

Privacy Policy – Study Participants

About this Policy

This privacy policy explains how Research Path Pty Ltd (ABN 62 124 637 163, “Research Path”, “we”, “us”, or “our”) uses the personal data we collect from you when you participate in a clinical study that utilises our software. Research Path acts as a data processor on behalf of the study sponsor (the “Data Controller”) in accordance with applicable data protection laws, including the EU General Data Protection Regulation (GDPR), the UK GDPR, the Australian Privacy Act 1988 (Cth), and relevant clinical trial regulations.

This privacy policy supplements, but does not replace, the study-specific participant information and Informed Consent Form (ICF) provided to you at your enrolling hospital or clinic. Please refer to your ICF for detailed information about the specific data collected in your study and the identity of the Data Controller (study sponsor). If there is any inconsistency between this policy and your ICF, the ICF shall prevail in respect of study-specific matters.

What data do we collect and why?

Research Path collects the following data as instructed by, and on behalf of, the Data Controller (study sponsor). The data we hold is pseudonymised: your full name is not stored in Research Path systems, and identification is limited to coded identifiers that cannot be used to directly identify you without additional information held separately by your clinical site. The only exception is a data-linkage identifier collected with your additional consent, as described below.

- Personal identification information (limited to date of birth, sex, initials, and a unique study participant code)
 - On occasion, studies may request consent to collect data linkage information such as your Medicare number (Australia only) or an ID for another study or registry, to support data sharing amongst projects or organisations that participants have consented to sharing information with. In this case, additional informed consent will be obtained.
- Health information and clinical data as required by the study you have consented to (special category data under GDPR Article 9), which may include:
 - hospital or clinic name where you were enrolled
 - hospital admission and other clinical event dates and times
 - surgical or other medical intervention monitoring data
 - blood and other laboratory test results
 - quality of life surveys and/or other validated questionnaires
 - adverse event data during admission
 - follow-up status after hospital discharge, such as mortality, hospital readmissions, and quality of life questionnaires
 - where the study uses these services, your randomised treatment allocation and the study medication assigned to you
- Documents uploaded by your study site to support the study records (for example, copies of test results). Sites are asked to remove identifying information before uploading, and any uploaded document that shows identifying information is deleted.

How do we collect your data?

The hospital clinical research nurse or staff member at the hospital or clinic where you consented to the study will directly provide Research Path with all of the data we collect. These data are only entered into our system once you have provided informed consent to study participation in accordance with applicable clinical trial regulations (including ICH Good Clinical Practice guidelines and, where applicable, EU Clinical Trial Regulation No 536/2014). Research Path does not collect data directly from you.

Some clinical studies may involve participants under the age of 18. Where a study involves minors, consent for the collection and processing of their personal data is provided by a parent or legal guardian in accordance with applicable laws, the study-specific ICF, and the requirements of the approving ethics committee. Where appropriate, the minor's assent is also obtained. Research Path applies the same technical and organisational safeguards to children's data as to all participant data, and does not process children's data for any purpose other than those described in this policy.

How will we use your data?

Research Path collects your data so that we can:

- provide clean and validated datasets to the researchers who manage the study;
- where the study uses these services, randomly allocate you to a study treatment group and manage the assignment of study medication; and
- provide the hospital or clinic where you enrolled with aggregate statistics to monitor the progress of their study participation and management.

Research Path has no rights to share, analyse, or retain your data for any purpose other than to provide these services to the study sponsor, including the monitoring information and the interim and final datasets. Your data will not be used for automated decision-making or profiling. Research Path does not use your data for any secondary purpose. Any further use of your data by the study sponsor is described in your ICF.

Legal basis for processing

As Data Controller, the study sponsor determines the legal basis for processing your personal data. Research Path processes your data only on the sponsor's documented instructions, under a Data Processing Agreement (GDPR Article 28).

Where the GDPR or UK GDPR applies, the legal bases commonly used for clinical trials, as described by the European Data Protection Board in [Opinion 3/2019](#), are:

Safety and reliability obligations: processing necessary to comply with legal obligations under clinical trial law, such as safety reporting and archiving (Article 6(1)(c)), together with reasons of public interest in the area of public health (Article 9(2)(i)).

