**Data collected by the app**

**Personal Information**

1. Patient’s full name
2. Patient’s full address
3. Patient’s Gender, Birthdate and Age
4. Patient’s Photographs and files
5. Notes on symptoms and other information
6. Medical Diagnostics and Vitals (Body temperature, pulse rate, blood pressure,etc)
7. Medical treatment information
8. Medical appointments
9. Patients’ doctor

**Non-Personal Information**

1. **App usage data** - This App Usage Data may include information such as your computer’s IP address, device model and version, device identifier, operating system, time zone, name of your mobile operator or ISP, application performance measurements, and error conditions
2. **App’s log data** – This log data may include certain outputs of the app, success and failure states of network calls, etc.

**How we store your data**

The app is meant for both Offline as well as Online use.

**How do we use your data**

1. We do not sell your data
2. All these personal details helps in creating a record of a certain patient. It helps the Users of this app (the Providers) to maintain the track of the patient.
3. For users’ assistance we may require the personal details of the Patients (such as DoB, name, etc) to easily track the patient and find their records
4. We may aggregate and combine all personal information that we receive through the app from the Patient’s section as well as from the app’s log and usage data and use them to provide better experience across our platforms (both Web and Mobile)

**Information Sharing and Disclosure**

1. The **Patients** are not our immediate/Primary/End Users of this app
2. The **Providers** (Nurse, Doctor, Clerk) are the primary End-users of this app
3. The Patients’ data is shared across various Providers with respect to the proceedings of the Patient’s visit, treatment, etc
4. **Compliance with Laws and Law Enforcement:** Please fill this as per the Law. I do not have any information regarding this

**Data Retention**

We retain all the data generated by the app and web client. If an account is deactivated/deleted, we move the data related to that account away from our active database BUT is retained in our Backup database.

**Security – How we protect your Data**

**Client Side**

1. Hashing Users’ Password – this App uses [BCrypt](https://en.wikipedia.org/wiki/Bcrypt) hashing function.
2. Local Database Encryption – Uses [AES-256 Cipher](https://pl.wikipedia.org/wiki/Advanced_Encryption_Standard) (using a combination of username and password as its key)

**Server Side**

1. Patient’s Identifiers are Validated using “[Mod10](https://pl.wikipedia.org/wiki/Advanced_Encryption_Standard)” algorithm. This is used while creating new Patient’s Identifiers and avoid errors.
2. Data is transmitted through a Secure SSL Connection
3. Strings are Hashed using [SHA-512](https://en.wikipedia.org/wiki/SHA-2)

**Reporting a Problem**

If you feel your account may have been compromised, or you discover abuse or misuse of OpenMRS Services, the Site or the OpenMRS App, please report it immediately to [provide\_a\_valid\_support\_link] and we’ll investigate.

**Policy towards Children**

This app is not intended for use by children under the age of 18. We will not knowingly collect any personal information from visitors under the age of 18. With any questions regarding this matter, please contact us at [provide\_a\_valid\_support\_link]

However this app may collect data of children (Patients) under 18 and they will be subjected to the above stated Policies.

**Changes to Privacy Policy**

The Privacy Policy is subjected to change without any prior notice. However, a statement regarding change in Policies will be posted on this page/document. Please check from time to time to ensure you are aware with the latest Policies.