HESSINGTON HEALTH

Privacy Notice

HESSINGTON HEALTH

Introduction

Thank you for reading our privacy notice.

We respect your privacy and are committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

This privacy notice is made up of ten sections as set out below. You can download a pdf version of the notice here – https://www.hessingtonhealth.com/privacy-notice.pdf. Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

We have also developed and implemented an internal data protection policy, designed to ensure that all of our staff are fully aware of their duties under relevant data protection legislation, and that they process your data accordingly. You can request a copy of our internal data protection policy by contacting us at GDPR@hessingtonhealth.com

INDEX

Important information and who we are

Purpose of this privacy notice

This privacy notice aims to give you information on how we collect and process your personal data, including any data you may provide to us directly via our website or otherwise.

It is important that you read this privacy notice together with any other privacy notice, fair processing notice or privacy policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

Controller

Hessington Health Limited is the controller and responsible for your personal data (collectively referred to as the Company, "we", "us" or "our" in this privacy notice).

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the data privacy manager using the details set out below.

Contact details

Our full details are:

Full name of legal entity: Hessington Health Limited

Name or title of data privacy manager: Dr Harjeev Rai, CEO and Medical Director (also the Data Controller)

Email address: hrai@hessingtonhealth.com

Postal address: 22 Crystal Court, 95 Bramley Road, London N14 4EY

Telephone number: +44(0)79 8479 1222

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.

Changes to the privacy notice and your duty to inform us of changes

This version was last updated on 24 May 2018 and historic versions can be obtained by contacting us.

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.

Third-party links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. The Standard data we collect about you

Personal data, or personal information, 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 follows:

- Identity Data
includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

- Contact Data
includes billing address, delivery address, email address and telephone numbers

- Financial Data
includes bank account and payment card details

- Transaction Data
includes details about payments to and from you and other details of products and services you have purchased from us.

- Technical Data
includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.

- Profile Data
includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

- Usage Data
includes information about how you use our website, products and services.

- Marketing and Communications Data
includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. 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 to calculate the percentage of users accessing a specific website feature. 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 notice.

3. The Special Categories of Personal Data we collect about you

We also collect Special Categories of Personal Data about you. This includes in particular your medical data and information about your health, genetic and biometric data, as well as details about your race or ethnicity, religious or philosophical beliefs, sex life, and sexual orientation. This data is required to provide you with the best treatment and care possible.

We may obtain this information from your existing employer, insurance provider, or records of medical services you have received in the past.

We may also collect information about criminal convictions and offences.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with the best medical care possible). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

4. 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:

- avail of our products or services;
- create an account on our website;
- subscribe to our service or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us some feedback.

- Direct interactions – medical data.

You may give us Special Category information about your health through your contact with us, including face-to-face (for example, in medical consultations, diagnosis and treatment) and by subscribing and accepting the terms of our Health-Port service.

- Automated technologies or interactions.

As you interact with our website, 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.

- Third parties or publicly available sources.

We may receive personal data about you from various third parties and public sources.

Special Categories of Personal Data (medical data) from relevant sources including existing health records, your GP and other medical practitioners including consultants, and your employer, including without limitation through our SMaRT Absence Management software.

- Technical Data from the following parties:

    - analytics providers;
    - advertising networks; and
    - search information providers.

- Contact, Financial and Transaction Data from providers of technical, payment and delivery services.

- Identity and Contact Data from data brokers or aggregators.

- Identity and Contact Data from publicly availably sources such as Companies House and the Electoral Register.

5. How 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:

- Where we need to perform the contract we are about to enter into or have entered into with you.

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

- Where we need to comply with a legal or regulatory obligation.

- Where it is necessary for the purposes of preventive or occupational medicine, to assess your fitness to work, and to provide medical diagnosis and health or social care or treatment.