Research activities: processing necessary for a task carried out in the public interest (Article 6(1)(e)) or for the sponsor's legitimate interests (Article 6(1)(f)), together with scientific research purposes (Article 9(2)(j)) or public interest in the area of public health (Article 9(2)(i)), subject to appropriate safeguards including pseudonymisation, data minimisation, and ethics committee approval. In some studies the sponsor may instead rely on your explicit consent (Articles 6(1)(a) and 9(2)(a)).

The informed consent you give to take part in a clinical trial is required by clinical trial law and is separate from consent as a legal basis under the GDPR. The specific legal basis that applies to your study will be identified in the participant information provided by your study site or the sponsor.

Under Australian law, the handling of health information in research is governed by the Privacy Act 1988 (Cth) and the guidelines approved under section 95A of that Act.

How do we store your data?

Research Path securely stores your data in Google Cloud Platform (GCP) data centres in Australia: the primary database is in Sydney, and encrypted backups are kept in Melbourne. Your data is encrypted at rest (AES-256) and in transit (TLS 1.2 or higher). Access to study systems is controlled by role-based authorisation, and multi-factor authentication is enabled by default. Access to the underlying data by Research Path staff is limited to designated staff who need it to provide the service. All access to physical infrastructure used to store your data is under strict controls managed by Google.

For further information on Google Cloud Platform's security and compliance certifications, see: <https://cloud.google.com/security/gdpr>

Research Path holds ISO/IEC 27001 certification for its information security management system.

Changes to study data are recorded in an audit trail. Audit trails are maintained in compliance with ICH Good Clinical Practice guidelines and applicable regulatory requirements, and are available for review by authorised parties including sponsors, ethics committees, and regulatory authorities during monitoring visits, audits, and inspections.

Research Path maintains validated computerised systems in accordance with ICH GCP, FDA 21 CFR Part 11, and applicable regulatory requirements for electronic records and electronic signatures. System qualification documentation is maintained separately and is available to sponsors and regulatory authorities upon request.

International data transfers

Your data is stored in Australia in Google Cloud Platform data centres. Australia does not currently hold a data adequacy decision from the European Commission. Where your data originates from a clinical trial conducted within the European Economic Area (EEA) or the United Kingdom, the following safeguards are in place to ensure your data is protected to an equivalent standard:

- Standard Contractual Clauses (SCCs) approved by the European Commission and, for UK data, the UK International Data Transfer Agreement or Addendum, are incorporated into our Data Processing Agreements with study sponsors and into Google Cloud Platform's data processing terms as our infrastructure sub-processor
- A Transfer Impact Assessment (TIA) has been conducted to evaluate the legal framework in Australia and confirm that adequate protections are in place for personal data transferred from the EEA
- Technical measures including encryption in transit and at rest, and strict access controls, provide supplementary safeguards as recommended by the European Data Protection Board

Research Path staff who access data are located in Australia. Our error-monitoring and session-diagnostics sub-processors (Rollbar and LogRocket) are based in the United States and may receive limited technical data that can include study data (see Sub-processors). These transfers are covered by Standard Contractual Clauses and, where the provider is certified, the EU-US Data Privacy Framework (and its UK Extension). In the event that access from an additional jurisdiction is required (for example, to provide technical support), the same contractual and technical safeguards will be applied, and the study sponsor will be notified.

Data retention

Research Path keeps your data for as long as the study sponsor instructs. During the study, your data is held in the live study database. When Research Path's service for the study ends, the study data is either returned to the sponsor or archived in encrypted cloud storage in Australia for the retention period the sponsor requires (15 years by default). When that period expires, the archived data is automatically and permanently deleted.

The retention period is set by the sponsor according to the regulatory requirements governing your study, and may include:

- a minimum of 15 years for most clinical trials conducted in Australia, under the NHMRC framework for the responsible conduct of research
- at least 25 years after the end of the trial for clinical trials of medicinal products conducted under the EU Clinical Trials Regulation ([Regulation \(EU\) No 536/2014, Article 58](#))
- any longer period required by the study sponsor, applicable national legislation, or the relevant ethics committee

ICH E6(R3) Good Clinical Practice requires essential records to be retained for the period required by applicable regulatory requirements. The longest applicable period will be followed.

What are your data protection rights?

