Privacy Notice

Last updated: 11 February 2026

Introduction

This privacy notice explains how **Vulpis Health Ltd** ("Vulpis Health", "we", "us", "our") collects, uses, stores, and shares your personal data when you use the **Vulpis Health Network**, which includes:

- Our mobile applications;
- Our websites and web applications; and
- Associated online services, booking systems, and review platforms.

The Vulpis Health Network is not intended to be accessed by children, but we recognise that adult carers may use it on behalf of children. As a result, we communicate in a way intended to be understood by adults, but we protect the personal data that we process with the enhanced care required when processing the personal data of minors.

This notice contains information for both patients and healthcare professionals. The information we process about these two groups is different. The sections are labelled "Patients" or "Healthcare Professionals" for easy reference. You do not need to review sections that do not apply to you

If you have difficulty understanding this notice, please contact us via the details just below for assistance.

1. Important Information and Who We Are

Controller – Vulpis Health Ltd, at Companies House with number 17029582.

Contact details:

- **Data Protection Officer (DPO)** – hello@VulpisHealth.com
- **General enquiries** – hello@VulpisHealth.com
- **Postal address** – Vulpis Health Ltd, 8 Oak Gardens, Edgware, London, Ha8 5LF

Supervisory authority – In the UK, you can contact the Information Commissioner's Office (ICO). If you live in the EU, you may contact your local supervisory authority.

The Vulpis Health Network may, from time to time, contain links to and from the websites of third parties. Please note that these websites (and any services accessible through them) are controlled by those third parties and are not covered by this privacy notice. You should review their own privacy notices to understand how they use your personal data before you submit any personal data to these websites or use these services.

We keep our privacy notice under regular review.

This version was last updated on the date at the top of the page. It may change and, if it does, those changes will be posted on this page and notified to you when you next visit the Vulpis Health Network.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during our relationship with you.

2. The Data We Collect About You

We collect and process different categories of personal data for patients and healthcare providers.

2.1 Patients

- **Identity Data:** Name, date of birth, gender.
- **Contact Data:** Address, email, phone number.
- **Appointment Data:** Bookings, provider names, dates, times, clinic location.
- **Health Data (special category):** Health conditions, treatments, procedures, other medical details required to arrange care.
- **Review Data:** Feedback, ratings, written comments, appointment verification details (e.g., date of visit).
- **Verification Data:** SMS, WhatsApp, or email verification codes.
- **Payment Data:** Tokenised payment details, transaction history.
- **Technical Data:** Device identifiers, IP address, browser type, operating system, app version, usage logs, cookies.
- **Marketing & Communication Preferences:** Opt-in/opt-out records, engagement with messages.
- **Location Data:** If enabled in app settings.

2.2 Healthcare Providers

- **Identity Data:** Name, title, gender, professional registration details (GMC, GDC, etc.).
- **Contact Data:** Work address, email, phone number.
- **Professional Profile Data:** Specialisations, qualifications, endorsements, peer connections, practice information.
- **Review Data:** Feedback from verified patients.
- **Referral Data:** Information from referring GPs or colleagues.
- **Technical Data:** Device identifiers, IP address, browser type, usage logs, cookies.
- **Marketing & Communication Preferences:** Opt-in/opt-out records, engagement with messages.

3. How We Collect Your Personal Data

- **Directly from you** – registration, bookings, feedback forms, enquiries, profile creation.
- **Automatically** – cookies, device analytics, log files, error tracking.

- **From healthcare providers** – when they input appointment or review verification details.
- **From verification systems** – SMS gateway, WhatsApp Business API, email verification.
- **From analytics tools** – anonymised usage data.

4. How We Use Your Personal Data (and the Lawful Basis or Bases for Doing So)

A table setting out more detail on these uses is in Annex A

Patients – We use your personal data to:

- Book and manage appointments (Contract).
- Process health data to arrange and deliver healthcare (Art. 9(2)(h) GDPR for healthcare purposes, in conjunction with Schedule 1, Part 1(2) of the DPA 2018) and, where relevant, with explicit consent (Art. 9(2)(a) GDPR).
- Verify reviews (Legitimate interests – to prevent fraud and protect platform integrity; Contract).
- Publish patient reviews (Legitimate interests – informing other patients; plus explicit consent / manifestly made public by data subject (if health details included)).
- Send appointment confirmations, reminders, and follow-ups (Contract).
- Improve our services (Legitimate interests – service enhancement, bug fixing).
- Send marketing communications (Legitimate interests for existing patients under the PECR soft opt-in rule; otherwise Consent).

