LutraHealth.

Privacy Notice

Last updated: November 2024

Your privacy, and the security of the data you share with us is the most important part of our business. We want you to know why we need your data, and what we do with it. Our privacy policy defines why we need your data, and how we look after it.

1) Who are we?

We are Lutra Health Ltd. Our registered office is 2 Oldfield Road, Bocam Park, Bridgend, CF35 5JL. Our company number is 13409714 (Lutra Health, we, us).

Lutra Health is a private company, based in the UK, which specialises in developing apps to help healthcare workers provide efficient and safe care for patients.

We are registered with the Information Commissioners Office to process personal and special categories of information under the Data Protection Act (2018), our registration number is A9028898.

For further information, please see our website www.lutrahealth.com

2)Why do we collect personal information about you?

We collect information about you in order to transmit it to other healthcare professionals who will then be able to make decisions about your care. We do not alter, adjust or interfere with the data that you or healthcare professionals give us.

3) What personal information do we need to collect about you and how do we obtain it?

Personal data means any information about an individual from which that person can be identified. We may collect, use, store and transfer different

kinds of personal data about you which we have grouped together as below. This will assist us to make decisions about your care we need:

- Identity Data includes names, marital status, date of birth;
- Contact Data includes postal and email addresses and telephone numbers;
- Financial Data includes bank and payment card details;
- Transactional Data includes information about any services received 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, device ID and other technology on the devices you use to access our platform or website;
- Profile Data includes any username, password, interests, preferences and feedback;
- Usage Data includes information about how you interact with our platform, website or services;
- Marketing and Communication Data includes your preferences in receiving marketing from us and our third parties and your communication preferences
- The organisation name of your Optometrist practice
- Demographic data – typically supplied by the patient/their carer and the examining Optometrist
- Clinical data – typically supplied by the examining Optometrist
- Medical history data – typically supplied by the patient/their carer

We do not require or collect data relating to:

- Your race or religion
- Your sexual orientation

4) How is your personal data collected?

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

- Your interactions with us. You may give us your personal data by filling in online forms or by corresponding with us by post, phone, email or otherwise.

- Automated technologies or interactions. As you interact with our platform and/or website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies.
- Third parties or publicly available sources. We will receive personal data about you from various third parties as set out below:
    - Optometrists
    - Hospitals
    - Healthcare professionals
- Identity and Contact Data is collected from healthcare professionals, data brokers or aggregators.

5) How we use your personal data

Legal basis

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- **Performance of a contract with you:** Where we need to perform the contract we are about to enter into or have entered into with you.
- **Legitimate interests**: We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) 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).

- **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.

- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if you subscribe to an email newsletter.

We have set out below, in a table format, a description of all the ways we plan to use the various categories of 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:

Purpose/Use	**Type of data**	**Legal basis**
To register you as a new customer or user	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver our services to you including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Dealing with your requests, complaints and queries	(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 manage our relationship with you)
To administer and protect our business and this 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 online 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 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, customer relationships and experiences and to measure the effectiveness of our communications and marketing	(a) Technical (b) Usage	Necessary for our legitimate interests (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)
To send you relevant marketing communications and make personalised suggestions and recommendations to you about goods or services that may be of interest to you based on your Profile Data	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests (to carry out direct marketing, develop our products/services and grow our business)
To carry out market research through your voluntary participation in surveys		Necessary for our legitimate interests (to study how customers use our products/services and to help us improve and develop our products and services).

Special Categories of data

Where we process special categories data, for example data concerning/ including health, racial or ethnic origin, or sexual orientation, we need to

meet an additional condition in the GDPR. Where we are processing special categories personal data for purposes related to the commissioning and provision of health services the condition is:

Purpose	**Type of Data**	**Legal Basis**	**Processing condition for special categories of personal data**
For the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	Data concerning health	a) Necessary Performance of a contract with you; b) Consent c) Necessary to comply with a legal obligation	a) Explicit Consent b) Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with health or social care. (Paragraph 2, Schedule 1, DPA 2018.)

6) What we may do with your personal information

The personal data we collect about you may also be used to:

- Remind you about your appointments and send you relevant correspondence.
- Review the way we provide information to healthcare organisations to ensure it is of the highest standard and quality.

