

Non Functional Requirements

Legend (For Sprint 2)

Bolded NFRs are currently fulfilled in the walking skeleton for Sprint 2.

Architecturally Significant
Architecturally Not Significant
Out of Scope

Security

ID	Description
<SEC1>	The system protects sensitive information from being exposed to external entities.
<SEC2>	Implement encryption between client and server communications.
<SEC3>	Store all sensitive information using industry-standard encryption.
<SEC4>	Store passwords using industry standard hashing algorithms (bcrypt).

Privacy

ID	Description
<PRV1>	The system provides robust access control, so each internal entity can only view data they need to do their job, thus protecting the patients' privacy.
<PRV2>	Provide separate privileges for user and admin level users.

Ease of use

ID	Description
<USE1>	The system should be easy to use and convenient for even non-technical actors to use and save time.
<USE2>	Minimize the total number of different pages a user must visit to use the system.
<USE3>	Simplify the layout of each page, only displaying information pertinent to the user.
<USE4>	Highlight buttons that perform key functionalities.

Error handling

ID	Description
<ERR1>	The system should detect errors in entered data and prevent, correct or handle them to ensure data integrity.
<ERR2>	Implement input validation to prevent the entry of invalid data.
<ERR3>	Provide clear and actionable error messages to guide users in correcting errors.
<ERR4>	Log all system errors for review and resolution.
<ERR5>	Monitor error logs and messages from the system to minimize wait time for providers use.
<ERR6>	Ensure the system can handle common errors such as incorrect data formats, missing required fields, and data entry discrepancies.

Flexibility

ID	Description
<CTM1>	The system will be used by many therapists, doctors, patients and other actors, each with their own unique situations and needs, and the system needs to accommodate all of them.
<CTM2>	Ensure the system can scale to handle varying workloads and user volumes.
<CTM3>	Administrators should be able to create/manage/delete accounts for Providers through a portal on the system, without directly interacting with the database.

Interoperability

ID	Description
<IOP1>	The system should integrate with existing Electronic Health Record and Patient Management systems.
<IOP2>	Ensure that non sensitive data can be shared with varying clinics in case of patient transfer.
<IOP3>	Provide APIs for data exchange within external systems for added security.

Data management

ID	Description
<DAT1>	The system should allow for the organization, management and processing of a diverse dataset and enable powerful and customizable analytics for its diverse set of stakeholders.
<DAT2>	Support import and export of various data in multiple formats.
<DAT3>	Allow users to filter through data they are authorized to access.

