

HealthFort Privacy Policy

Version 1.4 | Effective [date of publication]

This policy explains how HEALTHFORT LTD uses personal data in the HealthFort personal health-record service, including health records, family profiles, consultation recordings and AI processing.

HealthFort handles information that can be exceptionally private. We use it to provide the service the user requests, protect the service, and meet our legal duties. We do not sell personal data. The terms of the cloud AI services we use state that HealthFort content is not used to train their foundation models without our permission, and we have not given that permission.

1 Who we are

HEALTHFORT LTD is a company registered in England and Wales under company number 17386404. Our registered office is 483 Green Lanes, London, England, N13 4FG.

For personal accounts, HEALTHFORT LTD is normally the controller of the personal data described in this policy. Contact us at info@healthfort.uk or at the postal address above. Our postal address is a mail-handling address operated by UK Postbox Limited, which receives and may scan post on our behalf. Please do not send medical records or other health documents by post; email us first and we will arrange a secure way to send them.

2 When a clinic is involved

Our role depends on how HealthFort is provided:

- If you create and use a personal HealthFort account directly, HEALTHFORT LTD decides why and how the service processes your data and acts as controller.
- If a clinic supplies patient data to HealthFort or uses HealthFort to provide its own service, the clinic will normally be the controller and HEALTHFORT LTD will act as its processor under a separate data-processing agreement.
- We may remain a separate controller for limited account administration, billing, security, legal compliance and service communications. The clinic's privacy notice should explain its own purposes, legal bases and retention.
- A clinician who receives a copy of information that you share may become an independent controller of that copy under professional and healthcare record-keeping duties.

3 The information we process

Category	Examples
Account and identity	Name, email address, date of birth, contact details, account identifiers, authentication records and age confirmation.
Health and genetic information	Medical letters, prescriptions, laboratory results, conditions, allergies, medicines, vaccinations, procedures, DICOM images and reports, VCF files, family history, symptoms and other records you upload or enter.

Category	Examples
Derived service data	Extracted text and values, structured fields, source references, summaries, transcripts, appointment packs, search indexes, embeddings used to retrieve your own records, and corrections or notes.
Recordings	Consultation audio, participant information, transcript, descriptive summary and clinician approval status.
Family and dependant profiles	Profile details, records, relationship to the account holder, permission or authority evidence, and records of any objection or rights request.
Sharing and clinician access	Selected records, recipient details, access code or link, expiry, access and revocation logs, and any clinician account details.
Payment and plan	Plan, subscription status, amounts paid, transaction and invoice references and limited payment-method details, such as card type and last four digits. You enter full card details on Stripe's payment page; HealthFort does not receive or store full card numbers or security codes.
Communications and consent	Support messages, complaints, feedback, privacy requests, the consent wording accepted, date, time and withdrawal records, marketing preferences, unsubscribe records and email delivery records (for example sent, delivered or bounced).
Technical and security	IP address, device and browser information, session, audit and access logs, error data, security alerts and usage records needed to operate and protect the service.

A health record can incidentally reveal other special-category data, such as racial or ethnic origin, religious or philosophical beliefs, sex life, sexual orientation, disability, biometric information or political opinions. We treat that information with the same protections as the underlying record.

We do not use consultation audio for biometric identification or create a voiceprint unless a separate feature is introduced with specific notice, assessment and legal basis.

4 Where the information comes from

- you, when you create an account, upload a record, make a recording, add a note, correct an extraction or contact us;
- an authorised family member, representative, clinician or clinic;
- our payment provider, Stripe, which tells us whether a payment succeeded or failed and provides subscription, invoice and limited payment-method details;
- a record provider or connected service that you instruct to send information;
- the documents and recordings themselves, when HealthFort extracts or derives structured information; and
- your device and our systems, when they create access, security and operational records.

5 Why we use information and our legal bases

UK data-protection law requires an Article 6 lawful basis and, for special-category data, a separate Article 9 condition. The basis depends on the purpose and on whether HealthFort acts for an individual or for a clinic.

