PRIVACY POLICY

VisitHealth

This is our CURRENT Privacy Policy and was Last Revised on the 2nd of August 2022. For further information on our policies please Contact Us.

Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities should you need to. Please retain a copy for your records. This policy forms part of VisitHealth's terms and conditions and is incorporated into the Patient Medical Services Agreement.

By using our website (https://visithealth.london/), app (together the 'Platform') and/or receiving our healthcare services in any form via any media (the 'Services') you agree to accept the terms of this Privacy Policy, as updated from time to time. This Privacy Policy governs the use of your personal data processed through the Platform, our apps and through interactions with VisitHealth, whether through visits to our premises, our staff attending to you elsewhere, or via virtual appointments (telemedicine). It is recommended that you read this Privacy Policy each time you consider or choose to use the Platform or the Services to ensure that you have not missed any changes to this Privacy Policy.

UPDATES TO THIS POLICY

We regularly review this Privacy Policy and we may revise it from time to time to reflect any changes in its privacy practices. We reserve the right to make any revised policy effective for Personal Data we already have about you as well as any information we receive in the future. We will post a copy of the updated policy on our Platform prior to any change becoming effective. The effective date of this policy is displayed directly under the title of the document. If we make any material changes, we will notify you by means of a notice on the Platform prior to the change becoming effective.

Your continued use of the Platform and/or Service following any changes to the Privacy Policy (which will be notified to you as described above) signifies your acceptance of those changes.

COMPANY INFORMATION

VisitHealth Limited, registered in England and Wales with company number 10766569, (VisitHealth, we, us), respects the privacy of every person and is committed to protecting all of your personal data, including sensitive personal health and medical information (Personal Data). Our registered address is 1 Blythe Road, London, England, W14 0HG.

VisitHealth is a patient-focused company that strives to improve the health of our patients. We offer comprehensive private primary health care services together with preventative health care solutions. VisitHealth has a platform via which individuals in the UK ('Customer', 'Customers', 'you', 'your', 'yourself') may connect in real time, via phone call, chat, instant messaging and picture

messaging, to participating medics registered with the Nursing and Midwifery Council: www.gmc-uk.org, (the GMC) (known as 'VH Medics'), and may purchase the Services.

This Privacy Policy (together with our Terms and Conditions of Use set out and updated from time to time (Terms and Conditions)) applies to your use of:

the website at https://visithealth.london/ (Platform); and

- together, the Platform, and any of the services accessible via the Platform or as a patient receiving healthcare services from us, in whatever form.

For the purpose of the UK General Data Protection Regulation (UK GDPR), the UK Data Protection Act 2018and any data protection legislation from time to time in force in the UK (together the Data Protection Legislation), the data controller is VisitHealth Limited, 1 Blythe Road, London, England, W14 0HG. Our Data Protection Manager can be contacted by email at dpo@visithealth.co.uk

PERSONAL DATA WE COLLECT ABOUT YOU

Personal Data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). A data subject is the individual who the personal data relates to.

We collect, use, store and transfer different kinds of Personal Data about you which we have grouped together as follows:

A- Standard Personal Data

- Identity Data includes first name, maiden name, last name, marital status, title, date of birth, age, gender, location, income, username, password and other registration information, personal description and/or photograph.
- Contact Data includes billing address, email address and telephone numbers.
- Financial Data includes financial and payment card details. This information is maintained by our billing processing partner in a secure vault (compliant with the payment card industry security standard) for use when you decide to utilise any Services.
- Transaction Data includes details about payments to and from you and other details of Services you have purchased from us.
- Technical Data includes:
    - the type of device (mobile, smartphone, tablet or any other electronic device) you are using when you visit the Platform, the temporary or persistent unique device identifiers (UDIDs) placed by us or our service providers, the unique identifier assigned by VisitHealth to your device, the I.P. address of your device, your mobile operating system, the type of mobile internet browsers you

use and data about the way you use our Platform (Device Information);

- information about your visit, including the full uniform resource locators (URL) clickstream to, through and from the Platform (including date and time); Services you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs), consultation length(s), recurrence of visits and other interaction information, methods used to browse away from the page and any phone number used to call our customer service number (Website Information);
- details of your use of the Platform including, but not limited to, traffic data, weblogs and other communication data, whether this is required for our own billing purposes or otherwise, and the resources that you access (Log Information).

