

# Chapter 15. Users and User Roles

DHIS 2 comes with an advanced solution for fine-grained management of users and user roles. The system is completely flexible in terms of the number and type of users and roles allowed.

## 15.1. Users

A user in the DHIS 2 context is a human who is utilizing the software. Each user in DHIS 2 has a user account which is identified by a username. A user account allows the user to authenticate to system services and be granted authorization to access them. To log in (authenticate) the user is required to enter a valid combination of username and password. If that combination matches a username and password registered in the database, the user is allowed to enter.

In addition, a user should be given a first name, surname, email and phone number. This information is important to get correct when creating new users since certain functions in DHIS 2 relies on sending emails to notify users about important events. It is also useful to be able to communicate to users directly over email and telephone to discuss data management issues or to sort out potential problems with the system.

A user in DHIS 2 is associated with an organisation unit. This implies that when creating a new user account that account should be associated to the location where user works. For instance when creating a user account for a district record officer that user account should be linked with the particular district where she works. The link between user account and organisation unit has several implications for the operation of the system:

- In the data entry module, a user can only be entering data for the organisation unit she is associated with and the organisation units below that in the hierarchy. For instance, a district records officer will be able to register data for her district and the facilities below that district only.
- In the user module, a user can only create new users for the organisation unit she is associated with in addition to the organisation units below that in the hierarchy.
- In the reports module, a user can only view reports her organisation units and those below. (This is something we consider to open up to allow for comparison reports.)

A user role in DHIS 2 is also associated with a set of user roles. Such user roles are discussed in the following section.

## 15.2. User Roles

A user role in the DHIS 2 context is a group of authorities. An authority in this regard means the permission to perform one or more specific tasks. For instance, a user role may contain authorities to create a new data element, update an organisation unit or view a report. Such a group of authorities constitutes a user role.

In a health system the users are logically grouped with respect to the task they perform and the position they occupy. Examples of commonly found positions are:

1. National health managers
2. National health information system division officers (HISO)
3. Province health managers
4. District health records and information officers (DHRIO)
5. Facility health records and information officers (HRIO)
6. Data entry clerks

When creating user roles such positions within the health system should be kept in mind and it is often sensible to create a user role dedicated for each of those positions. The process of creating user roles should be aligned with the process of deciding which users are doing what tasks in the system.

First it should be defined which users should fulfill the role as system administrators. This will often be a part of the members of the national HIS division and should have full authority in the system. Second a user role should be created

roughly for each position. A sensible consideration of what authorities should be given each role must be done. An important rule is that each role should only be given the authorities which are needed to perform the job well - not more. When operating a large, centralized information system there is a need to coordinate the work between the people involved. This is made easier if only those who are supposed to perform a task have the authorities to perform it.

An example might highlight this issue: The task of setting up the basic structure (meta-data) of the system is critical to the system and should only be performed by the administrators of system. This means that the system administrator user role should have the authority to add, update and delete the core elements of the system such as data elements, indicators and data sets. Allowing users outside the team of system administrators to modify these elements might lead to problems with coordination.

National and provincial health managers are often concerned with data analysis and monitoring. Hence this group of users should be authorized to access and use the reports module, GIS module, data quality module and dashboard. However they would not need authority to enter data or update data elements and data sets. District information officers are often tasked with both entering data into the system coming from facilities which are not able to do so directly as well as monitoring, evaluation and analysis of data. This means that they will need access to all of the analysis and validation modules mentioned above in addition to the authority to access and use the data entry module.

In addition, a user role is associated with a collection of data sets. This affects the data entry module in that the user is only allowed to enter data for the data sets registered for her user role. This is often useful in situations where one wants to allow officers from health programs to enter data for their relevant data entry forms only.

A user can be granted one or any number of user roles. In the case of many user roles, the user is privileged with the sum of all authorities and data sets included in the user roles. This means that user roles can be mixed and matched for special purposes instead of merely creating new ones.

An important part of user management is to control which users are allowed to create new users with which authorities. In DHIS 2 one can control which users are allowed to perform this task. In this process the key principle is that a user can only grant authorities and access to data sets that the user itself has. The users at national, province and district level are often relatively few and can be created and managed by the system administrators. If a large part of the facilities are entering data directly into the system the number of users might become unwieldy. Experience suggests that delegating and decentralizing this task to the district officers will make the process more efficient and support the facility users better.