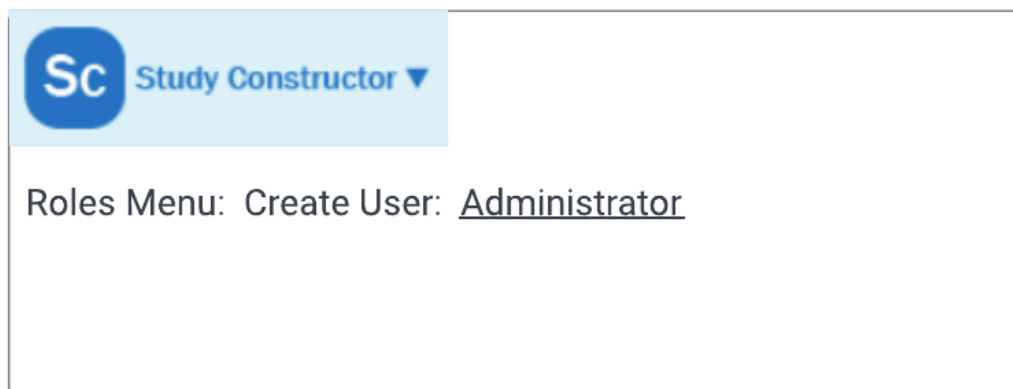
## Personas

### What Roles should I assign?

#### Partner Users:

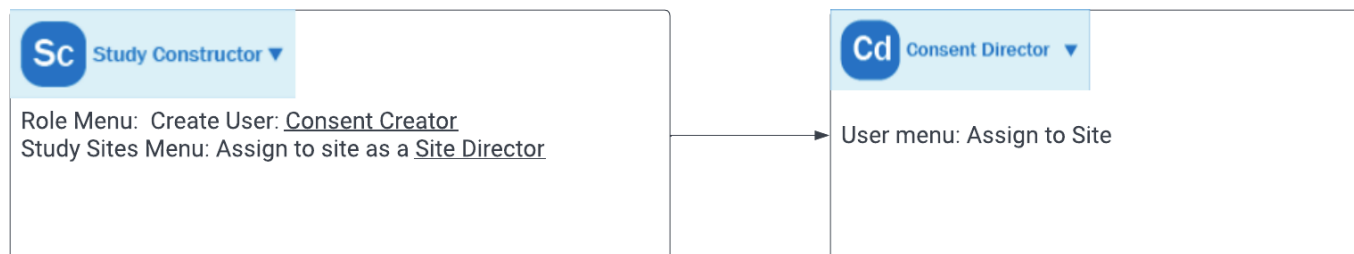
##### Administrator

Description: I'd like this user to have access to everything, from creating and assigning users, to seeing all consent data (including PII), to being able to perform all tasks. Use this Application and these menus:



##### Consent Creator

Description: I'd like this user to be able to create document templates in Consent Director. They are building consents. They will not be able to see PII. They will only have access to the Templates tabs in Consent Director:



## Consent Document Handler

Description: I'd like this user to be able to create individualized documents from published templates and send them to participants. They will be able to see the PII of participants, but only at the sites I assign them to and only have access to the Study Participants and Consents tabs.



## Site Director

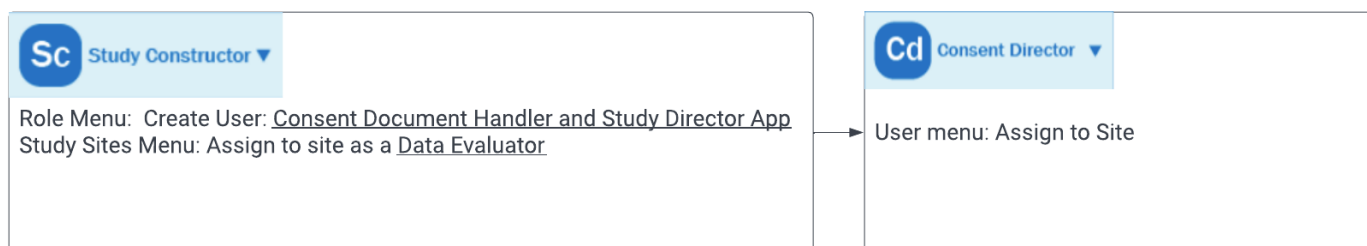
Description: I'd like to give this user a signing role in a document. They will be able to review and sign a document.