Purpose	Article 6 basis	Special-category condition
Create and administer a personal account; store, organise, extract and present records; provide search, sharing, recordings and requested exports	Necessary to perform our contract with you (Article 6(1)(b))	We first obtain explicit consent for the stated HealthFort service purposes (Article 9(2)(a))
Process clinic-supplied patient data on the clinic's instructions	Determined by the clinic; HealthFort processes under contract as processor	Determined and documented by the clinic, which may rely on healthcare or another applicable condition
Ensure the security of network and information systems; authenticate users; prevent unauthorised access and investigate incidents	Our and users' legitimate interests in operating a secure service (Article 6(1)(f)); legal obligation where applicable	Only where necessary and with an applicable Article 9 condition; we minimise access to health content
Take payments and manage subscriptions, including retrying failed renewals; billing, accounting, tax and contractual records	Contract (Article 6(1)(b)), legal obligation (Article 6(1)(c)) and our legitimate interests in preventing payment fraud (Article 6(1)(f))	Not required. We do not send health information to our payment provider.
Respond to rights requests, complaints, regulators, courts and lawful demands	Legal obligation (Article 6(1)(c)) and legitimate interests in establishing or defending legal claims (Article 6(1)(f))	Legal claims (Article 9(2)(f)) or another condition required by law
Send optional marketing	Consent (Article 6(1)(a)) and PECR where applicable	Not used. We do not use health or genetic information to decide who receives marketing or what it says.

We do not rely on a general claim of "service improvement" to reuse identifiable health records. Testing and improvement use synthetic, de-identified or aggregated material where possible. Any future research, clinical-trial matching or materially different use of identifiable health data will have a separate notice and, where required, separate explicit consent.

6 Explicit consent and withdrawal

For a direct consumer account, we ask for explicit consent before HealthFort processes health, genetic or other special-category data for document recognition, extraction, organisation, summaries, record search, sharing and any enabled recording feature.

You can withdraw that consent at any time through the account where available or by contacting us. Withdrawal does not make earlier lawful processing unlawful, but we will stop the consent-based processing. Because the service cannot operate without processing the records, withdrawal will normally require us to close the affected profile and begin deletion, subject to data we must retain by law or for legal claims.

Where a clinic is the controller, direct requests to the clinic as well as to us. We will assist the clinic as required by our agreement.

7 How artificial intelligence is used

AI is central to HealthFort's recognition, transcription, extraction, retrieval and plain-language description features. We send only the information needed for the selected feature to an approved processor and use generated identifiers rather than revealing a user-supplied filename where practicable.

- Microsoft processes prompts, document text, images, audio and outputs for HealthFort AI features through Microsoft Azure and Microsoft Foundry, acting as our processor under Microsoft's Products and Services Data Protection Addendum. Identifiable patient data is sent only to deployments configured for Microsoft's EU Data Zone; within that zone a request may be processed in any EU Member State. Microsoft states that prompts and outputs are not used to train its base models, or to train generative AI foundation models without our permission, which we have not given. Microsoft's abuse monitoring is enabled for our service: where Microsoft's automated systems flag possible misuse, prompts and outputs may be stored by Microsoft for a limited period and reviewed by authorised Microsoft staff.
- Google Cloud Vertex AI may process document content for HealthFort features through an EU endpoint that we select, including records in a child profile that an adult account holder uploads and manages. HealthFort is not directed to, and may not be used by, anyone under 18. Under Google's terms, data we derive through our use of Google Cloud is treated as our customer data, and Google's service terms restrict it from using that data to train or fine-tune its AI models without our permission, which we have not given. We use Google's generative AI services only to help organise and describe records for your information, not for clinical decision-making or as a substitute for professional medical advice.
- We do not use consumer AI accounts, Google AI Studio, a Gemini Developer API key or an unapproved fallback route for identifiable patient records.

