

Hospital Privacy Policy for Hospital Online Payments

1. Introduction

This Privacy Policy outlines how Advanced Veterinary Care Foundation ("we," "us," or "our") collects, uses, discloses, and safeguards your personal information when you utilize our online payment gateway for medical services through our website or dedicated payment portal. We are committed to protecting your privacy and ensuring the highest standards of data security, in compliance with applicable laws including the Information Technology Act, 2000 (as amended), the Digital Personal Data Protection Act, 2023 (DPDP Act), and Payment Card Industry Data Security Standard (PCI DSS) Level 1 requirements. By accessing or using the payment gateway, you consent to the practices described herein. If you do not agree, please refrain from using the service.

2. Information We Collect:

We collect only the minimum personal information necessary to process payments, verify identity, and deliver services.

- This includes: **Patient and Contact Details:** Full name, residential address, email address, phone number, and emergency contacts (if provided).
- **Medical and Service Information:** Medical record number, date of admission/discharge, treatment/service details, and any notes relevant to billing.
- **Payment Information:** Credit/debit card details (e.g., card number, expiry date, CVV), bank account details (e.g., account number, IFSC code), UPI ID, or other payment instrument identifiers. **Important:** We do not request or store full sensitive payment details post-transaction; only tokenized references are retained where necessary.
- **Voluntary Information:** Any additional details you provide, such as special billing instructions.
- We do not collect sensitive personal data (e.g., biometric information or full health records) unless explicitly required for service delivery and with your affirmative consent.

3. How we use your Information:

Your information is used solely for legitimate purposes and in a manner that respects your privacy. Specific uses include:

- **Payment Processing and Service Delivery:** To authorize, process, and confirm payments; schedule or confirm appointments/admissions; and provide veterinary medical services.
- **Billing and Financial Management:** Generating invoices, sending payment reminders, refunds, or status updates via email/SMS (with opt-out options).
- **Fraud Prevention and Risk Management:** Analyzing transaction patterns to detect and prevent unauthorized activity, in line with PCI DSS guidelines.

- **Legal and Regulatory Compliance:** Responding to lawful requests from government authorities, courts, or regulators; maintaining audit trails; and fulfilling tax/reporting obligations.
- **Service Improvement:** Anonymizing data for internal analytics to enhance payment gateway usability, security, and user experience (e.g., faster checkout processes).
- **Internal Record-Keeping:** Retaining records for a minimum of 7 years (as per statutory requirements) or until the purpose is fulfilled, after which data is securely deleted or anonymized. We do not use your data for marketing, profiling, or automated decision-making without explicit consent. Any secondary uses require your informed opt-in.

4. Data Security Measures

- Protecting your information is our top priority. We implement robust, multi-layered security protocols to safeguard data against unauthorized access, loss, alteration, or disclosure
- **Encryption Standards:** All data in transit is protected using TLS 1.3 (successor to SSL) [DB1.1]encryption. Payment data is tokenized immediately upon entry, ensuring we never store raw card details.
- **PCI DSS Compliance:** Our payment gateway is certified PCI DSS Level 1 compliant, with regular third-party audits and vulnerability assessments conducted quarterly.
- Access to payment data is restricted to authorized personnel only. We do not store sensitive payment details (such as full card numbers) after transaction completion.
- **Network Security:** Firewalls, and endpoint protection prevent breaches. We conduct annual penetration testing by certified ethical hackers.

5. Disclosure of Information

We adhere to a strict "no sharing" principle and disclose information only when absolutely necessary and under stringent controls:

We do not share your personal or payment information with third parties except:

- With payment gateway providers and financial institutions to complete transactions
- As required by law, regulation, court order, or law enforcement agencies
- With contracted service providers under obligation of confidentiality

6. Rights and Choices

You may request access or correction to your personal data by contacting frontoffice@sahmumbai.com. You may request details about the information stored and request its deletion as per legal requirements.

7. Cookies and Tracking

Our payment gateway uses essential cookies for functionality (e.g., maintaining secure sessions) and security (e.g., fraud detection). We may use cookies for session management and to enhance the website experience, but do not track users for marketing purposes.

8. Updates to Policy

This policy may be updated from time to time. Changes will be posted on our website, and your continued use of the payment portal constitutes acceptance of the updated policy.

9. Contact Information

For privacy-related queries or concerns, please contact: frontoffice@sahmumbai.com / 022-6538 3538