- Profile Data includes your email or mobile telephone number and username, password, purchases or orders made by you, your interests, preferences, feedback and survey responses (where not anonymised by you).
- Usage Data includes information about how you use our Platform and Services click movements, browsing time and details.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

B- Special Categories of Personal Data

Special Categories of Personal Data (or 'Sensitive Personal Data') includes information about your physical and mental health, your NHS or other medical records; measurements, weight, blood pressure or glucose levels; test results; health history, family history, medication details and other health information, health concerns, description of symptoms, allergies, data concerning sex life or sexual orientation, race, ethnic origin, and genetic and biometric data (when processed to uniquely identify an individual), data about any criminal convictions and offences (we may process this data when carrying out anti-fraud or anti-money-laundering checks).

Information that VH Medics on record in your online notes (your Electronic Medical Records or 'EMRs') which include relevant and pertinent information that you have discussed with VH Medics. Such EMRs may also include VH Medic' comments, diagnoses and commentary as well as factual information, medical advice and the symptoms that you have presented with in a session.

HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through:

3

Commented [MR1]: Again, please check and confirm.

Commented [VG2R1]: Some of these features are not active as of the moment. Like the online account.
But we'd prefer to keep it for the time when relevant (should happen shortly)

Do we need to mention online payments here?

Commented [Selin3R1]: "make an online purchase" under direct interactions will cover online payments.

- Direct interactions. You may give us your Identity, Contact and Financial Data and Sensitive Personal Data by filling in forms, communicating with us directly, submitting or uploading information to our Platform or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
    - create an online account on our Platform;
    - search for the Platform or any Service;
    - make an online purchase;
    - log in to the Platform and use the Services;
    - face to face interactions (for example, in medical consultations, diagnosis and treatment);
    - by filling in an application or other forms;
    - report a problem with the Platform;
    - request marketing to be sent to you;
    - enter a competition, promotion or survey;
    - contact us; or
    - provide us with your feedback.
- Automated technologies or interactions. As you interact with our Platform, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.
- Location data. We may also use GPS technology to determine your current location only if you enable the location services by turning on GPS settings in your device to allow us to do so. Some of our location-enabled Services require your personal data for the feature to work. If you wish to use the particular feature, you will be asked to consent to your data being used for this purpose. You can withdraw your consent at any time by turning off your GPS setting in your device.
- Third parties or publicly available sources. We may receive personal data about you from various third parties, including, for example, local NHS practices and community services, doctors, GPs and other health care professionals, hospitals, clinics and other health care providers, brokers and insurers, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers such as Google, search information providers, credit reference agencies, your parent or guardian, if you are under 18 years old.

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 your relationship with us.

4

Commented [MR4]: Could you please confirm whether this is still used or if you have plans to use it in the future?

Commented [VG5R4]: No, we do not. And doubt we ever did.
I expect this is meant for future mobile application.

Commented [Selin6R4]: We may keep it for future App uses.

HOW AND WHY WE USE YOUR PERSONAL DATA

We will only use your Personal Data when the law allows us to. Most commonly, we will use your Personal Data in the following circumstances:

- We process Personal Data about you because the processing is necessary;
    - for the performance of the contract that we have with you (or are about to enter into with you) to make available the Services, or to take steps at your request before entering into a contract;
    - for compliance with a legal or regulatory obligation which we are subject to;
    - for the purposes of our legitimate interests (or those of a third party), except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data; or
    - in limited circumstances where you have provided your consent.

We process Sensitive Personal Data (relating to your health and medical records), in accordance with this Privacy Policy, only where:

- you have given us explicit consent to do so;
- the processing is necessary to protect the vital interest of you or another person where you or that person is physically or legally incapable of giving consent;
- the processing is necessary to establish, make or defend actual or potential legal claims;
- where the processing is necessary for the provision of healthcare or treatment or the management of healthcare systems and services;
- for scientific or historical research purposes;
- the processing is necessary for reasons of public interest in the area of public health pursuant to applicable laws; or
- the processing is necessary to establish, exercise or defend legal claims.

The table below explains what we use your personal data for and why.