AI providers may perform automated safety or abuse monitoring and may retain flagged content for the period their terms allow. Where practicable we use features that do not store prompts or outputs, but because abuse monitoring is enabled, flagged content may still be stored and reviewed by the provider as described above. HealthFort does not make decisions about you based solely on automated processing that have legal or similarly significant effects. Our payment provider's automated fraud checks are described in section 8.

8 Who receives information

We disclose personal data only where needed for the purposes in this policy. Not every processor receives every category of data.

Recipient or category	Purpose and position
Hetzner Online GmbH	Hosts the HealthFort application, databases and uploaded files on a server in Hetzner's Falkenstein data centre in Germany, and stores our encrypted backups in Hetzner storage within the EU/EEA, as our processor. Hetzner's terms limit processing to the EU/EEA for EU server locations. Hetzner provides the data centre, hardware and network; HealthFort configures and secures the server and encrypts stored data and backups.

Recipient or category	Purpose and position
Microsoft group companies and Microsoft's subprocessors	Microsoft Azure and Microsoft Foundry AI processing, related storage, security and support, as our processor under Microsoft's Products and Services Data Protection Addendum. Identifiable patient data is sent only to deployments in Microsoft's EU Data Zone. Microsoft engages subprocessors under a general authorisation in its terms and publishes a list on its website. Microsoft acts as an independent controller for limited business operations, such as billing, account management and financial reporting, using aggregated or statistical information and without accessing the content of our data.
Google Cloud EMEA Limited (Ireland), other Google group companies and Google's subprocessors	Vertex AI processing of document content for AI features, as our processor under the Google Cloud Data Processing Addendum and Google's service-specific terms. Google uses group companies and third-party subprocessors listed on its website and must notify us before adding a new one.
UK Postbox Limited, UK	Provides our registered-office address and mail handling as our processor. It receives post addressed to us, may scan and store it, and forwards it to us. It processes data mainly in the UK and EEA.
Email and business-software providers	Receive and store emails you send us, including to info@healthfort.uk, and our replies. They act as our processors.
Sendinblue SAS (trading as Brevo), France	Sends account emails, such as sign-up and security codes, and marketing emails if you have opted in. Brevo receives your name, email address and the emails we send you, and records delivery information. We do not include health information in emails or give it to Brevo. Brevo acts as our processor and also uses limited data as a separate controller for its own purposes, such as security and spam prevention, as described in its privacy policy. Brevo's main hosting is in the EU, but some of its subprocessors and group companies, including in the United States and India, may access data.
Stripe and its group companies, including Stripe, LLC in the United States	Provides our payment page, subscription billing, invoices and receipts. When you pay, Stripe collects your name, email address, payment details, the billing details the payment page asks for, and information about your device and browser, including IP address. We also give Stripe the plan, price and transaction details. We do not send health information to Stripe. Stripe automatically assesses payments for fraud risk and may decline a payment as a result. Stripe acts as our processor when it takes payments on our instructions, and as a separate controller when it uses this information for its own purposes, including preventing fraud and financial loss, working with banks and payment networks, meeting its legal and regulatory obligations, and improving its products, as explained in Stripe's privacy policy.
Clinics, clinicians and people you choose	Receive only the records or outputs you direct us to share, or process data under a clinic arrangement.

Recipient or category	Purpose and position
Professional advisers, insurers, regulators and authorities	Only where reasonably necessary for advice, insurance, legal claims, safeguarding, compliance or a lawful request.
A buyer or successor to the business	Limited disclosure during a genuine corporate transaction, subject to confidentiality and continued protection of personal data.

We keep a current processor record, assess a provider before allowing it to receive identifiable health data, and review our providers' notices of new subprocessors. We will update this policy or provide another appropriate notice if a material new recipient changes how your data is used.