Healthcare Providers – We use your personal data to:

- Maintain and publish your professional profile (Contract, Legitimate interests).
- Display verified patient reviews (Legitimate interests).
- Facilitate peer networking and endorsements (Consent, Legitimate interests).
- Send service updates (Legitimate interests).
- Send marketing (Legitimate interests for existing relationships under PECR; otherwise Consent).

Automated Decision-Making (including AI)

We do not make decisions based solely on automated processing or profiling that produce legal effects concerning you (or have similarly significant effects).

5. Sharing Your Information

We may share your personal information but will only do so when this is fair and lawful. We will not share your information with any third parties for the purposes of direct marketing.

We use third parties who provide elements of services for us. We have contracts in place with these service providers. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

In some circumstances we are legally obliged to share information. For example under a court order or to a regulator or law enforcement when required to do so.

We may share your information with our professional advisers (for example our lawyers) when it is necessary for them to perform their professional duties.

We might share your information with prospective purchasers of our business.

Appointment Requests and Sharing Your Information with Healthcare Providers

When you submit an appointment request through Vulpis Health, the information you provide – which may include health information – will be shared directly with the healthcare professional, clinic, or hospital you have chosen. We do this with your explicit consent and in the public interest of managing health and social care. Once your request has been transmitted, the healthcare provider becomes the controller of your information and is responsible for how they handle it. We recommend you review their own privacy notice. Vulpis Health will retain a record of your request to resolve queries and for legal and regulatory purposes – details on how long that retention is for are found in the table in Annex A below.

6. International Transfers

Where we transfer your personal data outside the UK or EEA, we ensure appropriate safeguards are in place in accordance with GDPR, including:

- Adequacy decisions, where applicable;
- Standard Contractual Clauses;
- Additional contractual and technical safeguards. Contact the DPO for details.

7. Data Retention

Specific retention periods for each category of personal data are set out in the table in Annex A. These periods are based on legal requirements, regulatory guidance, and legitimate business needs.

Data Category	**Retention**
Patient medical records	8 years (adults) / until age 25 (children)
Verified reviews	Indefinite (anonymised)
Unverified reviews	Indefinite (anonymised)
Financial records	7 years
Marketing preferences	Until withdrawn + 3 years suppression
Technical logs	90 days
Provider profiles	Active account + 7 years

8. Your Legal Rights

Under UK and EU data protection laws, you have the following rights which can be exercised by contacting our DPO at hello@VulpisHealth.com. We will respond to your request within one calendar month:

- Access your data;
- Correct inaccuracies;
- Request deletion;
- Restrict processing;
- Object to processing (including marketing);
- Request data portability;
- Withdraw consent.

Special considerations:

- Anonymous reviews cannot be deleted after verification.
- Some provider and patient data must be retained for regulatory compliance.

9. Cookies

We use cookies (small files which remember a user's electronic device) to help improve the Vulpis Health Network in a variety of different ways.

See our **Cookie Policy** for full details of the cookies we use and how to manage them.

To keep this notice easier to use and navigate and minimise updates, we do not duplicate all the information on our Cookie Policy in this notice.

10. Contact

-
    - **DPO:** hello@VulpisHealth.com
    - **General enquiries:** hello@Vulpis Health.com
- **Postal address :** Vulpis Health Ltd, 8 Oak gardens, Edgware, London, HA8 5LF

Annex A – Purposes of Processing

Where we rely on Legitimate Interests, we carry out a balancing test considering your interests, fundamental rights and freedoms. This is documented separately.

