PatientGO – Privacy Policy

Illingworth Research Group Limited have been asked by the clinical trial sponsor/their nominated third party to facilitate your clinical trial (**Clinical Trial**) travel, accommodation and/or expenses as part of the Clinical Trial. In order to do this, we must collect, store and share your personal information, making us the "data processor". This means that we hold and use personal data about you.

This policy sets out how we collect and use personal information about you to facilitate the travel, accommodation and expense reimbursement Service (also known as PatientGO), in accordance with the General Data Protection Regulation (GDPR) and data protection legislation. This policy applies only to participants, who will use the Service. The personal data provided to us during your use of the App is separate and independent from the Clinical Trial data as outlined in your consent documentation, with the Clinical Trial sponsor/their nominated third party.

Please read the following carefully, to understand our practices regarding your personal data and how we will use it in respect of the App, and your use of the Service.

Consent to installation of the App

Under data protection laws, we are required to provide you with certain information about who we are, how we process your personal data and for what purposes, and your rights in relation to your personal data.

By installing the App, you are indicating your consent to our processing of your personal and Special Category data (such as your name, contact details, passport details, financial and medical information for example) as described in this policy.

How you can withdraw consent

You may change your mind and withdraw consent at any time by contacting us PatientGO@illingworthresearch.com but that will not affect the lawfulness of any processing carried out before you withdraw your consent. Please note that withdrawing your consent may affect our ability to carry out any requests you have made within the App, such as expense reimbursements for example.

Introduction

This policy (together with our end-user licence agreement as set out at https://illingworthresearch.com/patientgo-terms (**EULA**) and any additional terms of use incorporated by reference into the EULA, together our **Terms of Use**) applies to your use of:

- PatientGO Version 1 mobile application software (**App**) available on both Google Play and the Apple Store. Once you have downloaded or streamed a copy of the App onto your mobile telephone or handheld device (**Device**).

- The PatientGO service accessible through the App (**Services**) that is available on the App Site or other sites of ours (**Services Sites**). This policy sets out the basis on which any personal data (including Special Category data) we collect from you, or that you provide to us, will be processed by us.

- This App is not intended for use by children (a "Child" is anyone under the age of 18) and where the participant of the Clinical Trial is a Child who wishes to use the App and Service, the App is made available and the Services provided only where the person holding parental responsibility of the Child is the User of the App. Please read the following carefully to understand our practices regarding your personal data (including Special Category data) and how we will treat it.

This policy is provided in a layered format with sections relating to the following:

[IMPORTANT INFORMATION AND WHO WE ARE]

[THE DATA WE COLLECT ABOUT YOU]

[HOW IS YOUR PERSONAL DATA COLLECTED?]

[HOW WE USE YOUR PERSONAL DATA]

[DISCLOSURES OF YOUR PERSONAL DATA]

[INTERNATIONAL TRANSFERS]

[DATA SECURITY]

[DATA RETENTION]

[YOUR LEGAL RIGHTS]

[GLOSSARY]

[DESCRIPTION OF CATEGORIES OF PERSONAL DATA]

Important information and who we are

Illingworth Research Group Limited is the controller and is responsible for your personal data (collectively referred to as "Illingworth", "we", "us" or "our" in this policy).

If you have any questions about this privacy policy, please contact us using the details set out below.

Contact details

Our full details are:

- Full name of legal entity: Illingworth Research Group Limited
- Email address: PatientGO@illingworthresearch.com
- Postal address: Suite 5, Silk House, Park Green, Macclesfield, Cheshire, SK11 7QJ, United Kingdom

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 or other competent supervisory authority of an EU member state if the App is downloaded outside the UK.

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

We keep our privacy policy under regular review. This version was last updated on 23 June 2020.

We reserve the right to update this Privacy Policy at any time, without prior notice. We encourage you to regularly check the Privacy Policy for any changes.

It is important that the personal and Special Category data we hold about you is accurate and current. Please keep us informed if there are any changes during our relationship with you.

The data we collect about you

We may collect, use, store and transfer different kinds of personal data about you as follows:

- Identity Data.

- Contact Data.
- Financial Data.
- Transaction Data.
- Device Data.
- Content Data.
- Profile Data.
- Usage Data.
- Special Category Data.

We explain the categories of personal data here [LINK TO DESCRIPTION OF CATEGORIES OF PERSONAL DATA BELOW] and we explain what **Special Category** data is, below.

Special Category data

We collect Special Categories of Personal Data about you (this may include details about your race or ethnicity, religious or philosophical beliefs and information about your health). We will only collect and process special Category Data when it is specifically required in order to fulfil any requests you make within the App, such as travel or accommodation arrangements.

How is your personal data collected?

We will collect and process the following data about you:

- **Information you give us.** This is information (including Identity, Contact and Financial Data) you consent to giving us about you by filling in forms on the App Site and the Services Sites (together **Our Sites**), or by corresponding with us (for example, by email or chat). It includes information you provide when you register to use the App Site, download or register an App, subscribe to our Service, search for an App or Service, and when you use the App to facilitate travel and accommodation requests, reimburse expenses, report a problem with an App, our Services, or any of Our Sites. If you contact us, we will keep a record of that correspondence.
- **Information we collect about you and your device.** Each time you visit one of Our Sites or use one of our Apps we will automatically collect personal data including Device, Content and Usage Data. We collect this data using cookies and other similar technologies. Please see our cookie policy [LINK TO COOKIE POLICY] for further details.
- **Information we receive from other sources including third parties and publicly available sources**. We will receive personal data about you from various third parties as set out below:
    - Identity and Contact Data from the trial sponsor or their nominated third party based who may be based inside **OR** outside the UK.