Research Path would like to make sure you are fully aware of all of your data protection rights. Because the study sponsor is the Data Controller, requests to exercise your rights are handled by the sponsor, usually through your study site. Research Path does not hold your name, so we cannot identify you without your study site's help. If you contact us, we will pass your request to the sponsor without undue delay and help the sponsor respond to it. Depending on the law that applies to your study, you may be entitled to the following:

The right to access: You have the right to request copies of your personal data.

The right to rectification: You have the right to request that any information you believe is inaccurate be corrected, and that information you believe is incomplete be completed.

The right to erasure: You have the right to request that your personal data be erased, under certain conditions. Please note that in clinical trials, erasure may be limited by regulatory obligations requiring data retention for patient safety and scientific integrity.

The right to restrict processing: You have the right to request that the processing of your personal data be restricted, under certain conditions.

The right to object to processing: Where processing is based on public interest or legitimate interests, you have the right to object to the processing of your personal data, under certain conditions.

The right to data portability: Where processing is based on your consent, you have the right to request that the data collected about you be transferred to another organisation, or directly to you, in a structured, commonly used, and machine-readable format.

The right to withdraw consent: Where processing is based on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal. Please note that in the context of clinical trials, withdrawal from the study does not require deletion of data already collected where retention is required by law or regulatory obligation.

Rights related to automated decision-making: Research Path does not use your personal data for automated decision-making or profiling.

Under the GDPR, the Data Controller must respond to your request within one month. In complex cases, this period may be extended by a further two months, in which case you will be told within the first month. If you would like to exercise any of these rights, please contact your study site, or contact us at compliance@researchpath.com.au or our Data Protection Officer (see below).

Data breach notification

In the event of a personal data breach that affects your data, Research Path will:

- notify the Data Controller (study sponsor) without undue delay after becoming aware of the breach, within the timeframe agreed in our Data Processing Agreement, so that the sponsor can meet its own notification obligations, including the 72-hour deadline for notifying supervisory authorities under GDPR Article 33
- cooperate with the Data Controller to notify the relevant supervisory authority where the breach is likely to result in a risk to your rights and freedoms
- cooperate with the Data Controller to notify you directly where the breach is likely to result in a high risk to your rights and freedoms, in accordance with GDPR Article 34
- document all breaches, including the facts, effects, and remedial actions taken, regardless of whether notification to the supervisory authority is required
- where the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth) applies, ensure that the Australian Information Commissioner and affected individuals are notified, by Research Path or by the sponsor as agreed between us
- meet the breach notification requirements of any other jurisdiction that applies to your study

Regulatory authority access

As part of your participation in a clinical study, your pseudonymised data may be accessed by authorised representatives of the following parties for the purposes of monitoring, auditing, and inspection in accordance with ICH Good Clinical Practice guidelines and applicable clinical trial regulations:

- the study sponsor and their authorised delegates (including monitors and auditors)
- independent ethics committees or institutional review boards overseeing the study

- regulatory authorities including, but not limited to, the Australian Therapeutic Goods Administration (TGA), the European Medicines Agency (EMA), national competent authorities in EU/EEA member states, the UK Medicines and Healthcare products Regulatory Agency (MHRA), Health Canada, and the United States Food and Drug Administration (FDA)

These parties are bound by confidentiality obligations and may only access your data to the extent necessary to verify the integrity of the clinical trial and protect your safety. Your consent to this access is obtained as part of the study-specific ICF.

Sub-processors

Research Path engages the following sub-processors in the delivery of its services:

- **Google Cloud Platform (Google LLC):** Provides the cloud infrastructure (compute, storage, networking, and managed database services) on which Research Path is hosted. Data is stored in the Sydney, Australia region (australia-southeast1), with backups in the Melbourne, Australia region (australia-southeast2). Google's data processing terms, security certifications, and GDPR compliance documentation are available at cloud.google.com/terms/data-processing-addendum.
- **Microsoft 365 (Microsoft Corporation):** Document and file storage. May hold exported copies of de-identified study datasets. Data is stored in Australia.
- **Zoho Mail and Zepeto (Zoho Corporation):** Project email, and system notification emails (such as password resets and study notifications) sent to study staff. These emails may occasionally contain minimal study information. Data is stored in Australia.
- **Rollbar (Rollbar Inc., United States):** Application error monitoring. Error reports may contain limited technical data from the screen or request on which an error occurred.
- **LogRocket (LogRocket Inc., United States):** Session diagnostics for study staff using the system, used to investigate and resolve technical issues.