What we use your personal data for	**Our reasons**
Providing you with Services and to send you essential information about the Services	To perform our contract with you or to take steps at your request before entering into a contract

What we use your personal data for	Our reasons
	Necessary for the purposes of preventive or occupational medicine
Registering you and setting you up as a new customer	To perform our contract with you
Validating your Account and/or to reset your username and password if required	To perform our contract with you
Management of your Account with us	To perform our contract with you
Creating a record of the consultations, care/advice and Services you receive. (e.g. electronic medical records)	To perform our contract with you
Facilitating treatment or the provision of medical services.	To perform our contract with you
Planning your care and treatment, monitoring the quality of your treatment and care, sharing your sensitive personal data with other health care professionals and health care providers who are treating you, so that they can provide treatment.	To perform our contract with you Consent in certain circumstances Where it is necessary to protect the vital interest of you or another person to prevent a serious threat to your health and safety or that of others where you or that person is physically or legally incapable of giving consent Where it is necessary for reasons of public interest in the area of public health
Verifying your identity and where applicable, your parental responsibility for any under 18 family member you add to your Account.	To perform our contract with you To comply with a legal obligation
Operating and improvement of the Platform and to ensuring that content from the Platform is presented in the most effective manner for you and your computer or device	To effectively perform our contract with you For our legitimate interests i.e. to make sure we can deliver the best service to

What we use your personal data for	Our reasons
	you and respond to you when you need us
Notifying you about changes to the Platform and/or Services and/or to this Privacy Policy or our Terms and Conditions or Patient Medical Services Agreement.	To perform our contract with you To comply with a legal obligation
Undertaking planning, Service evolution, new product development, Service delivery, internal and external performance indicators and a range of other business intelligence functions	To effectively perform our contract with you For our legitimate interests i.e. to make sure we can deliver the best service to you and respond to you when you need us
To carry out surveys and/or provide feedback from you about the Services or about customers' habits as a consumer	To effectively perform our contract with you For our legitimate business interests to provide our services
Allowing you to participate in interactive features of the Services	To effectively perform our contract with you Consent in certain circumstances
Protecting your safety during an emergency by contacting emergency services and your emergency contact	Consent in certain circumstances Where it is necessary to protect the vital interest of you or another person to prevent a serious threat to your health and safety or that of others where you or that person is physically or legally incapable of giving consent
Maintaining a detailed record of the medical care you receive to safely	To comply with a legal obligation

What we use your personal data for	Our reasons
provide future care based on your medical history	To effectively perform our contract with you
Customer service and responding to any queries you raise with us and to provide customer support	To effectively perform our contract with you For our legitimate interests i.e. to make sure we can deliver the best service to you and respond to you when you need us
Preventing and detecting fraud against you or us	For our legitimate interests or those of a third party, i.e. to minimise fraud that could be damaging for you and/or us
Conducting checks to identify our customers and verify their identity Screening for financial and other sanctions or embargoes Other activities necessary to comply with professional, legal and regulatory obligations that apply to our business, e.g. under health and safety law or rules issued by our professional regulator	To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, i.e. to minimise fraud and to prevent consumers registering more than one account in order to exploit our services.
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Management of promotions or competitions that you choose to enter	To perform our contract with you For our legitimate interests or those of a third party, i.e. to study how customers use our products/services, to develop them and grow our business
Ensuring business policies are adhered to, e.g. policies covering security and internet use	For our legitimate interests or those of a third party, i.e. to make sure we are following our own internal procedures so we can deliver the best service to you

What we use your personal data for	Our reasons
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service to you at the best price
Ensuring the confidentiality of commercially sensitive information	For our legitimate interests or those of a third party, i.e. to protect trade secrets and other commercially valuable information To comply with our legal and regulatory obligations
Statistical analysis to help us manage our business, e.g. in relation to our financial performance, customer base, product range or other efficiency measures	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service to you at the best price
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	For our legitimate interests i.e. to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy
Preventing unauthorised access and modifications to systems	For our legitimate interests or those of a third party, i.e. to prevent and detect criminal activity that could be damaging for you and/or us To comply with our legal and regulatory obligations
Updating and enhancing customer records and our service provided to you	To perform our contract with you or to take steps at your request before entering into a contract To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g. making sure that we can

What we use your personal data for	Our reasons
	keep in touch with our customers about existing orders and new products
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing of our services	Where you have given your consent In certain circumstances, for our legitimate interests or those of a third party, i.e. to promote our business and services to existing and former customers

We also collect, use and share Aggregated Data such as statistical or demographic data. Aggregated Data may be derived from your Personal Data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data for: (i) statistical analysis, improvement of the Services and customisation of UX-design and content layout or creation; or (ii) sharing with government agencies or regulators that oversee and monitor health care providers in both the public and private sectors. However, if we combine or connect Aggregated Data with your Personal Data so that it can directly or indirectly identify you, we treat the combined data as Personal Data which will be used in accordance with this Privacy Policy.