## Data Management Roles (CRAs often assume these roles but never all three for one person)

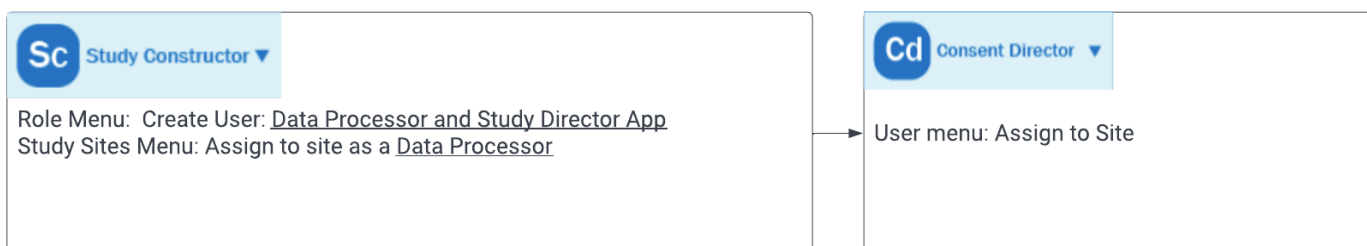
### Data Evaluator

Description: I'd like to give this user the ability to view deidentified consent data but not create or delete them:



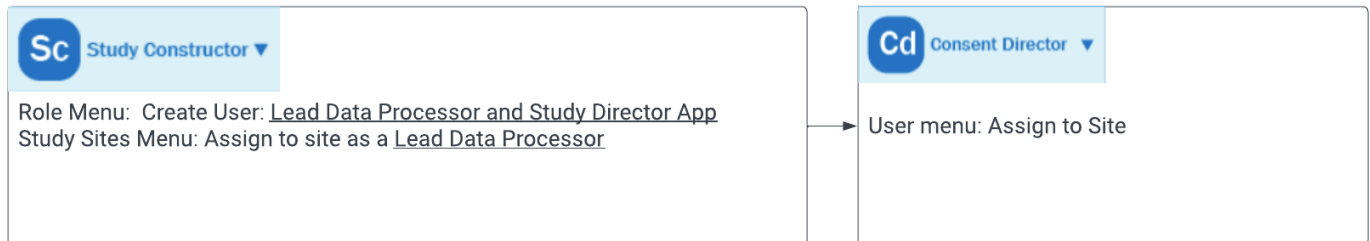
### Data Processor

Description: I'd like to give this user the ability to view deidentified consent data but not create or delete them. They should be able to create a soft or snapshot lock:



## Lead Data Processor

Description: I'd like to give this user the ability to view deidentified consent data but not create or delete them. They should be able to create any type of database lock, including a hard lock:





## Best Practices

### **Best Practice 1: Do not assign Site-level roles to study configuration and data management users**

Clintech recommends that you do not assign any of the three Site-level roles (for instance, Site Director) to users who also fill any of the study configuration or data management functions.

Users with Site-level roles can potentially see Personally Identifiable Information (PII).

### **Best Practice 2: Select only site-level roles when assigning a user to a Site**

When you assign a user to a Site, pick only one of the Site User roles. Even though you can select data management roles when you link the user to a Site, we recommend that you do not.

See Best Practice 1 above for an explanation.

### **Best Practice 3: Do not give one user both Consent roles**

A single user should not be assigned both the Consent Creator and Consent Document Handler. Doing so can cause problems when the user tries to access Consent Director

### **Best Practice 4: Limit or avoid assigning the Administrator role**

The Administrator role allows comprehensive access to study configuration and consent data. Even users who do not intend to do so can inadvertently change key study settings, modify the permissions of other users if given this "overpowered" role.

### **Best Practice 5: Assign single roles whenever possible during development and testing, as well as in production**

During the configuration and testing phases of a study, it may seem easier to give a relatively small number of personnel a variety of roles. Doing so means a user only needs to remember a single set of login credentials to access multiple applications. However, this practice does not reflect how user assignments work in a real world study and may lead to the reporting of invalid defects.

Best Practice 6: We suggest **NOT** giving the Study Director App role to users who fill these functions:

- Study Designer
- Study Evaluator
- Site Assistant
- Engineer
- Consent Creator
- Consent Document Handler

If you assign Study Director App to users with the above roles, they will be able to login to Study Director and see the application's Menu, including Reports. However, they will not be able to view study data or perform other work in Study Director

This content is meant for training purposes only. It is proprietary and includes confidential information of ClintechInc. It is not intended to be distributed, copied, or modified without the written consent of Clintech Inc.

For questions about this content please email,  
[support@clintech.com](mailto:support@clintech.com)