A Data Processing Agreement is in place with each sub-processor, incorporating Standard Contractual Clauses where they are required for international transfers. Research Path will not engage additional sub-processors without authorisation from the Data Controller (study sponsor) in accordance with the terms of the applicable Data Processing Agreement. Depending on the agreement, this may require prior written consent or general written authorisation with a right to object to changes. An up-to-date list of sub-processors is available upon request by contacting compliance@researchpath.com.au.

What are cookies?

Cookies are small text files placed on your device by a website, for example to keep you signed in. For further information, visit allaboutcookies.org.

How do we use cookies?

Study participants do not use Research Path systems directly, so no cookies are placed on your device by Research Path. Our systems use cookies for a single purpose: to keep clinical research staff securely signed in. No personal data is stored in cookies. We do not use cookies for analytics, advertising, or tracking purposes. Only strictly necessary session cookies are used, and no consent is required for these under the EU ePrivacy Directive.

Privacy policies of other websites

At times Research Path software websites contain links to other websites. Our privacy policy applies only to our software, so if you click on a link to another website, you should read their privacy policy.

Changes to our privacy policy

Research Path keeps its privacy policy under regular review and places any updates on this web page. Where changes are material, we will notify the Data Controller (study sponsor), who may in turn inform participants. This privacy policy was last updated in October 2026.

Data Protection Officer

Research Path has appointed a Data Protection Officer (DPO) who is responsible for overseeing our data protection strategy and ensuring compliance with applicable data protection laws. You may contact our DPO directly with any questions or concerns regarding the processing of your personal data:

Data Protection Officer
Research Path Pty Ltd
Email: dpo@researchpath.com.au

EU and UK GDPR Representatives

As Research Path is established outside the European Economic Area and the United Kingdom, we have appointed the following representatives in accordance with GDPR Article 27 and UK GDPR Article 27 respectively:

EU GDPR Representative

Instant EU GDPR Representative Ltd

Adam Brogden

Email: contact@gdprlocal.com

Tel: +353 1 554 9700

Office 2, 12A Lower Main Street, Lucan, Co. Dublin, K78 X5P8, Ireland

UK GDPR Representative

GDPR Local Ltd

Adam Brogden

Email: contact@gdprlocal.com

Tel: +44 1772 217 800

1st Floor Front Suite, 27–29 North Street, Brighton, BN1 1EB, United Kingdom

How to contact us

If you have any questions about Research Path's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.

Email us at: compliance@researchpath.com.au

Research Path Pty Ltd
Room 5, 233 Barker St, Castlemaine Victoria 3450, Australia
ABN: 62 124 637 163

How to contact the appropriate authority

Should you wish to make a complaint, we recommend first contacting your study site or the study sponsor. If you feel that your concern has not been addressed in a satisfactory manner, you may contact the relevant supervisory authority:

- **Australia:** Office of the Australian Information Commissioner (OAIC), www.oaic.gov.au, phone 1300 363 992
- **European Union:** the data protection authority in the EU/EEA member state where you are located or where the alleged infringement occurred. A list of EU data protection authorities is available at edpb.europa.eu
- **United Kingdom:** Information Commissioner's Office (ICO), ico.org.uk
- **Switzerland:** Federal Data Protection and Information Commissioner (FDPIC), www.edoeb.admin.ch
- **New Zealand:** Office of the Privacy Commissioner, www.privacy.org.nz
- **Canada:** Office of the Privacy Commissioner of Canada, www.priv.gc.ca, or the privacy commissioner of your province
- **Hong Kong:** Office of the Privacy Commissioner for Personal Data (PCPD), www.pcpd.org.hk

References

- Privacy Act 1988 (Cth)
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- UK GDPR
- Regulation (EU) No 536/2014 (Clinical Trials Regulation)
- EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation and the GDPR
- ICH E6(R3) Guideline for Good Clinical Practice
- Australian Code for the Responsible Conduct of Research, 2018 (NHMRC)

Document Control

Last Review Date	October 2026
Next Scheduled Review	October 2027
Document Owner	Technical Director (Adam Meehan)
Review Trigger Events	A change to sub-processors or to where data is hosted or accessed from; a change to applicable data protection or clinical trial legislation or regulator guidance; studies with participants in a new jurisdiction; a change to the Data Protection Officer or the EU or UK representatives; findings from a data breach, audit or inspection.