

Privacy Policy for Shifa Patient APP

1. Purpose

This Privacy Policy outlines the principles and practices adopted by Shifa International Hospitals Limited. (the "Company") in relation to the collection, use, storage, transfer, and disclosure of personal and medical information of individuals using the Shifa Patient App. This Policy is intended to provide transparency and ensure compliance with all applicable legal standards, including fundamental privacy protections enshrined under Pakistani law.

2. Scope

This policy applies to all patients, clients and employees at Shifa International Hospitals Ltd (SIHL).

3. Policy with Procedure and Responsibilities

The Company acknowledges that the protection of personal data is a matter of legal and ethical responsibility. Accordingly, any personal information collected through the Service is being obtained with the informed, explicit, and freely given consent of the user. Users shall be clearly informed of:

- The nature and type of personal information collected;
- The purpose for which such information is processed;
- The legal basis for such processing;
- Their rights to access, correct, or request deletion of their personal data;
- The circumstances under which their data may be shared, which shall be limited to legal obligations, user authorization, or where strictly necessary for the performance of the Service.

The Company further undertakes that all personal data received will be treated with strict confidentiality and protected through reasonable technical and organizational safeguards to prevent unauthorized access, misuse, alteration, or disclosure.

By accessing or using the Service, users acknowledge and agree to the terms set out in this Privacy Policy. The Company reserves the right to update this Policy periodically in line with changes in the legal or regulatory framework, or as may be necessitated by operational requirements.

a. Interpretation and Definitions

i. Interpretation

The terms defined below shall have the meanings assigned to them whenever they appear in this Privacy Policy, regardless of whether they are used in singular or plural form. Headings are for reference purposes only and shall not affect the interpretation of this Policy.

ii. **Definitions**

For the purposes of this Privacy Policy:

- **Account** refers to a unique registration created by the user to access and utilize specific functionalities of the Service.
- **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the Company. "Control" refers to the ownership of at least fifty percent (50%) of the voting shares, equity interest, or other securities entitled to vote for the election of directors or other managing authority.
- **Application** refers to the *Shifa Patient App*, a mobile software application developed and maintained by the Company for patient engagement and service delivery.
- **Company** (also referred to as "We", "Us", or "Our") means **Shifa International Hospitals Limited**, a company incorporated under the laws of Pakistan with its principal place of business at Pitras Bukhari Road, Sector H-8/4, Islamabad, Pakistan.
- **Country** refers to the Islamic Republic of Pakistan.
- **Device** means any electronic equipment or computing tool used to access the Service, including but not limited to mobile phones, tablets, desktop computers, or other internet-enabled devices.
- **Personal Data** refers to any information relating to an identified or identifiable natural person, including but not limited to names, contact information, identification numbers, or health-related information collected through the Service.
- **Service** refers to the *Shifa Patient App* and its associated functionalities, interfaces, and platforms through which the Company provides healthcare-related services.
- **Service Provider** means any natural or legal person who processes data on behalf of the Company, including but not limited to third-party vendors, contractors, or consultants engaged to facilitate or support the provision of the Service.
- **Usage Data** refers to data that is collected automatically during the course of using the Service. This may include technical data such as Internet Protocol (IP) addresses, browser types, device identifiers, access times, and interactions with specific features of the Application.
- **User** (also referred to as "You" or "Your") means the individual accessing or using the Service, or, where applicable, the legal entity on behalf of which such individual is authorized to access or use the Service.

b. **Collecting and Using Your Personal Data**

i. **Types of Data Collected**

The Company may collect the following categories of personal data and such data shall be collected solely for the legitimate purposes specified herein.

1. **Personal Data**

While using the Service, you may be requested to provide certain personally identifiable information that may be used to contact, identify, or serve You. This information may include, but is not limited to:

- Full name (first name and last name);
- Email address;
- Mobile or telephone number;
- Residential address, including city, province, and postal code;
- Any other information voluntarily provided by You through forms, messages, or feedback functions within the Service.

The provision of such Personal Data shall be entirely voluntary. The Company will not collect such data without Your awareness and affirmative action.

2. Usage Data

Usage Data is collected automatically when You interact with the Service. This may include technical and diagnostic information such as:

- The Internet Protocol (IP) address of Your Device;
- The type and version of browser used;
- The pages or features of the Service that You visit or access;
- The date and time of Your access;
- The duration of Your interaction with specific features;
- Unique device identifiers;
- Diagnostic and performance-related metadata.

This data is collected for the purposes of system optimization, service improvement, analytical assessment, and to ensure security and accountability in the use of the Application.

3. Information Collected via Device Permissions

The Application may request access to and collect additional information stored or accessible on Your Device, including:

- **Location data:** to support location-based features and enhance service accuracy;
- **Access to camera and photo library:** where You voluntarily upload documents or media necessary for the functioning of specific features of the Service.