A1 – Patients

Purpose / Activity	Categories of Personal Data	Special Category Data	Lawful Basis (UK/EU GDPR)	Additional Condition for Special Category Data	Retention Period	Rationale for Retention
Appointment booking and management	Identity, Contact, Appointment Data	Health Data (conditions, treatments)	Performance of a contract – necessary to arrange your appointment	Art. 9(2)(h) – healthcare purposes	8 years (adults) / until age 25 (children)	NHS requirements for clinical records

Healthcare service delivery	Identity, Contact, Appointment Data	Health Data	Performance of a contract – to deliver the healthcare services you request	Art. 9(2)(h)	As above	Ensures continuity of care and regulatory compliance
Review verification	Identity, Contact, Appointment Data, Verification Data	Health Data (only to confirm attendance)	Legitimate interests – to prevent fraudulent reviews and ensure platform integrity; Performance of a contract	Art. 9(2)(h)	Verification data deleted after 90 days; verified reviews retained indefinitely (fully anonymised in accordance with ICO guidance)	Fraud prevention, protecting service trust
Publishing patient reviews	Review Data	Health Data (if included in review text)	Legitimate interests – to inform other patients and support provider choice	Explicit consent (Art. 9(2)(a)) / Manifestly made public by the data subject (Art 9(2)(e))	Indefinite (anonymised)	Supports transparency and informed decision-making
Patient communications (service updates, reminders)	Identity, Contact, Appointment Data	None	Performance of a contract – to send essential updates	N/A	Account lifetime	To maintain service and appointment accuracy
Marketing communications	Identity, Contact, Marketing Preferences	None	Legitimate interests with soft opt-in under PECR (for existing patients who have not opted out); Explicit consent required for new patients and non-patients	N/A	Until withdrawn + 3 years suppression	Ensures suppression list accuracy
Fraud prevention & security	Identity, Contact, Technical Data, Verification Data	None	Legitimate interests – to secure systems and prevent unauthorised use	N/A	90 days for logs	Security monitoring and incident detection
Platform analytics	Technical Data, Usage Data, Cookies	None	Legitimate interests – to improve services	N/A	26 months	Google Analytics default retention for anonymised data
Personalisation	Technical Data, Usage Data, Location Data	None	Consent – only applied if you enable this feature	N/A	Account lifetime	Improves user experience
Legal compliance	All categories as necessary	Health Data (if relevant)	Legal obligation – to comply with statutory requirements	Art. 9(2)(h) or Art. 9(2)(f) – legal claims	As required by law	Regulatory or legal defence purposes

A2 – Healthcare Providers

Purpose / Activity	Categories of Personal Data	Special Category Data	Lawful Basis (UK/EU GDPR)	Additional Condition for Special Category Data	Retention Period	Rationale for Retention
Profile creation and maintenance	Identity, Contact, Professional Profile Data	None	Performance of a contract – to display your services	N/A	Active account + 7 years	Maintain records for regulatory and contractual compliance

Publishing patient reviews	Review Data (about provider)	Health Data (in review context)	Legitimate interests – to inform patients about your services	Explicit consent/publication (Art. 9(2)(a)/(e)) from patient	Indefinite (following full anonymisation process with regular reviews)	Supports transparency and informed choice
Peer networking & endorsements	Identity, Professional Profile Data, Endorsements	None	Consent – if you choose to participate; Legitimate interests – to build professional connections	N/A	Until withdrawn	Professional relationship building
Communications (service updates, policy changes)	Identity, Contact	None	Legitimate interests – to keep you informed about operational matters	N/A	Account lifetime	Service continuity
Marketing communications	Identity, Contact, Marketing Preferences	None	Legitimate interests (soft opt-in under PECR for existing relationships); Consent for others	N/A	Until withdrawn + 3 years suppression	Marketing list management
Fraud prevention & security	Identity, Contact, Technical Data	None	Legitimate interests – to protect accounts and platform security	N/A	90 days for logs	Security monitoring
Platform analytics	Technical Data, Usage Data, Cookies	None	Legitimate interests – to improve provider-facing features	N/A	26 months	Service performance analysis
Legal compliance	All categories as necessary	None	Legal obligation – to meet statutory and regulatory requirements	N/A	As required by law	Compliance with healthcare and data protection laws