

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 by hashing and using industry standard encryption on sensitive information like patient info and data from being exposed to external threats.
<SEC2>	Using HTTPs between client and server communications.
<SEC3>	Store all sensitive information using industry-standard encryption. (TBD)
<SEC4>	Store passwords using industry standard hashing algorithms (bcrypt).

Privacy

ID	Description
<PRV1>	The system ensures that each staff member can only access the information they need, keeping patients' privacy protected.
<PRV2>	Give different access levels to regular users and administrators.

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>	Make each page simple by showing only the information the user needs.
<USE4>	Make important buttons stand out.

Error handling

ID	Description
<ERR1>	The system should catch mistakes in the data and fix or manage them to keep the information accurate.
<ERR2>	Use input checks to stop invalid data from being entered.
<ERR3>	Show clear and helpful error messages to guide users in fixing mistakes.
<ERR4>	Log all system errors for review and resolution.
<ERR5>	Monitor error logs and messages from the system to minimize wait time for provider use.
<ERR6>	Make sure the system can deal with common mistakes like wrong data formats, missing required fields, and data entry errors.

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.