Marketing

You will receive marketing communications from us if you have requested information from us or purchased Services from us and you have not opted out of receiving that marketing

We may use your personal data to send you updates (by email, text message, telephone or post) about our products and services, including exclusive offers, promotions or new products and services.

We have a legitimate interest in using your personal data for marketing purposes (see above 'How and why we use your personal data'). This means we do not

usually need your consent to send you marketing information. However, where consent is needed, we will ask for this separately and clearly.

You have the right to opt out of receiving marketing communications at any time by :

- contacting us at hello@visithealth.co.uk; or
- using the 'unsubscribe' link in emails;

We may ask you to confirm or update your marketing preferences if you ask us to provide further products and services in the future, or if there are changes in the law, regulation, or the structure of our business.

We will always treat your personal data with the utmost respect and will obtain your express opt-in consent before we share your personal data with any third party for marketing purposes.

Change of Purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

WHO DO WE SHARE YOUR PERSONAL DATA WITH?

We may have to share your personal data with the parties set out below for the purposes set out in the section above.

- In order to provide the Services, we need to share your Sensitive Personal Data with VH Medics and members of the VisitHealth team (from time to time, as required) who have been appropriately checked (including DBS checked) to ensure they meet the requirements to access such information (in accordance with UK law).
- We may share your Sensitive Personal Data with healthcare providers and health care professionals such as your NHS GP practice, doctors, clinicians, pharmacists, referring practitioners, specialists, hospitals, clinics, pathology and imaging centres, secondary care specialist and emergency services so that they can provide treatment to you and so that we can monitor the quality of your treatment and care. For example, we may share your personal health information to plan your care. This may include prescriptions, lab work, other digitised / digital health information that you make available to us about you from time to time. VisitHealth will make all reasonable endeavours to procure that such persons securely store,

Commented [VG7]: In healthcare we have to run "enhanced" DBS. I think it might be worth mentioning?

Commented [Selin8R7]: We believe it is sufficient as it is for the privacy policy but it is good to know, thanks for the info.

transmit or destroy such data and comply in all respects with applicable Data Protection Legislation from time to time.

- We may pass personal information to people who process data for us in accordance with this Privacy Policy, for example, companies which provide data storage, data analytics, advertising, IT support and other services. We have contracts with these third parties and we vet them to ensure they are contractually bound to protect your privacy.
- We may disclose your personal information to the following third-party data processors:
    - We may disclose or otherwise make available Personal Data about you to service providers that assist the function of the Platform. These service providers may collect device-specific data. This data will not be associated in any way with your Account or any Personal Data that identifies who you are; we use this data to improve our Platform.
    - Your email address and mobile number may be shared with third parties working with VisitHealth in the delivery and development of the Services and the Platform, to track usage, and these details may be used to advertise new VisitHealth services to you from time to time but only where you have opted-in to receive marketing communications (unless a legitimate interest applies, as mentioned above).
    - You should also know that we work with third party analytics companies to discover how we can improve, update and change the Platform. Such third parties may therefore gain access to your Personal Data where you have consented to this (but not any medical records or other Sensitive Personal Data).
- In addition, we may share your Personal Data with third parties:
    - to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your Personal Data in the same way as set out in this Privacy Policy;
    - if we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation or request;
    - enforce or apply the Terms and Conditions or terms of the Patient Medical Services Agreement or to investigate potential breaches of these documents;
    - to protect the rights, property or safety of VisitHealth, our customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction; and/or
    - to our insurers and brokers, our bank and credit reference agencies.

We only allow our service providers to handle your personal data if we are satisfied that they take appropriate measures to protect your personal data. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. If any such third party requires access to your Sensitive Personal Data in order to perform the agreed services, we will make all reasonable endeavours to procure that such third party complies with: (i) the terms of this Privacy Policy; and (ii) applicable Data Protection Legislation from time to time as well as seeking informed consent from you.

Where the processing is necessary for reasons of public interest in the area of public health, we may share your Personal Data with a third party. For example, we may share your Personal Data with the UK Government departments or other relevant authorities:

- to report reactions to medicines or problems with products;

  if a VH Medic believes that you may have been exposed to, or may be at risk of spreading, certain specified serious diseases or conditions.

Where the processing is necessary in relation to an actual or potential legal claim – If you are involved in a legal dispute, VisitHealth may share your Sensitive Personal Data in response to a court order, legal demand or other lawful process;

- The Police – VisitHealth may share Sensitive Personal Data if asked to do so by the police in certain limited circumstances, including reporting of certain types of injuries.

