Security0

The application must implement basic security behaviors:

Category	Behavior
Authentication	Authenticate using the combination of domain id, project id, user name and a password.
Authorization	Based on the user role, the user may access setfinder queries created by other users, view patient notes, etc.
Confidentiality	Sensitive data must be encrypted (Patient Notes).
Data Integrity	Data sent across the network cannot be modified by a tier.
Auditing	All queries and retrieval of patient data is stored for auditing purposes.
User Lockout	Users with the role of DATA_OBFSC will be limited to the number of times they can run the same query in a project. Once they reach that limit their account will be locked out and they will not be able to run queries again until an administrator unlocks the account.