# Implementation

7.6.1 As a Patient, I want to download my medical history in a portable and secure format, so that I can easily transfer it to another healthcare provider.

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

A screen shot of a computer code

Description automatically generated

A computer screen shot of a program code

Description automatically generated

7.6.2 As a Patient, I want to request the deletion of my personal data, so that I can exercise my right to be forgotten under GDPR.

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

If the user logs in with their Google account, they will be able to delete the account.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Once deleted the account the user will be redirected to the log in page.

# Privacy Policy of SARM

#### 7.6.3 As a Patient, I want to know what data will be processed, in what manner, and how I Acceptance can exercise my rights.

#### 7.6.4 As a Patient, I want to know for how long my personal data will be kept.

## 1. Introduction

SARM (Surgery Scheduling and Management System) respects privacy and is committed to protecting your personal data in compliance with the General Data Protection Regulation (GDPR). This policy outlines how we collect, process, store, and protect your data, along with your rights as a data subject. You can contact our team through this 210 987 122 customer support line, available from 8 am until 10 pm.

This policy will remain accessible at any time through the "Profile Settings" menu.

## 2. Personal Data Collected

Our team collect the following personal data based on specific and explicit purposes:

* **Identification**: Full name, date of birth.
* **Contact Information**: Email address, phone number, emergency contact.
* **Medical Data**: Medical history, medical record number.
* **Appointment History**: Information about consultations and surgeries.

We may also collect information provided by third parties (such as doctors or hospitals) when necessary to deliver our services and we will notify the data subjects.

## 3. Legal Basis for Processing

We rely on the following legal bases to process your data by following the Article 6(1):

1. **Consent**: explicitly provided by the patient for specific purposes.
2. **Contract Execution**: necessary for providing services such as scheduling and managing surgeries.
3. **Legal Obligation**: to comply with applicable laws, such as storing medical records.
4. **Public Interest**: related to public health and hospital resource management.

## 5. Data Subject Rights

Patients have the following rights under Articles 12-23 of the GDPR:

1. **Access**: know if your data is being processed and obtain a copy.
2. **Rectification**: correct inaccurate or incomplete data.
3. **Erasure** ("Right to Be Forgotten"): request the deletion of data when no longer needed.
4. **Restriction of Processing**: limit processing under certain circumstances.
5. **Data Portability**: receive your data in a structured format and transfer it to another controller.
6. **Objection**: refuse processing in specific situations, such as direct marketing.
7. **Complaint**: file a complaint with a supervisory authority, such as the CNPD.

## 6. Data Retention and Legal Obligations

SARM will delete retained customer personal data after 10 years after the last consultation, as required by national health laws, relative to medical records. The contact information data is retained while the account is active and deleted 6 months after inactivity unless legally required otherwise. Our team can use anonymized data for research and statistical purposes.

Certain data may be retained due to legal obligations, including documentation of consent for medical treatments, records related to litigation or legal audits and data for public health monitoring or legal investigations.

## 7. Security Measures

SARM team implement the following measures to protect your data:

* **Access Control**: restricted to authorized personnel only.
* **Encryption**: secure storage of sensitive data.
* **Regular Audits**: periodic assessments to identify and address vulnerabilities.