

## Privacy Policy Summary

Project title:HealOfy:A Self-help App

Team no: 15

Team Members:Shreya Chavan,Aparajita Kumari, Nandini Yadav ,Nikita Mishra

Please answer the following in as much detail as you can provide. In the table below, “user” refers to the “data subject” – the person(s) whose personal data is being collected and processed in your application.

<b>Data Fiduciaries</b>  <i>Identify the organizations/entities that “determine the purpose and means of processing of personal data”</i>	<b>Purpose Determination:</b>  The app's primary purpose is to facilitate communication between patients and doctors, allowing patients to register and schedule appointments. This clearly defines the reason for processing personal data, which is to facilitate medical consultations and appointments.  <b>Means of Processing Determination:</b>  The app provides specific features such as appointment scheduling, chat functionality between patients and doctors, and access to podcasts and jokes. These features are designed to serve the purpose of facilitating communication and providing additional support to patients. The app's structure and functionality determine how personal data is processed to enable these features.
<b>Nature of the application/platform</b>  <i>Summarize the overall purpose of your solution – what it broadly does, and not how it does it</i>	The Healofy platform is designed to provide comprehensive healthcare support to users. Its overall purpose is to facilitate communication and interaction between patients and healthcare providers, enabling users to schedule appointments, consult with doctors, access educational resources such as podcasts, and engage with supportive content like jokes. In essence, Healofy aims to serve as a holistic healthcare solution, offering a range of features to support users' physical and emotional well-being.
<b>Personal data collected</b>	<i>For each item of personal and/or sensitive data, mention the item and the purpose for which it is collected List one data item per line</i>
<b>Data Item</b>	<b>Purpose</b>
<b>FirstName</b>	To store the firstname of the user and identify the patient/doctor
<b>LastName</b>	To store the lastname of the user and identify the patient/doctor
<b>Age</b>	To know if the user is above 18 years of age
<b>Email</b>	To store it as a unique identification id
<b>Experience(doctors)</b>	To know the years of experience for better recommendation purposes
<b>LicenseId(doctors)</b>	To verify idc the doctor has a verified license id

<b>Informed consent</b> <i>List the steps at which user consent is obtained, and the mechanism of consent collection.</i>	<p>When registering into the application, the patient is advised to be mindful and focused about the data they are letting out because it will be shown to the doctors once registered.</p>
<b>Data Minimization</b> <i>Are all data items collected required for the proposed processing? Identify those that are not needed for the stated purposes</i>	<p>Only the data set like Age, Name, Severity of the patient are at display</p>
<b>Confidentiality</b> <i>How is this ensured. List any 3<sup>rd</sup> parties with whom the data is shared, and the purpose</i>	<p>Here the moderators are the only one who can observe the chats between patients and doctors. This is to ensure that everything is operating well and within guidelines.</p>
<b>Purpose Limitation</b> <i>Identify mechanisms in place to prevent data use for other than stated purposes</i>	<p>We have a separate table in the database to store username and passwords in the database. This helps us to work with patient data without showing the critical information of the patient when a doctor wants to see them as we retrieve just the information from the patient table not the users.</p> <p>All the passwords are encrypted while storing it in the database so that no kind of information leak can happen.</p>
<b>Security</b> <i>List the security related mechanisms and technical safeguards to protect privacy</i>	<p>Each role has a set of functionality they can work with. We have authenticated the entire app using role-based login so that a specific user who has a specific role can open a particular dashboard to retrieve information.</p> <p>We have established DTOs that interact with the API requests so that the database is not under any invasion threat.</p>
<b>Data Retention</b> <i>For what period of time is the collected data stored. What happens to the data at the end of that period</i>	<p>As long as the patient is associated with the app, a patient/doctor can delete their account and hence all their data will be removed.</p>
<b>Data Deletion Requests</b> <i>Describe the mechanism by which users can request deletion of some or all of their data. If no such mechanism exists, state so</i>	<p>If a patient no longer wants to use the app, they can delete their accounts and none of their personal data will be there. The posts that they had contributed to will still remain in the forum. No such mechanism has been created for the deletion of posts.</p>

<p><b>Account Deletion</b>  <i>How are requests for deletion of accounts by users handled. What happens to the data of accounts that are deleted</i></p>	<p>If a user decides to stop using the app, they have the option to delete their account, ensuring that none of their personal data remains stored within the platform. So, all of their data is safely removed.</p>
<p><b>Revoking Consent</b>  <i>Can users revoke some or all of the consent they have provided. What is the mechanism for revoking consent?</i></p>	
<p><b>Other Privacy related remarks</b></p>	