- Prepare statistics on our performance to meet the needs of our customer.
- Help to train and educate healthcare professionals.
- Report and investigate complaints, claims and untoward incidents.
- Report events to the appropriate authorities when we are required to do so by law.
- Review your suitability for research study or clinical trial.
- Contact you with regards to patient satisfaction surveys relating to our services so as to further improve our services to patients.
- Where possible, we will always look to anonymise/ pseudonymise your personal information so as to protect patient confidentiality, unless there is a legal basis that permits us to use it and we will only use/ share the minimum information necessary.

7) Who do we share your data with?

We may share your personal data where necessary with the parties set out below for the purposes identified in section 5 above:

- Internal third parties
- External Healthcare organisations and providers
- Legal professionals
- Care quality commission
- Public bodies such as but not limited to HMRC
- 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

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.

8) International Transfers

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK to countries which have laws that do not provide the same level of data protection as the UK law.

Whenever we transfer your personal data out of the UK to service providers, we ensure a similar degree of protection is afforded to it by ensuring that the following safeguards are in place:

- We will only transfer your personal data to countries that have been deemed by the UK to provide an adequate level of protection for personal data; or
- We may use specific standard contractual terms approved for use in the UK which give the transferred personal data the same protection as it has in the UK.

9) Data Security and how we maintain your data

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.

Your data is held securely on AWS (Amazon Web Services) cloud servers, which achieve the relevant security for healthcare records. AWS is the international gold standard for cloud based data storage as documented here and upheld by AWS's customer contract terms.

10) Links to other websites or services

Our Service may contain links to other websites that are not operated by Us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

11) Marketing

Direct Marketing

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us and you have not opted out of receiving the marketing.

We may also analyse your Identity, Contact, Technical, Usage and Profile Data to form a view which products, services and offers may be of interest to you so that we can then send you relevant marketing communications.

Third-party marketing

We will get your express consent before we share your personal data with any third party for their own direct marketing purposes.

Opting out of marketing

You can ask to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us.

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes

12) Cookies

For more information about the cookies we use and how to change your cookie preferences, please see lutrahealth.com/app/cookie-policy

13) Changes to our privacy policy

We may update our Privacy Policy from time to time. We will let you know via email, a prominent notice on our service or by requesting that you read and accept the new Privacy notice before allowing access to our service. The change will become effective and when the “Last updated” date at the top of this Privacy Policy is published.
You are advised to review this Privacy Policy periodically for any changes.

14) Retention of your personal data

We will retain your data as described in our data retention policy.

In general terms we retain data for adults for eight years after the last point at which the data was accessed. We retain data destruction certificates for twenty years.

15) How do we transmit your data?

When we are required to send your personal data using either email or delivery within the app, we cannot guarantee the security of your data if it is sent by email. We will only use email to transfer your personal data when this has been requested by the
receiving organisation (for example the NHS). We are not responsible for any personal data processing which occurs after we have sent the information to the receiving healthcare organisation, and you should refer to that organisations data protection policies for information on how they will use the data we supply.

16) What are your legal rights?

If we need to use your personal information for any reasons beyond those stated above, we will discuss this with you and ask for your explicit consent. The Data Protection Act 2018 gives you certain rights, including the right to:

- Request access to the personal data we hold about you, e.g. in health records (commonly known as a “subject access request”). This enables you to receive a copy of the personal data that we hold about you and to check that we are lawfully processing it.

- Request the correction of inaccurate or incomplete information recorded in our health records, subject to certain safeguards. 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 in certain circumstances. 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, 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) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.

- Withdraw consent at any time where we are relying on consent to process your personal data (see the table in section 5 for details of when we rely on your consent as the legal basis for using your 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.

- 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.

- Choose if data from your health records is shared for research and planning purposes.

- In certain circumstances you may have the right to 'object' to the processing (i.e. sharing) of your information where the sharing would be for a purpose beyond your care and treatment (e.g. to plan and improve health and care services, to research and develop cures for serious illness).

- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:

    - If you want us to establish the data's accuracy;
    - Where our use of the data is unlawful but you do not want us to erase it;
    - 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
    - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it

- If you wish to exercise any of these rights in relation to your data please contact us at iris@lutrahealth.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 could 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 could 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.

17) How can I contact you to discuss my data?

Please email us at "iris@lutrahealth.com" to discuss any questions you may have about how we collect, store and use your data.

18) Complaints and contacting the Information Commissioner

The Information Commissioner's Office (ICO) is the body that regulates the Trust under Data Protection and Freedom of Information legislation. https://ico.org.uk/. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the ICO at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510
Email: casework@ico.org.uk