Cookies

We use cookies and/or other tracking technologies to distinguish you from other users of the App, App Site, the distribution platform (Appstore) or Services Sites and to remember your preferences. This helps us to provide you with a good experience when you use the App or browse any of Our Sites and also allows us to improve the App and

Our Sites. For detailed information on the cookies we use, the purposes for which we use them and how you can exercise your choices regarding our use of your cookies, email PatientGO@illingworthresearch.com.

How we use your personal and Special Category data

We will only use your personal data when the law allows us to do so. Most commonly we will use your personal data in the following circumstances:

- Where you have consented before the processing.
- Where we need to perform a contract we are about to enter or have entered 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.

Click here [*LINK TO GLOSSARY: LAWFUL BASIS*] to find out more about the types of lawful basis that we will rely on to process your personal data.

Purposes for which we will use your personal and Special Category data

Purpose/activity	**Type of data**	**Lawful basis for processing**
To install the App and register you as a new App user	Identity Contact Financial Device	Your consent Performance of a contract with you Necessary for our legitimate interests (to reimburse your expenses)
To process in-App requests and deliver Services including managing requests for travel/accommodation and fulfilling reimbursement requests.	Identity Contact Financial Transaction Device Location Special Category data	Your consent Performance of a contract with you Necessary for our legitimate interests (to reimburse your expenses)
To manage our relationship with you including notifying you of changes to the App or any Services	Identity Contact Financial Profile	Your consent Performance of a contract with you Necessary for our legitimate interests (to keep records updated and to analyse how customers use our Services) Necessary to comply with legal obligations (to inform you of any changes to our terms and conditions)
To administer and protect our business and this App including	Identity Contact	Necessary for our legitimate interests (for running our

troubleshooting, data analysis and system testing	Device	business, provision of administration and IT services, network security)

Disclosures of your personal data

When you consent to providing us with your personal and Special Category data, we will also ask you for your consent to share your personal data with the third parties set out below for the purposes set out in the table above:

- Internal Third Parties as set out in the *Glossary*.
- External Third Parties as set out in the *Glossary*.
- 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 and Special Category data in the same way as set out in this privacy policy.

International transfers

Many of our external third parties are based outside the UK so their processing of your personal data will involve a transfer of data outside the UK.

Whenever we transfer your personal data out of the UK, 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 Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

Data security

All information you provide to us is stored on our secure servers. Information stored “at rest” on our secure servers is protected using industry standard data encryption. Where we have given you (or where you have chosen) a password that enables you to access certain parts of Our Sites, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Once we have received your information, we will use strict procedures and security features to try to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way. Data being transmitted between you as the User (**End User**) and Illingworth as part of the Service is protected using industry standard encryption methods. Data stored on our servers is protected using encryption at rest and state of the art firewalls to prevent unauthorised access.

No personally identifiable data is stored on the End User device. Two encrypted tokens are stored on the End User device to facilitate ease of login.

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

Data retention

By law we have to keep basic information about you (including Contact, Identity, Financial and Transaction Data) for seven years after you're the completion of the Clinical Trial for financial audit purposes.

In some circumstances you can ask us to delete your data: see [*Your legal rights*] below for further information.

In some circumstances we will 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.

Your legal rights

Under certain circumstances you have the following 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 or your personal data*.]
- [*Right to withdraw consent*.]

You can exercise any of these rights at any time by contacting us at Suite 5, Silk House, Park Green, Macclesfield, Cheshire, SK11 7QJ, United Kingdom **OR** PatientGO@illingworthresearch.com

Glossary

Lawful basis

Consent means processing your personal data where you have signified your agreement by a statement or clear opt-in to processing for a specific purpose. Consent will only be valid if it is a freely given, specific, informed and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

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

Third parties

Internal third parties

Other companies in the Illingworth Group acting as joint controllers or processors and who are based in Spain, France, Italy, Australia and the United States of America and provide IT and system administration services and undertake leadership reporting.

External third parties

Service providers acting as processors who provide IT and system administration services.

Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.

Service providers acting as processors who provide travel, accommodation and transportation to you as part of the Services.

HM Revenue and Customs, regulators and other authorities acting as processors or joint controllers base in the UK who require reporting of processing activities in certain circumstances.

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. 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.

Description of categories of personal data

- **Identity Data**: first name, last name, maiden name, username or similar identifier, marital status, title, date of birth, gender, passport information including number, name, country of issue and expiry date.
- **Contact Data**: home address, email address, telephone numbers and emergency contact details.
- **Financial Data**: bank account and payment card details.
- **Transaction Data**: includes details about payments to you and details of in-App requests.
- **Device Data:** includes the type of mobile device you use, a unique device identifier (for example, your Device's IMEI number, the MAC address of the Device's wireless network interface, or the mobile phone number used by the Device),] mobile network information, your mobile operating system, the type of mobile browser you use, and time zone setting information.
- **Content Data:** includes information stored on your Device, including photos, videos or other digital content;
- **Profile Data**: includes your username and password, in-App request history, your preferences and feedback.
- **Usage Data**: includes details of your use of any of our Apps or your visits to any of Our Sites including, but not limited to, traffic data and other communication data, whether this is required for our own billing purposes or otherwise and the resources that you access.

Special Category data

This will include any information you provide to us specifically related to a request you make within the App (such as a request for transport, or accommodation), and may include details about your race or ethnicity, religious or philosophical beliefs and information about your health.