  National Security – VisitHealth may share, if required, your Personal Data with UK Government officials for national security reasons.

If you grant us access, we may be able to collect information from third party services when you use them, such as smart devices, mobile health applications, Microsoft HealthVault or Google Health and any other data storage connection points to which you provide us access to.

Certain features of the Platform link to social networking. Ensure when using these features that you do not submit any Personal Data that you do not want to be seen, collected or used by third parties.

If you would like more information about who we share our data with and why, please Contact Us.

COOKIES

A cookie is a small text file that may be placed on your computer or device when you visit the Platform. We use cookies on our Platform. Please see https://visithealth.london/cookie-policy/ for our cookie policy.

Commented [Selin9]: We deleted the detailed info as to cookies here as they are now included in the cookie policy.

For further information on cookies generally, including how to control and manage them, visit the guidance on cookies published by the UK Information Commissioner's Office, www.aboutcookies.org or www.allaboutcookies.org.

If you would like details of the cookies we use on our website, please Contact Us.

SECURITY

The importance of security for all your Personal Data including, but not limited to, Sensitive Personal Data is of great concern to us. At VisitHealth, we have gone to great lengths to manage the security and integrity of the Platform and to ensure that we use best–in-class services when providing secure transmission of information from your computer or device.

Personal Data collected via the Platform is stored in secure environments that are not available or accessible to the public; only those duly authorised people, officers, employees or agents of VisitHealth who need access to your information in order to do their jobs are allowed access. Anyone who violates our privacy or security policies is subject to disciplinary action, including possible termination of their contract with VisitHealth and civil and/or criminal prosecution.

VisitHealth uses the latest technologies to ensure the utmost security, including utilising several layers of firewall security and encryption of Personal Data to ensure the highest level of security.

Where your personal data is held

The Personal Data that we collect from you may be held at our offices, third party agencies, service providers, representatives and agents as described above (see above: 'Who do we share your personal data with').

Some of these third parties may be based outside the UK/EEA. For more information, including on how we safeguard your personal data when this happens, see below: 'Transferring your personal data out of the UK`. We will take all steps reasonably necessary to ensure that your Personal Data is treated securely and in accordance with this Privacy Policy.

We may collect and store Personal Data on your device using application data caches and browser web storage (including HTML 5) and other technology.

Transferring your personal data out of the UK

To deliver services to you, it is sometimes necessary for us to share your personal data outside the UK, for example:

- with your and our service providers located outside the UK;
- if you are based outside the UK;

Under data protection law, we can only transfer your personal data to a country or international organisation outside the UK where:

- the UK government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'adequacy decision');

- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under data protection law

We may also transfer information for the purpose of our compelling legitimate interests, so long as those interests are not overridden by your interests, rights and freedoms. Specific conditions apply to such transfers and we will provide relevant information if and when we seek to transfer your personal data on this ground.

If you would like further information about data transferred outside the UK, please Contact Us.

Security of your Personal Data

We have appropriate security measures to prevent personal data from being accidentally lost, used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality. We also have security procedures in place as well as technical and physical restrictions to access to ensure that your personal data is safeguarded at all times. We have procedures in place to deal with any data security breach. We will notify you and any applicable regulator of a data security breach where we are legally required to do so.

When using the Platform, all your Personal Data, including but not limited to your debit or credit card number(s), are transmitted through the internet using Secure Socket Layers (SSL) technology. SSL technology causes your browser to encrypt your entered information before transmitting it to our secure server. SSL technology, an industry standard, is designed to prevent a third party from capturing and viewing your Personal Data. VisitHealth also takes the following measures to protect your Personal Data online:

Two-Step Process

You are required to go through a two-step verification process to create and restore your Account. Online access to your Account is protected with a password that you create. We strongly recommend that you do not disclose your password to anyone. VisitHealth will never ask you for your password in any unsolicited communication (including unsolicited correspondence such as letters, phone calls, email or text messages). You will only ever be able to reset your password using a two-step process.

Information

Since any information you provide to us on the Platform will be transmitted using a secure connection, if your web browser cannot support the required level of security you will not be able to use the Platform properly. The most recent versions of Google Chrome, Safari, Microsoft Edge and Firefox can support a secure connection and can be downloaded for free from their respective

websites. Should you choose to download and/or install any such package such actions are at your own risk.

