the Virtual Doctors: Data Protection Policy

Effective Date: June 2026

Virtual Doctors ("Virtual Doctors", "VDrs", "we", "our", or "us") is committed to protecting your privacy and ensuring transparency in how we collect, use, and safeguard your personal data.

This Privacy Policy explains how your information is handled when you use our mobile application, website, and telemedicine services.

For the purposes of applicable data protection laws (including UK GDPR and EU GDPR), Virtual Doctors acts as the **Data Controller**.

---

1. Information We Collect

1.1 Personal Information You Provide

We may collect:

- Full name
- Email address
- Phone number
- Date of birth
- Account login credentials
- Communication content (messages, consultation notes)

This information is **required** to create an account and provide healthcare services. If you choose not to provide this information, you may not be able to use core app features.

1.2 Health and Medical Information (Sensitive Data)

We collect health-related data necessary for care, including:

- Medical history
- Symptoms and diagnoses
- Consultation records
- Treatment notes and referrals

This data is **required** to provide medical consultations and healthcare services.

We **do not use health data for advertising, profiling, or marketing purposes**.

1.3 Device and Technical Information

Collected automatically:

- IP address
- Device type and operating system
- App version
- Device identifiers
- Log data (crash reports, diagnostics, usage data)

Required vs Optional

- Some technical data is **automatically collected (required)** for app functionality and security
- Some analytics data may be **optional**, depending on device settings and configurations

---

1.4 Communications Data

- Messages between users and healthcare professionals
- Customer support interactions

Required to provide consultation and support services.

1.5 Volunteer and Donor Information

- Contact details
- Engagement history

Optional, used only if you choose to engage as a volunteer or donor.

---

2. How We Use Your Information

We use your data to:

- Provide medical consultations and healthcare services
- Create and manage user accounts
- Enable secure communication with healthcare professionals
- Improve app performance and reliability
- Monitor and diagnose technical issues
- Respond to enquiries and support requests
- Ensure security, fraud prevention, and legal compliance

We **do not use personal or health data for advertising or targeted marketing**.

---

3. Google Play Data Safety Alignment

In accordance with Google Play requirements, we disclose:

Data Collected

We collect:

- Personal information (e.g., name, contact details)
- Health data (sensitive data)
- App activity and performance data

The app does not use a specific unique identifier for each device.

Data Sharing

- Data is shared **only with healthcare providers and essential service providers**
- Data processed via Firebase is used only for:
    - Analytics
    - Crash reporting
    - Performance monitoring

We **do not share data for advertising or cross-app tracking**
We **do not sell user data**

Data Collection Purpose

- Healthcare delivery
- Application functionality
- Security and fraud prevention
- Service improvement
- Data processing activities are set out at the end of the document

---

4. Third-Party Services

We use trusted third-party providers such as:

- Cloud hosting providers
- Secure telemedicine platforms

These services may process:

- Device information
- App usage data
- Crash logs

This data is used strictly for:

- Service functionality
- Security
- Performance improvement

It is **not used for advertising, profiling, or third-party marketing**.

---

5. App Permissions

We request only the permissions necessary for core features:

Camera

- Used for video consultations and medical image capture
- **Optional**, but required for video consultations

Microphone

- Used for audio communication during consultations
- **Optional**, but required for live consultations

Storage

- Used to store and retrieve medical documents securely
- Limited to app-related files only

Internet Access

- Required for app functionality and communication

If permissions are denied, some features may not function properly.

---

6. Data Sharing

We may share data only:

- With healthcare professionals (acting as independent controllers for care delivery)

- Cloud hosting providers (data processors under contract)
- When required by law or legal obligation

We **do not sell personal data**
We **do not share data for advertising purposes**

---

7. International Data Transfers

We rely on Standard Contractual Clauses (SCCs) and equivalent safeguards for international transfers.

