

User Access Level (Roles and Privileges)

Background

OpenMRS uses privileges and roles to control access to data within the system. Privileges define what can or cannot be done in the system (e.g., *Edit People* or *Add User*) while Roles are used to group privileges into a more manageable grouping. To make the system easier to manage, roles can contain other roles as well as privileges. Roles inherit all privileges that exist within the child roles.

OpenMRS Roles & Privileges

Privileges: Some OpenMRS privileges are built into the system and cannot be deleted. Other privileges may be added by modules. It is unlikely that you will be adding new privileges yourself, since privileges are only useful when they are understood and used by the system. On the other hand, you will definitely be creating new roles to fit your needs and will be managing privileges within those roles.

Roles: OpenMRS also has some special roles that are predefined and cannot be deleted. These roles are *Anonymous*, *Authenticated*, *Provider*, and *System Developer*.

- a. *Anonymous* role: Any privileges granted to the *Anonymous* role will be available to people without logging into the system. Generally, *Anonymous* privileges are kept very restricted, since patient information might otherwise be compromised.
- b. *Authenticated* role: Privileges granted to the *Authenticated* role are granted to anyone that logs into your system, no matter what other role(s) they might be assigned. Granting privileges to the *Authenticated* role is an easy way to grant privileges to all users of the system.
- c. *Provider* role: Provider represents the most basic care provider and can serve as the basic role from which to build specialized providers (physicians, clinical mentors, nurses, medical students, etc.).
- d. *System Developer* role: The *System Developer* role is automatically granted full access to the system and should only be granted to system administrators. Super users (system administrators) are automatically granted all privileges in the system; therefore, you must be very careful to protect your system administrator password.

See the [Privilege Helper](#) module which lets you figure out what privileges are required to perform a particular task, and then helps you assign those privileges to roles. Common scenarios would be to define roles like *Provider* that is inherited by *Physician*, *Nurse*, *Clinical Officer*, etc. You can then control most of the privileges within the *Provider* role and those changes will affect all types of providers in the system. If you find

that you have to go through multiple roles and edit them to make a change, then you could likely

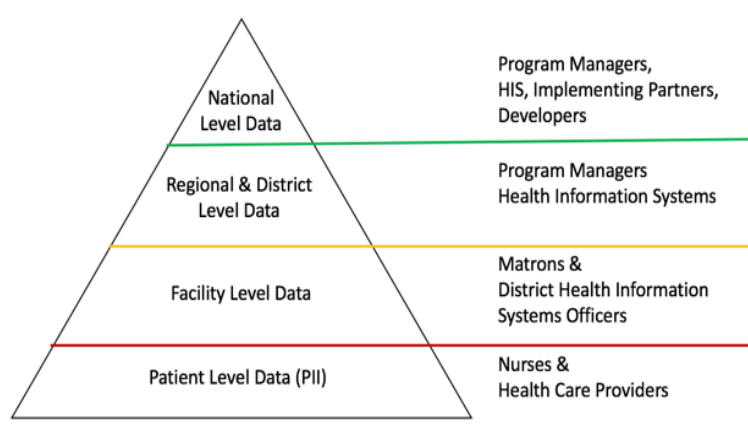
Recommendations for PTracker User Access Levels

PTracker has the following potential users (Facility staff) noted during our pilot site assessments:

- Senior Nurse – Enter ANC and PNC patient data
- Nurses (midwives) – at district hospitals enter L&D patient data. In health centers and Clinic they also enter ANC and PNC data.
- Health Assistants – In high volume sites operating with limited staff, health assistants enter PNC (Mother-Baby follow up data) to help ease the nurses' workload
- Data clerks – Enter data retrospectively for ART sites
- Nursing Students – Enter ANC and PNC patient data
- Medical Students - At L&D enters patient data

Privileges for these facility staff can vary between facilities based on workload and staffing. For example, in smaller facilities, it will be possible to have a Health assistant with similar privileges as a nurse in a larger facility. Therefore, defining roles will provide an efficient way to manage user access level.

Referencing the OpenMRS definition of User Access Level, we recommend at minimum the following privileges for these various facility staff.



Role	Privilege(s)	Users
Data Entry Clerk	Register Patient View patient Edit patient Add Encounters (follow-up visits)	Nurses Health Assistants Medical Students Nursing Students

Role	Privilege(s)	Users
	View/Run Reports	
Facility Manager	Register Patient View Patient Edit patient Add Encounters (follow-up visits) Edit Encounters (follow-up visits) View/Run Reports	Facility In-charges RM&E/ HIS Staff
	View/Run Reports	PMTCT program managers (national) District program officers
System Administrator (The administrator's privileges will be restricted to the national level)	Configure System Add Users Edit User Account Information	National HIS Officers IT analyst

**Encounters are follow-up ANC/PNC visits*

Acknowledgment

- Adopted from [OpenMRS Wiki](#), last modified by [Rafal Korytkowski](#) on [2012-06-04](#)