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third-party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us at GDPR@hessingtonhealth.com.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us at GDPR@hessingtonhealth.com if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new patient	(a) Identity (b) Contact	Performance of a contract with you
To deliver medical care, diagnosis and treatment and related services to you	(a) Identity (b) Contact (c) Financial (d) Special Category (health) (e) Special category (criminal offence data)	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us) (c) consent (d) healthcare basis
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review, take a survey or provide other feedback	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers/clients use our products/services)
To enable you to complete a survey or to provide other feedback	(a) Identity (b) Contact (c) Profile (d) Usage	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how patients and clients use our products/services, to develop them and grow our business)

	(e) Marketing and Communications	
To administer and protect our business and our website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers/clients use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer/client relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers/clients for our products/services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about products/services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any company outside our group of companies for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by contacting us at GDPR@hessingtonhealth.com at any time.

Where you opt out of receiving marketing messages, this will not apply to personal data provided to us as a result of a product service purchase, warranty registration, product/service experience or other transactions.

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 you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at GDPR@hessingtonhealth.com.

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.

6. Disclosures of your personal data

We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 5.

- Internal Third Parties. These are other companies in our corporate group who may act as joint controllers or processors and who may be based inside or outside the EU.

- External Third Parties. These may include:

    - Your employer and insurance provider.
    - Service providers who may act as processors based inside or outside the EU and who provide IT, system administration and other services.
    - Professional advisers who may act as processors including lawyers, bankers, auditors and insurers based inside or outside the EU who provide consultancy, banking, legal, insurance and accounting services.
    - HM Revenue & Customs, regulators and other authorities who may act as processors based inside or outside the EU who require reporting of processing activities in certain circumstances.

- 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 notice.

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.

7. International transfers

Some of our external third parties may be based outside the European Economic Area (**EEA**) so the processing of your personal data may involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.

- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.

- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

Please contact us at GDPR@hessingtonhealth.com if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

8. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9. Data retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our patients (including Contact, Identity, Financial and Transaction Data) for at least six years after they cease being customers for tax purposes.

Details of other retention periods for different aspects of your personal data are contained in our retention policy which you can request from us by contacting us at GDPR@hessingtonhealth.com.

In some circumstances you can ask us to delete your data and in some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

10. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. Please click on the links below to find out more about these rights:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

If you wish to exercise any of the rights set out above, please contact us at:
GDPR@hessingtonhealth.com.

No fee usually required

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.

What we may need from you

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.

Time limit to respond

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.

11. Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract

Means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation

Means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Healthcare basis

Means the processing of your Special Category Personal Data relating to your health for the purposes of medical diagnosis, the provision of health care or treatment, or the management of healthcare systems.

YOUR LEGAL RIGHTS

You have the right to:

Request access

to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction

of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure

Of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing 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), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. 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.

Object to processing

Of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing

Of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer

Of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time

Where we are relying on consent to process your personal data. 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 products or services to you. We will advise you if this is the case at the time you withdraw your consent.

CONTACT

For any enquiries or for additional information contact us using our details below.

We are practicing from the following affiliated hospitals and clinics

› London
10 Harley Street
London
W1G 9PF

› Spire Bushey Hospital
Heathbourne Road
Bushey, Hertfordshire
WD23 1RD

› BMI Cavell Hospital
Cavell Drive
Uplands Park Road
Enfield
EN2 7PR

› BMI Shelburne Hospital
Queen Alexandra Road
High Wycombe
Bucks
HP11 2TR

› Warwickshire Nuffield Hospital
The Chase, Old Milverton Lane
Leamington Spa, Warwickshire
CV32 6RW

Contact Details
Telephone: +44 (0) 8000 886 418
Email: info@hessingtonhealth.com

Address
Hessington Health Ltd
22 Crystal Court
95 Bramley Road
London, N14 4EY

Website
www.hessingtonhealth.com

For new business opportunities
sales@hessingtonhealth.com

Dr H Rai CEO Hessington Health Ltd, 22 Crystal Court, 95 Bramley Road, London, N14 4EY