- Data may be processed globally with safeguards:

- Standard Contractual Clauses (SCCs)
- Equivalent legal protections and Data processing agreements with providers

---

8. Data Security

We implement safeguards including:

- Data is encrypted in transit and at rest using industry-standard methods
- Access controls and authentication
- Monitoring and audit logging
- We do not share personal or sensitive user data with third parties for advertising, marketing, or monetization purposes.
- Admin actions are logged and error logs are maintained

---

9. Data Retention

We retain data only as long as necessary:

Google Analytics, GA4 separates data into two types with different retention periods:

• Event data (individual interactions such as page views, button clicks, scrolling) is retained for 2 months
• User data (user properties such as age, location, logged in/out status) is retained for 14 months

---

10. Your Rights

You have the right to:

- Access your data
- Correct inaccuracies
- Request deletion
- Restrict or object to processing
- Withdraw consent
- Request data portability
- Lodge complaints with authorities

---

11. Account and Data Deletion

You can request deletion by writing to:

- Doctors can request deletion of the account by sending a Zendesk request from within the app.
- Requests are processed within 14 days
- Deletion does removes all personally identifiable information (PII) for that user. The user record itself remains in the database but with the name and email replaced with placeholder values (e.g. "(deleted)").

12. Children's Privacy

We do not allow independent accounts for users under 18. Data relating to minors is processed exclusively via authorised guardians or licensed healthcare professionals with appropriate consent

.

13. Analytics and Tracking

We use limited analytics tools to:

- Monitor performance
- Identify issues
- Improve user experience

We **do not track users across other apps or services**
We **do not use analytics for advertising purposes**

14. Automated Decision-Making and Profiling

Important Transparency Statement

- We **do not use automated decision-making or profiling** to make medical, legal, or significant decisions about users
- Healthcare decisions are made by **qualified human healthcare professionals**
- Technology is used only to support service delivery (e.g., communication, record management)

15. Legal Basis and Consent

We process data based on:

- User consent
- Provision of healthcare services
- Legal obligations

Consent Collection

- During account registration
- When submitting health information

Withdrawing Consent

You can withdraw consent:

- Via app settings (where available)
- By contacting: **privacy@virtualdoctors.org**

---

16. Changes to This Policy

We may update this policy periodically.
Significant changes will be communicated within the app or by other means.

---

17. Contact Information

✉ info@virtualdoctors.org
+44 1273 963887

www.virtualdoctors.org

the Virtual Doctors Registered Office: Sussex Innovation Centre University of Sussex, Falmer, Brighton, BN1 9SB. Registered Charity No: 1129924 the Virtual Doctors Registered Company the Virtual Doctors Ltd Number 06848059 (England and Wales). Administrative Office Tel: 01273 454755

This privacy policy is publicly accessible at: https://virtualdoctors.org/privacy-policy-2/

18. Data Processing Activities

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Type of recipient to whom Personal Data is transferred
Date of birth.	Patient	Activities relating to the provision of medical services, including obtaining, recording or storing the Personal Data, carrying out activities based on the Personal Data such as disclosing it to health care professionals and using it to suggest treatment plans and diagnose medical conditions, recording the Personal Data and destroying it when appropriate.	Providing diagnostic and treatment advice to rural health workers to reduce unnecessary referrals and advance their medical skills and knowledge.	Volunteer health care professionals in the UK and Zambia and VDrs employees.
Special Categories of Personal Data, including data relating to health conditions, diagnosis, treatment and medical history.	Patient	See above.	See above.	See above.
Personal Data, such as name, address, date of birth, phone number, CV and bank details.	VDrs employee / volunteer	Obtaining, recording and storing the Personal Data.	Staff administration, remuneration and records.	VDrs employees, including managers and those with HR responsibility.
Special Categories of Personal Data, including health records such as medical reports, self certification forms, documentation required to establish rights to statutory sick pay and other sickness benefits or leaves of absence and criminal offence records.	VDrs employee	Obtaining, recording and storing the Personal Data.	Staff administration, remuneration and records.	VDrs employees, including managers and those with HR responsibility.

Personal Data, such as name, address, date of birth, email address, phone number and bank details.	Donors (including trustees, grant makers, individual and corporate donors)	Obtaining, recording and storing the Personal Data.	Administrative purposes; donation recording (including confirmation and receipts); contact purposes; marketing purposes (where individual has opted-in).	VDrs employees and managers.
Personal Data, such as name, address, Internet Protocol (IP) address. Other information collected automatically, including technical information about your browser type and version, time zone setting, browser plug-in types and versions, operating system and platform.	Website user	Obtaining, recording and storing the Personal Data.	Administration purposes; website functionality/improvement (including but not limited to troubleshooting, testing, statistics).	VDrs employees and managers.