PRIVACY AND COOKIE POLICY

VisitHealth

This is our CURRENT Privacy Policy and was Last Revised on the 19th of September 2019. For further information on our policies please Contact Us.

Please read this privacy policy carefully and retain a copy for your records. This policy forms part of VisitHealth's terms and conditions.

By using our website (http://visithealth.co.uk) and app (the 'Platform'), to obtain access to our healthcare services (the 'Services') you agree to accept the terms of this Privacy Policy, as updated from time to time. If you do not agree with this policy, you should not use the Platform or the Services. 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

VisitHealth may revise this Privacy Policy from time to time to reflect any changes in legislation or to 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).

VisitHealth uses 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, with participating medics registered with the Nursing and Midwifery Council: www.gmc-uk.org, (the GMC) (known as VH medics), and you may purchase the Services (as defined below).

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

- the website at visithealth.co.uk and any app we may have (Platform); and
- any of the Services accessible via the Platform.

For the purpose of the General Data Protection Regulation ((EU) 2016/679) (GDPR) and any data protection legislation from time to time in force in the UK including the Data Protection Act 2018 or any successor legislation (together

the Data Protection Legislation), the data controller is VisitHealth Limited, 24 Elgin Court, 164 Elgin Avenue, London, W9 2NU. Our Data Protection Officer can be contacted by email at dpo@visithealth.co.uk.

COMPLAINTS

You 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.

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).

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

- Identity Data includes first name, maiden name, last name, marital status, title, date of birth, age, gender. username, password and other registration information, personal description and/or photograph.
- Contact Data includes billing address, email address and telephone numbers (both landline and mobile).
- Financial Data includes financial and payment card details. This information is maintained by our billing processing partner in a secure vault (who is 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 or tablet) 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 password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- Usage Data includes information about how you use our Platform and Services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- Special Categories of Personal Data (or "Sensitive Personal Data") includes 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. Information that VH medics on the Platform record in your online notes (your Electronic Medical Records or EMRs) will include relevant and pertinent information that you have discussed with the VH medics on the Platform. 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 an appointment. We will also collect and process demographic information about you (where available) such as your age, location, gender and income. To protect your EMRs we print hard copies and place these in a secure vault environment at regular intervals throughout the year.

HOW IS YOUR PERSONAL DATA COLLECTED?

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

- Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
    - create an online account (Account) on our Platform;
    - Upload Personal Data on the Platform via your Account:
    - search for the Platform or any Service;
    - make an online purchase;
    - log in to the Platform and use the Services;
    - report a problem with the Platform;
    - request marketing to be sent to you;
    - enter a competition, promotion or survey; or
    - give us some 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. 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, business partners, sub-contractors, payment and delivery services, advertising networks, analytics providers, search information providers and credit reference agencies.

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.

LAWFULNESS OF OUR PROCESSING

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 the Service available to you;
    - for compliance with a legal obligation which we are subject to; or
    - for the purposes of our legitimate interests, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Data.
- We process Sensitive Personal Data (relating to your health and medical records), in accordance with this Privacy Policy, only where:
    - you have agreed to do so at the time that you register an Account with us;
    - 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 in relation to an actual or potential legal claim; or
    - the processing is necessary for reasons of public interest in the area of public health.
- When you first create an Account, we ask for your consent to send you marketing communications (by emails, text message, post and/or telephone) about our Services that we think may be of interest to you.

We may request your consent to process your Personal Data but we do not rely on explicit consent from you as the legal basis for processing your

Personal Data in relation to providing healthcare Services. Where we rely on consent as a legal basis for processing your Personal Data (for example, to send direct marketing communications to you), you have the right to withdraw consent to marketing at any time by Contacting Us.

HOW WE USE YOUR DATA

Essential Uses of Personal Data

We process the Personal Data we collect in order to provide you with the Services and to send you essential information about the Services (where you ask us to send you such information) and to help us with the operation of the Platform. We could give lots of examples; here are some typical examples:

- to provide you with the information and Services that you request from us;
- we will use the email address and mobile number you provide when you register to send you a text message requesting that you validate your Account and/or to reset your username and password if required;
- to notify you about changes to the Platform and/or Services and/or to this Privacy Policy or our Terms of Use;
- to ensure that content from the Platform is presented in the most effective manner for you and your computer or Device;
- to undertake planning, Service evolution, new product development, Service delivery, internal and external performance indicators and a range of other business intelligence functions;
- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to allow you to participate in interactive features of the Services;
- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you; and
- to respond to any queries you raise with us and to provide customer support.