This information may either be stored locally on Your device or transmitted securely to the Company's servers or those of a designated Service Provider. You retain the right to grant, restrict, or revoke these permissions at any time through Your Device's settings.

c. Use of Your Personal Data

The Company shall process Personal Data strictly for legitimate, specific, and clearly defined purposes. All processing activities shall be carried out in a manner that respects user privacy and complies with legal obligations.

Subject to the bases outlined herein, the Company may use Your Personal Data for the following purposes:

i. Provision and Maintenance of the Service

To enable access to and continued functioning of the Application and its associated features, including troubleshooting, technical support, and monitoring of Service performance.

ii. User Account Management

To create, verify, and manage Your Account as a registered user of the Service and allowing access to various functionalities available to registered users. This may include authentication, access to health records or history, and personalization of the Service to meet Your specific needs.

iii. Fulfilment of Contractual Obligations

To carry out and perform any contractual relationship or transaction entered into by You with the Company, including the provision of healthcare services, processing of appointments, or provision of medical information or purchase of products and services.

iv. Communication with Users

To communicate with You via email, telephone, SMS, or mobile push notifications for the purpose of:

- Notifying You of system updates, administrative messages, or security alerts;
- Sending reminders related to appointments, prescriptions, or test results;
- Responding to queries, support requests, or service-related feedback.

v. Promotional and Informational Content

To send You updates, newsletters, or offers relating to services provided by the Company that may be similar to those previously availed, unless You have opted out of such communications. Users may withdraw consent to receive such materials at any time by following the unsubscribe procedure or notifying the Company.

vi. Request Management

To receive, respond to, and manage any requests or instructions initiated by You through the Application or other communication channels.

vii. Business Transfers

To evaluate or execute any potential merger, acquisition, restructuring, reorganization, or sale of assets, wherein Personal Data may form part of the assets transferred. In such cases, safeguards shall be implemented to ensure continuity of privacy obligations.

viii. Legal and Regulatory Compliance

To comply with any legal obligations imposed under applicable laws and to support regulatory audits, reporting, or dispute resolution.

ix. Service Improvement and Analytics

To carry out data analysis, usage trends, and customer behavior assessments in order to improve the quality, security, and effectiveness of the Service and enhance the user experience.

d. Sharing of Your Personal Data

The Company acknowledges its legal and ethical duty to maintain the confidentiality and integrity of all Personal Data collected. Accordingly, such data shall not be disclosed to any third party except in accordance with the provisions set forth in this Policy.

Subject to the foregoing, Your Personal Data may be shared in the following limited and controlled circumstances:

i. With Service Providers

The Company may engage third-party service providers to facilitate the provision of the Service, including but not limited to data hosting, analytics, support services, or secure payment processing. These providers shall act under strict contractual obligations that require them to:

- Process data only on the Company's instructions;
- Implement appropriate technical and organizational measures to safeguard data;
- Refrain from using the data for any purpose other than providing services on behalf of the Company.
- Maintain confidentiality.

ii. In Connection with Business Transfers

In the event of any proposed or actual merger, acquisition, restructuring, or transfer of Company assets, Personal Data may be disclosed to prospective or actual acquirers, subject to:

- Execution of confidentiality undertakings; and
- Continued application of privacy protections consistent with this Policy.

iii. With Affiliates

Your Personal Data may be shared with Affiliates of the Company for purposes consistent with those outlined in this Policy. All such Affiliated entities shall be required to observe data privacy standards no less protective than those contained herein.

iv. With Business Partners

The Company may share Your Personal Data with selected business partners solely for the purpose of offering integrated or value-added services. In such cases, You shall retain the right to opt out at any time.

v. With Other Users

In limited circumstances, where You voluntarily share information or engage in interactive components of the Service (such as forums or reviews), such information may become visible to other users. You are advised to exercise caution and discretion when sharing personal data in publicly accessible areas.

vi. With Your Consent

Where You have given explicit and informed consent, the Company may disclose Your Personal Data for other purposes not specified above. Such consent may be withdrawn at any time, without affecting the lawfulness of processing conducted prior to withdrawal.

vii. In Compliance with Legal Obligations

The Company may be legally required to disclose Personal Data in response to valid legal process, such as a court order, regulatory request, or applicable law enforcement inquiry. In such instances, only the minimum amount of data necessary for compliance shall be disclosed.

e. Retention of Your Personal Data

The Company shall retain Your Personal Data only for as long as is necessary to fulfill the specific purposes for which it was collected, as outlined in this Privacy Policy, or as required to comply with legal, regulatory, or contractual obligations.