9 International transfers

Your health records are stored outside the UK: our main database and uploaded files are hosted by Hetzner in Germany, our encrypted backups are stored within the EU/EEA, and identifiable patient content sent for AI processing goes to Microsoft's EU Data Zone or a Google EU endpoint. The UK treats EEA countries as providing adequate protection, and these transfers rely on UK adequacy regulations. Our providers and their subprocessors may also process some data in other countries, including the United States and India, for example for payments, support, security or account administration.

Where data is transferred, we use a lawful safeguard appropriate to the recipient, such as UK adequacy regulations, the UK Extension to the EU-US Data Privacy Framework for an actively certified US recipient, the UK International Data Transfer Agreement, or EU Standard Contractual Clauses with the UK Addendum. Where required, we complete a transfer risk assessment and use additional technical and organisational measures.

Microsoft's EU Data Zone can process a request in any EU Member State within that zone. Google's terms allow processing in other countries where Google or its subprocessors have facilities, subject to the location commitments in its service terms. Microsoft's terms rely on the EU Standard Contractual Clauses with the UK Addendum and Microsoft's certification under the UK Extension to the EU-US Data Privacy Framework for transfers outside the UK and EEA. Stripe processes payment information in the United States and other countries where it operates; for data it processes for us, Stripe's terms rely on the UK Extension to the EU-US Data Privacy Framework and standard contractual clauses, and when it acts as a controller it is responsible for its own transfers. Brevo's terms rely on standard contractual clauses and, for US recipients, the Data Privacy Framework.

10 How long we keep information

We keep personal data only for as long as needed for the stated purpose, taking account of user instructions, legal duties, security, disputes and the way our providers delete data.

Information	Retention approach
Account and health content	Kept while the relevant profile or account is active. On verified deletion or consent withdrawal, we stop ordinary use and delete it from active systems, subject to legal exceptions. Copies in our encrypted backups are deleted or overwritten according to our backup-retention schedule.
Recordings, transcripts and summaries	Kept until the user deletes them, the clinic instructs deletion, or the applicable profile/account is closed, unless a shorter setting is shown.

Information	Retention approach
Sharing and access records	Kept while needed to show who received access, protect the account and resolve a dispute or security issue.
Security, audit and error records	Kept for the shortest period needed to secure the service, investigate incidents and demonstrate accountability; incident-related records may be kept longer.
Consent, contract, billing and complaint records	Normally kept for up to six years after the relevant relationship or matter ends where needed for legal, tax or claims purposes.
Processor residual copies and backups	Deleted or overwritten under each provider's deletion terms, which differ between providers. For example, Google Cloud's terms provide for deletion within a maximum of 180 days after we delete data, and Microsoft deletes stored customer data within 180 days after our subscription ends. Not every provider commits to a fixed timetable for every backup or log; we can tell you on request what applies to a particular provider.

If law, litigation or a regulator requires preservation, we isolate the necessary information and keep it only for that purpose. We anonymise information when we no longer need to identify anyone and may keep genuinely anonymous statistics.

Our email and payment providers keep information as their terms and privacy policies describe. We keep a record of an unsubscribe for as long as needed to respect it. Stripe may need to keep payment and transaction records for financial-services, anti-money-laundering or fraud-prevention reasons even after you close your HealthFort account.

11 Security

We use technical and organisational measures appropriate to the sensitivity of the records. These include encryption in transit; encryption of stored production data and backups, which we apply and manage ourselves because our hosting provider does not encrypt stored data on our behalf; access controls; authentication; audit logging; backups; separation of development and production environments; and written data processing agreements with our processors, which require them to protect data and to tell us without undue delay about a security breach affecting it.

HealthFort is not end-to-end encrypted: the service must be able to read content on the server to extract, transcribe and summarise it. No internet service can guarantee absolute security. You should use a strong unique password, protect your devices and tell us promptly about suspected unauthorised access.

12 Family profiles and information about other people

If you create a profile for another person, you must have parental responsibility, legal authority or that person's informed permission. You should show or explain this policy to them in a way they can understand and tell us if your authority changes.