Essential Use and Disclosure of Sensitive Personal Data

We process Sensitive Personal Data for the purpose of providing treatment and medical Services to you, as described in more detail below:

- To create a record of the consultations, care/advice and Services you receive. Some examples of the information collected or created through this process are electronic medical records that may be uploaded by you or created as a result of your use of the Services;
- To facilitate treatment or the provision of medical services by a VH medic. VisitHealth may share your Sensitive Personal Data with doctors, technicians or VisitHealth employees, as required to fulfil its contractual obligations to you. For example, departments 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, transmit or destroy such data and comply in all respects with applicable Data Protection Legislation from time to time;

- To share your Sensitive Personal Data with people not at VisitHealth including, but not limited to, referring practitioners, specialists, GP practices, hospitals, pharmacists, pharmacies and other healthcare providers who are treating you;
- To use and disclose your Sensitive Personal Data to help us in the operating and improvement of the Platform. For example, VisitHealth may use Sensitive Personal Data to review the treatment and provision of Services by certain VH medics. VisitHealth may also use Sensitive Personal Data to measure the performance of its own staff and may share Sensitive Personal Data with third parties who VisitHealth engages to provide various Services on the Platform or to VisitHealth itself, such as VH medics and other healthcare workers, research agencies and clerical services providers. If any such third party requires access to your Sensitive Personal Data in order to perform the agreed services, VisitHealth 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;
- Where the processing is necessary to protect the vital interest of you or another – for example – VisitHealth may use and disclose your Personal Data to the extent required to protect the vital interests of you or someone else, where the relevant person is physically or legally incapable of giving consent. For example, to prevent a serious threat to your health and safety or that of others, including but not limited to instances of child abuse or neglect;
- Where the processing is necessary for reasons of public interest in the area of public health – VisitHealth may share your Personal Data where it is necessary for reasons of public interest in the area of public health. 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 wounds.
- National Security – VisitHealth may share, if required, your Personal Data with UK Government officials for national security reasons.

We also collect, use and share aggregated data such as, statistical or demographic data for any purpose. Aggregated data may derive 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.

You have the right to ask us to restrict processing of your Personal Data (including Sensitive Personal Data) and a right to object to our processing of your Personal Data (including Sensitive Personal Data) in this way, but if you do either of these, it may impact on your use of the Services and/or we may not be able to provide you with information about the Services that you have requested us to provide to you.

Non-Essential Uses

We may also use Personal Data for non-essential uses. This is on an opt-in basis. If you have opted in, you can choose to opt out at any time by contacting us as we set out at the start of this Privacy Policy.

For example, we may send you email feedback forms to complete about us or any aspect of the website and/or the Services. We may also use it to provide you, or permit selected third parties to provide you with information about goods or services we feel may interest you. We will only contact you for such purposes if you have consented to this. If you do not want us to use your Personal Data in this way, or to pass your details on to third parties for marketing purposes, please Contact Us.

WHO DO WE SHARE YOUR PERSONAL DATA WITH?

Personal information:

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 also need to share your Personal Data with other healthcare providers including diagnostic providers and laboratories to assist us in delivering the Services to you.
- 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 people 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.
- 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 (but not any medical records). If you do not consent to such use of Personal Data, please do not use the Platform.

- 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 our Terms of Use or to investigate potential breaches; and/or
  - 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.

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 purpose and only permit them to process your Personal Data for specified purpose and in accordance with our instructions.

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.

COOKIES

A cookie is a small text file that may be placed on your computer or Device when you visit the Platform. When you next visit the Platform, the cookie allows us to distinguish you from other users. There are two categories of

cookies: (a) 'persistent cookies' that remain on your computer or Device until deleted manually or automatically; and (b) 'session cookies' which remain on your computer or Device until you close your browser, when they are automatically deleted.