While we strive to protect your Personal Data from unauthorised access, use or disclosure, VisitHealth cannot ensure or warrant the security of any information you transmit to us via the Platform. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

YOUR RIGHTS

Under certain circumstances, you have the following legal rights in respect of your Personal Data which you can exercise at any time:

- A right to be informed about and request access to your Personal Data and a copy of any Personal Data that we hold relating to you

Most information we hold about you is in your patient record, accessible from the Platform. However, you have the right to submit a request, which enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- A right to request rectification of your Personal Data

If you believe that any of your data is incorrect, you can ask us to correct it. We make sure to do so if this is the case, however, we may need to verify the accuracy of the new data you provide to us.

- A right to request erasure of your Personal Data in certain situations

This enables you to ask us to delete or remove personal data where there is no lawful basis for us to continue to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below). Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. In particular, our obligation under applicable laws to retain patient records means we may not be able to erase your medical record.

- A right to ask us to restrict processing of your Personal Data in certain circumstances,

This enables you to ask us to suspend the processing of your personal data if you would like us to verify it is accurate; where the data has been processed unlawfully, but you do not want us to erase it; where you need us to hold the data even if we no longer require it to establish, exercise or defend legal claims; where you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

- A right to object to our processing of your Personal Data in certain other circumstances

You can object

—at any time to your personal data being processed for direct marketing (including profiling);

—in certain other situations to our continued processing of your personal data, e.g. processing carried out for the purpose of our legitimate interests.

- A right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party (data portability)—in certain situations

Your Personal Data will be provided in a structured, commonly used, machine-readable format. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Note that this right only applies to information you have provided to us.

- A right not to be subject to a decision based solely on automated processing (including profiling);
- If we use your personal data for the purposes of automated decision-making (a decision solely by automated means without any human involvement) and those decisions have a legal (or similarly significant effect) on you, you have the right to challenge to such decisions under the GDPR. You may request human intervention, express your point of view, and obtain an explanation of the decision from us. A right to withdraw consent at any time (where relevant)

Where we rely on consent as a legal basis for processing your personal data (for example, in certain occasions, to process your Sensitive Personal Data or to send direct marketing communications to you). You have the right to withdraw consent to marketing at any time by Contacting Us. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

A right to lodge a complaint about how we treat your Personal Data with the Information Commissioner's Office.

If you exercise your right to object to our processing of your Personal Data or if you exercise your right to ask us to restrict processing of your Personal Data, it may impact on your use of the Services and/or Platform and/or we may not be able to provide you with information about the Service that you have requested us to provide to you.

Exercising Your Rights

If you wish to discuss or make a request in respect of any of the above rights, please Contact Us or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights.

If you would like to exercise any of your rights, please:

- Contact Us;
- provide enough information to identify yourself; and

- let us know what right you want to exercise and the information to which your request relates.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

HOW LONG WE KEEP PERSONAL DATA

We will keep your personal data while you have an account with us or we are providing Services to you. Thereafter, we will keep your personal data for as long as is necessary:

- to respond to any questions, complaints or claims made by you or on your behalf;
- to notify you of any health or safety risk in relation to any of the products that have been delivered to you
- to show that we treated you fairly;
- to keep records required by law.

To determine appropriate retention period, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process your personal data and the applicable legal, regulatory, tax, accounting, or other requirements. In any case, we will not keep your personal data for longer than necessary. Different retention periods apply for different types of personal data. When it is no longer necessary to keep your personal data, we will delete or anonymise it.

We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

How to make a complaint

Please Contact Us if you have any query or concern about our use of your information. We hope we will be able to resolve any issues you may have.

You also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with

your concerns before you approach the ICO so please contact us in the first instance.

OTHER PROVISIONS

Other Links

The Platform may contain links to let you to visit other websites or mobile applications easily. If you click on a link to a third-party site or app, you will leave the Platform and go to the site or app you selected. Because VisitHealth cannot control the activities of third parties, we cannot accept responsibility for the content of any such sites or apps or for any use of your Personal Data by such third parties and we cannot guarantee that they will adhere to the same privacy practices as VisitHealth. If you visit a third-party website that is linked to our site, you should read that site's privacy policy before providing any personal information.

Social Media Sharing

Our Platform includes some social media features and widgets are either hosted by a third party or hosted directly on our Platform. Your interactions with these features are governed by the privacy policy of the company providing it.

HOW TO CONTACT US

You can contact us and our data protection manager by post, email or telephone if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint.

Our contact details are shown below:

Our contact details	
Address:	VisitHealth Limited, 1 Blythe Road, London, England, W14 0HG
Email address:	dpo@visithealth.co.uk
Telephone number:	+ 44 020 3795 5811

Last revision date: 02 August 2022