Where the person is a child, the account holder must act in the child's best interests and take their views into account according to their maturity. Children do not operate their own HealthFort accounts. We apply provider-routing restrictions so that child-profile content is not sent to an AI service whose terms prohibit that use.

If the represented person contacts us, we may verify identity and authority, restrict the account holder's access, separate or delete records, or refer the request to the relevant controller. Genetic information may reveal facts about biological relatives; upload and share it cautiously.

13 Recordings and clinicians

The person starting a consultation recording must give all participants clear notice and obtain any permission required by law, professional duties and clinic policy. HealthFort processes the audio to create a transcript and descriptive summary. A clinician must verify the output before clinical use.

When you share records with a clinician, revocation prevents future access through HealthFort but cannot erase a copy already downloaded or entered into the clinician's records. The clinician or clinic may then have its own retention and privacy duties.

14 Your rights

Depending on the circumstances, you may have the right to:

- be informed about processing and obtain a copy of your personal data;
- correct inaccurate or incomplete data;
- ask for deletion or restriction;
- receive data you provided in a structured, commonly used, machine-readable format and transmit it to another controller;
- object to processing based on legitimate interests or to direct marketing;
- withdraw consent at any time; and
- not be subject to a solely automated decision producing legal or similarly significant effects. HealthFort does not make such decisions. Our payment provider's automated fraud checks are described in section 8.

Rights are not absolute and an exemption may apply. We may ask for information to verify identity or authority. We normally respond within one month. We may extend by up to two further months where a request is complex or numerous, and will tell you within the first month. We do not normally charge a fee, but may do so or refuse a request where the law permits for manifestly unfounded or excessive requests.

To exercise a right, contact info@healthfort.uk. A self-service export may be available on some plans, but data-protection rights are available regardless of subscription tier.

If you contact one of our processors directly, it will normally refer you to us. For information that Stripe or Brevo hold as separate controllers, you can also contact them directly; their privacy policies explain how.

15 Marketing, analytics and cookies

We send account and security emails because they are needed to operate your account. We send marketing emails only if you have opted in, and every marketing email contains an unsubscribe link; you can also opt out by contacting us. Account and marketing emails are sent through our email provider, Brevo, which may record whether an email was delivered and, where enabled, whether it was opened or a link was clicked. Our emails never contain health or genetic information, and we will never ask you to send your password or health records by email.

We use cookies and similar storage that are strictly necessary for sign-in, security and preferences. When you pay, you use pages hosted by Stripe; on those pages Stripe sets its own cookies and collects device and browser information, including for security and fraud prevention, as described in Stripe's cookie policy. If we introduce non-essential analytics or advertising technologies, we will provide a cookie notice and obtain consent where PECR requires it.

16 Children

HealthFort accounts are for adults aged 18 or over. The service is not directed to children. An authorised adult may manage a child profile as described above, but a child must not log in or use the account as an end user.

17 Sale, training and research

We do not sell personal data. The terms of the Microsoft and Google services we use state that our customer content is not used to train their foundation models without our permission, and we have not given that permission. We do not use identifiable health records for unrelated model training, commercial research or clinical-trial matching under this policy.

If we introduce research or another materially different purpose, we will provide specific information before it begins and obtain separate explicit consent where required. Declining an optional research purpose will not remove access to the ordinary HealthFort service.

18 Complaints

Please contact us first at info@healthfort.uk so we can investigate. You may also complain to the Information Commissioner's Office at ico.org.uk or by telephone on 0303 123 1113. If a clinic controls the relevant data, you may also complain to the clinic.

You can write to HEALTHFORT LTD, 483 Green Lanes, London, England, N13 4FG. Please read the note in section 1 before sending anything by post.

19 Changes to this policy

We may update this policy when the service, providers, law or processing changes. We will show the current effective date and notify you of a material change by email, in-app message or another appropriate method before it takes effect where practicable. If a new purpose requires consent, we will ask rather than treating continued use as consent.