The cookies VisitHealth uses:

- Essential cookies are required for the operation of the Platform and without them the Platform can't operate properly.
- Performance cookies allow us to see and count the number of visitors to the Platform and what they do during their visit. We use the information from these cookies to improve the Platform's performance. The data from these cookies doesn't allow us to identify you.
- Experience cookies allow the Platform to remember your choices, which means we can personalise your experience of the Platform. Data collection by experience cookies is used by our analytics systems (including third party systems) to monitor and enhance the Platform's user-friendliness.
- Marketing cookies track and record your visits to the Platform, including but not limited to the actual pages you visit and the links you have clicked or followed. We use this data to make the content of the Platform more relevant to/for you based on what we know about you. We do share information about your activity on the Platform that is stored by these cookies with our agents, agencies and other third-party ad networks and this information can be used to advertise products to you on other sites. Any data we share is anonymous and cannot be used to identify you.

Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.

You can REFUSE cookies, by activating settings of your chosen browser(s). If you alter your browser settings to refuse cookies your access to the Platform will be restricted.

SECURITY

The importance of security for all your Personal Data including, but not limited to, Sensitive Personal Data is important 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 the 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 utmost security, including utilising several layers of firewall security and encryption of Personal Data to ensure the highest level of security.

Data Storage

The Personal Data that we collect from you may be shared with our third-party processors (who provide analytics, payment processing, information and/or other support services) which are located and/or store data in the USA. These services are all provided by organisations which are compliant with the EU-US Privacy Shield, which means that there are appropriate safeguards in place in order to protect your Personal Data. By submitting your Personal Data, you agree to this transfer, storing or processing of your Personal Data. 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.

Certain features of the Platform link to social networking. Please 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.

Security when using the Platform

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.

No data transmission over the internet can be guaranteed to be 100% secure. 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:

- A right to request access to your Personal Data and a copy of any Personal Data that we hold relating to you;
- A right to request rectification of your Personal Data;
- A right to request erasure of your Personal Data;
- A right to ask us to restrict processing of your Personal Data and a right to object to our processing of your Personal Data (but if you do either of these, 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); and
- A right to lodge a complaint about how we treat your Personal Data with the Information Commissioner's Office.
- If you wish to discuss or make a request in respect of any of the above rights, please refer to the relevant sections below or Contact Us.

Accessing Your Personal Information

We believe that patients should have access to their medical information without charge where possible, to enable patients to take a more active role in their own health future.

For access to Personal Data please Contact Us.

Right to Amend

We do not allow ANYONE to AMEND EMRs created or held by VisitHealth. We only ever allow authorised contributors (that is, VH medics and you) to 'add to' records, making an update to the information without deletion of the original record. We believe this approach is for everyone's benefit and best ensures the integrity of the information we hold. If you would like to update your medical information, please Contact Us and direct your query to a member of our Clerical Team.

VisitHealth may, in circumstances such as these, deny your request to update your record (this is a non-exhaustive list):

- Your request has not been submitted in writing and does not include a valid reason.
- VisitHealth did not create the record or original information, in which case you should contact the creator, author or originator of the records. (In the case the creator, author or originator of the record is no longer in legal operation or accessible we may be able to assist you: please clarify this in your request.)
- VisitHealth does not hold the record and/or that information may not be updated at your request but requires another party's authorisation.

HOW LONG WE KEEP PERSONAL INFORMATION

Patient Personal Data gathered during the consultation process will be retained for 30 years in line with the CQC's retention policy. Personal Data about registered users who have not used our consultation services will be deleted after 5 years of inactivity on the Platform, unless we are required to retain such information for any legal or regulatory reason.

If you agree to be added to our mailing list, we will keep your personal information for that purpose for two years after you register your interest or latest use of our Services (unless you tell us that you would like to continue hearing from us). If you advise that you do not want to be added to our mailing list or you ask to be removed, we will delete your Personal Data (aside from keeping a record that you have asked us not to send you marketing information).

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.

Accessing Information Held by Us

If you would like a copy of all of the Personal Data, we hold about you please Contact Us.

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

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.