The criteria used to determine the retention period include, but are not limited to:

- The nature and sensitivity of the Personal Data;
- The purpose(s) for which the data was collected and whether those purposes have been fulfilled;

- The existence of any ongoing legal obligations, including retention required by healthcare regulations, tax authorities, or courts of law;
- The potential need to retain data for the establishment, exercise, or defense of legal claims.

i. Retention for Legal and Regulatory Compliance

Personal Data may be retained where it is necessary to satisfy any legal or regulatory requirement, including obligations imposed by health, corporate, taxation, or financial services laws. In such cases, data shall be retained only for the period required by law and shall be subject to appropriate access controls.

ii. Retention for Service Functionality and Security

Usage Data and technical logs may be retained for a limited period to enable system diagnostics, enhance security, and monitor Service performance. Where such data is anonymized or aggregated, it may be retained for longer periods for analytical and service development purposes.

iii. Deletion and Archiving Protocols

Once the applicable retention period has expired, the Company shall ensure that Personal Data is securely deleted, anonymized, or archived, unless further retention is justified by a continuing legal obligation or lawful basis. The Company shall employ appropriate deletion mechanisms and conduct periodic reviews to ensure compliance with its retention protocols.

f. Transfer of Your Personal Data

Your Personal Data may be processed, stored, or accessed in jurisdictions outside of Your own geographic location, including locations where data protection laws may differ from those applicable in Pakistan. Where such cross-border transfers are necessary for the operation of the Service or the engagement of third-party Service Providers, the Company shall ensure that adequate safeguards are implemented to protect the integrity and confidentiality of such data.

i. User Consent and Awareness

By using the Service and submitting Your Personal Data, You expressly acknowledge and consent to the transfer, processing, and storage of Your data in jurisdictions outside Pakistan, including where data protection standards may not be equivalent to those under Pakistani law. In every instance, such transfers shall be carried out only where they are necessary for the fulfillment of the Service or are otherwise permitted by applicable law.

ii. Data Transfer Safeguards

To ensure that any transfer of Personal Data outside Pakistan maintains the same level of protection required under this Policy, the Company shall adopt one or more of the following safeguards:

- Contractual commitments requiring third parties to adopt adequate privacy and security measures, including data processing agreements;
- Secure transmission methods using encryption and controlled access protocols;
- Restriction of access to Personal Data strictly to authorized personnel and only on a need-to-know basis.

iii. Limitation on International Transfers

Personal Data shall not be transferred to any jurisdiction unless:

- It is reasonably necessary for the provision of the Service;
- There are adequate technical and organizational controls in place to safeguard the data;
- The transfer is either necessary for the fulfillment of the Service or conducted with the informed consent of the data subject.

The Company remains responsible for ensuring the security and lawful processing of Your Personal Data, regardless of the location of such processing activities.

g. Disclosure of Your Personal Data

The Company is committed to maintaining the confidentiality and integrity of Your Personal Data. Disclosure of such data shall occur only in circumstances where it is legally required, expressly authorized by You, or otherwise justified under applicable legal principles. Any such disclosure shall be limited to the minimum data necessary and subject to appropriate safeguards.

i. Business Transactions

In the event that the Company is involved in a merger, acquisition, restructuring, reorganization, asset sale, or similar corporate transaction, Your Personal Data may be transferred to the acquiring or successor entity. In such cases:

- You will be provided with prior notice of such transfer, to the extent feasible;
- The successor entity shall be bound by the terms of this Privacy Policy or a substantially similar privacy commitment;

ii. Compliance with Legal Obligations

The Company may disclose Your Personal Data where required to do so under applicable laws or in response to:

- A valid court order, legal summons, or administrative directive;
- A formal request from a regulatory or enforcement authority;
- Statutory obligations relating to public health, national security, or criminal investigations.

In each case, the Company shall ensure that:

- The request is verified and legally binding;
- Only the minimum necessary data is disclosed;

iii. Protection of Rights and Interests

Personal Data may also be disclosed where such disclosure is reasonably necessary and proportionate to:

- Protect, enforce or defend the legal rights, safety, or property of the Company, its employees, patients or its stakeholders;
- Prevent, detect, or investigate suspected fraud, abuse, or unlawful activity;
- Enforce the terms and conditions of the Service, including investigations of potential violations;
- Protect the personal safety of users or the general public.

iv. With Your Explicit Consent

The Company may disclose Your Personal Data for purposes not expressly covered by this Policy only where You have provided **explicit, informed, and voluntary consent** to such disclosure. This consent may be withdrawn at any time, without prejudice to the lawfulness of any prior processing.

h. Security of Your Personal Data

The Company recognizes the importance of protecting the confidentiality, integrity, and availability of Your Personal Data and is committed to implementing appropriate administrative, technical, and organizational measures to prevent unauthorized access, disclosure, alteration, or destruction of such data.

i. Security Safeguards and Protocols

To this end, the Company has adopted industry-recognized security practices and procedures, including but not limited to:

- **Encryption technologies** to protect data in transit and at rest;
- **Access control mechanisms** to limit data access to authorized personnel on a need-to-know basis;
- **Audit trails and logging** to monitor system access and detect anomalous activity;

- **Regular vulnerability assessments** and security updates to address emerging threats;
- **Secure data storage environments**, including the use of certified data centers and firewalls.

ii. Employee Awareness and Confidentiality

All personnel with access to Personal Data are required to sign confidentiality agreements and undergo periodic data protection and information security training to ensure compliance with internal policies and applicable laws.

iii. Third-Party Service Providers

Where third-party Service Providers are engaged for data processing activities, the Company ensures that such providers implement equivalent levels of security and are contractually obligated to handle data securely and in accordance with the Company's instructions.

iv. Limitations

While the Company takes all reasonable and proportionate steps to protect Personal Data, no method of electronic transmission or storage is completely secure. Therefore, absolute security cannot be guaranteed. The Company shall not be held liable for breaches caused by circumstances beyond its control, including but not limited to force majeure events or sophisticated cyberattacks that could not have been reasonably foreseen or prevented.

v. Reporting of Security Incidents

In the event of a data breach or security incident affecting Your Personal Data, the Company will:

- Promptly assess the nature and scope of the breach;
- Take immediate corrective and containment measures;
- Where required by applicable law, notify affected users and/or regulatory authorities in a timely manner.

i. Children's Privacy

The Company is committed to protecting the privacy and safety of minors and recognizes the special considerations involved in processing personal data belonging to children.

i. Intended Audience

The Service is not designed for or directed at children under the age of **eighteen (18) years of age or twenty one (21) years of age for those who have a guardian appointed by a court (the "Age of Majority")**. The Company does not knowingly collect, use, or disclose

Personal Data from individuals below this age threshold without verified parental or legal guardian consent.

ii. Parental or Guardian Consent

If it becomes known to the Company that a child under the Age of Majority has submitted Personal Data without the prior, verifiable consent of a parent or legal guardian:

- The Company shall take prompt steps to delete such data from its records;
- Access to or use of the Service by such a minor may be restricted or disabled, as appropriate;
- Where feasible, the parent or guardian shall be notified.

iii. Educational or Health Use Cases

Where the Service is accessed on behalf of a minor for legitimate purposes—such as the management of medical appointments or health records—the Company may process the child’s data only through the authenticated account of the parent or legal guardian.

iv. Guidance to Parents and Guardians

Parents and legal guardians are encouraged to monitor and guide their children's use of electronic applications and to instruct minors never to share personal information without supervision.

j. Links to Other Websites

The Service may, from time to time, contain links to external websites, third-party platforms, or online services that are not owned, operated, or controlled by the Company. These links are provided solely for user convenience or informational purposes.

i. No Endorsement or Control

The inclusion of any third-party link within the Service does not constitute an endorsement, recommendation, or warranty of the content, accuracy, reliability, or privacy practices of such external sites. The Company exercises no control over and bears no responsibility for the availability, operations, or policies of any third-party website or service.

ii. Independent Privacy Policies

Users are strongly advised to carefully review the **privacy policies, terms of use, and security practices** of any third-party website they choose to visit. Such websites may have their own policies and procedures governing the collection and use of personal data, which may differ from those of the Company and may not offer equivalent protections.

iii. No Liability

The Company shall not be held liable for any loss, damage, unauthorized disclosure, or inconvenience arising from a user's reliance on or interaction with external websites accessed through links embedded in the Service. Any data shared by You with a third party shall be governed solely by that party's privacy practices.

k. Changes to this Privacy Policy

The Company reserves the right to review, revise, or amend this Privacy Policy at its sole discretion to reflect:

- Changes in applicable laws or regulatory requirements;
- Updates to the Service or internal data processing practices;
- Evolving user expectations or feedback;
- Technological advancements or changes in operational models.

i. Notice of Changes

Where material changes are made that may affect Your rights or the manner in which Your Personal Data is processed, the Company shall provide prior notice by:

- Posting a clear and conspicuous notification within the Application;
- Updating the "Last Updated" date at the top of the Policy;
- Where appropriate, providing direct notice to registered users via email or in-app notification.

ii. User Responsibility

You are advised to review this Privacy Policy periodically to remain informed of any updates. Continued use of the Service after any changes have been posted shall constitute Your acceptance of the revised Policy.

If You do not agree to the amended terms, you must immediately discontinue use of the Service and may exercise Your rights regarding data access or deletion as provided herein.

The Company is committed to addressing all inquiries in a timely and transparent manner, and where appropriate, will cooperate to ensure full compliance with data protection obligations.

a. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or the handling of your data, you may contact us through any of the following:

- **Email:** info@shifa.com.pk
- **Website:** <https://www.shifa.com.pk>
- **Phone:** +92-51-8464646