Overview

6.6.4 Project User Roles · https://i2b2.org/docs/6-6-4-project-user-roles/

Each user will have at least two roles per *user_id* and *project_id* combination. These two roles can be further defined as a **Data Protection role** and a **Hive Management role**.

The data protection role establishes the detail of data the user can see while the hive management role defines the level of functionality the user has in a project. The following tables summarize the roles in a hierarchical order of least to most access.

Data Protection Roles

Role	Access Description
DATA_OBFSC	OBFSC = Obfuscated • The user can see aggregated results that are obfuscated (example: patient count). • The user is limited on the number of times they can run the same query within a specified time period. If the user exceeds the maximum number of times then their account will be locked and only the Admin user can unlock it.
DATA_AGG	AGG = Aggregated • The user can see aggregated results like the patient count. • The results are not obfuscated and the user is not limited to the number of times they can run the same query.

DATA_LDS	LDS = Limited Data Set • The user can see all fields except for those that are encrypted. • An example of an encrypted field is the blob fields in the fact and dimension tables.
DATA_DEID	DEID = De-identified Data • The user can see all fields including those that are encrypted. • An example of an encrypted field is the blob fields in the fact and dimension tables.
DATA_PROT	PROT = Protected • The user can see all data, including the identified data that resides in the Identity Management Cell.

Hive Management Roles

Role	Access Description
USER	Can create queries and access them if he / she is the owner of the query.
MANAGER	Can create queries as well as access queries created by different users within the project.

Note

Additional roles can be added to the PM_PROJECT_USER_ROLES table but there will not be any recognized hierarchy to those roles.