Policy Number:	**POL-PO-003**
Policy Title:	**Privacy**
Effective Date:	**29 Nov 2024**
Authored by **Signature and Date:**	**Quality Assurance Lead Consultant** ***Signature on File***
Reviewed by **Signature and Date:**	**Legal Consultant** ***Signature on File*** **Director, Clinical Operations** ***Signature on File***
Approved by **Signature and Date:**	**Founder and Director** ***Signature on File***

1. Purpose

The purpose of this Privacy policy is to describe how Alithia Life Sciences Pty Ltd (hereinafter referred to as Alithia) collects and uses Personal Information, in the course of business activities, in compliance with applicable data protection regulations including the Australian Commonwealth Privacy Act (1988). To the extent possible and where applicable, Alithia endeavours to address and accommodate General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) requirements.

Alithia is committed to safeguarding the privacy of all clients, vendor partners, stakeholders, Investigational sites, clinical trial participants and staff, by ensuring that Personal Information required or disclosed to Alithia is protected.

2. Scope

This policy applies to all Alithia staff [1] when managing Personal Information requested by, or disclosed to Alithia by any party, including but not limited to Alithia job applicants, Clients, Vendors, Investigational Sites and any parties enquiring via the Alithia Website "Contact Us" page.

This policy includes how Alithia collects, stores, uses, shares, transfers and deletes Personal Information.

Personal Information is defined as information or opinion about an identified individual, or an individual that is reasonably identifiable. For example, personal information may include:

- Name, signature, address, phone number, date of birth
- Sensitive information (race/ethnicity, politics, religion, union membership, sexual orientation, criminal record, health or genetic information)
- Employee record information
- Credit Information
- Voice print and facial recognition biometrics
- Photographs
- IP address
- Photo
- Mobile location information

Alithia makes no representation or warranties in relation to the privacy practices of any third party organisations or information that provide or collect via their websites.

3. Responsibilities

All Alithia Staff are required to

- immediately report any possible privacy breach or data misuse to the Alithia Privacy Officer
- abide by the relevant data privacy principles when accessing and managing Personal Information
- understand and comply with requirements of ***POL-IT-001, Technology and Equipment Use*** when using company hardware and other devices, and to seek further information if unclear

[1] Alithia Staff means all its Directors and Officers, its employees, its interns, any third party consultants and contractors that it engages from time to time.

- understand and comply with IT security requirements set out ***POL-IT-003, Data Security and Protection*** and requirements of Alithia's IT partner
- follow best practices for data protection, which include but are not limited to the following:
    - where possible, use of a dedicated work computer that fully complies with Alithia security standards. This includes the installation and operation of RAMMP (remote Access and Monitoring Management and Protection Software) used to remotely manage and protect laptops)
    - keep work computer and other applicable devices containing company information in a safe location (eg, don't leave laptop unattended in full view)
    - follow all IT guidance and recommendations made by Alithia's IT partner
    - use strong passwords and regularly change these
    - don't share or document passwords; Alithia uses LastPass software for password security and Multifactor Authentication (MFA) is enforced (using Authenticator)
    - password required computer screen lock function when the computer is unattended
    - don't download information to portable drives
    - don't retain any Personal Information beyond the agreed or required timeframe
    - don't allow unauthorised people access to Alithia devices
    - don't install any unapproved software on Alithia computers (ie, any software that is not pre-approved or part of the standard Alithia Operating environment), without approval of Alithia management and Alithia IT Partner
    - when travelling avoid the use of free wifi/public wifi

Alitha management, with support from Alithia IT Vendor are responsible for ensuring:

- Systems and process are in place to restrict and monitor access to sensitive data
    - This not only includes access to clinical trials databases, but to all Alithia databases where Personal Information is stored
- Systems are secured to protect against cyberattacks
- Data protection practices are followed by all staff (access authorization, data encryption, system back-ups, shredding or secure waste for any physical documents)
- Data protection best practices are regularly communicated to all staff

4. Data Privacy Principles

The Australian Commonwealth Privacy Act contains 13 privacy principles that set standards, rights and obligations, including:

- The collection, disclosure, and usage of personal data
- Governance and responsibilities requirements
- Integrity of personal information
- An individual's right to access personal information

Lawfulness, fairness, and transparency are paramount. Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed.

5. Information Alithia Collects

Alithia may collect and process the following types of information as part of its general business activities to support the conduct of clinical trials:

Source	Personal Information	Legal Basis - Method of Consent for Legitimate business
Client and Vendors	Contact details including: First and last names, role, address, email, phone	• Via direct contact with Alithia • Contact details left on Alithia Website • Via provision of Survey responses after signed Confidentiality Agreement available • Signed Contracts
	Financial data eg, Client and Vendor Bank account details for payment and invoicing purposes	
	Survey data eg, information collected about a Vendor during a Vendor qualification survey	
Clinical Trial Sites Staff (eg, Principal Investigator)	Staff Contact details including: First and last names, role, address, phone, email, place of work, qualifications, education, awards, clinical trial experience	• Via Clinical Trial Research Agreements/Clinical Trial Investigation Agreements and need to comply with Good Clinical Practice requirements • Via provision of responses in feasibility surveys
	Personal information included with curriculum vitae, training certificates	
	Clinical Trial expertise and performance metrics	
Clinical Trial Participants	De-identified health information - Trial ID number, date of birth, gender, age	• Signed, Participant Information and Informed Consent Form (PICF) • SAE forms where applicable • EDC systems
	Medical results/history where required for eligibility purposes or which accompany an adverse event report (these should be redacted to only include Trial ID number)	
Alithia Staff	Contact details including: First and last names, role, address, email, phone, date of birth, gender, race and ethnicity, marital status, emergency contact, citizenship or legal status, education, professional licenses – required for employment purposes, any known conflicts of interest	• Signed employment or consultancy contracts • Compliance with Good Clinical Practice requirements
	Financial data eg, Client and Vendor Bank account details for salary and consultant payment purposes	
Job Applicants	Contact details including: First and last names, role, address, email, phone, LinkedIn, gender, race and ethnicity, citizenship or legal status, education, professional licenses – required for potential employment purposes	• Information submitted to Alithia for consideration
Event Attendees	First and Last Name, Job title, Company and Work contact details (address, email, phone)	• Provision of business card at an event/conference
Web Site Visitors	First and Last name, IP address, email	• Provision of information on a website

6. How Alithia Uses Personal Information

Alithia uses personal information to facilitate the conduct of Alithia's business, managing and monitoring clinical trial projects.

This can include but is not limited to:

- data processing in the course of service provision (eg, to make payments)
- Compliance when required by Law or Good Practices (eg, Audit and Regulatory Agency Inspections)
- To address requested communications, answer enquiries

7. Data Sharing and Disclosure

Alithia may share personal information to third parties nationally and or globally, when necessary for trial purposes and only for the purpose it was collected. Data is shared and disclosed under the specific circumstances and only with permission (unless Alithia is under a legal obligation to disclose). The following is a non-exhaustive list of examples of disclosure to third parties:

- Clinical trial site personnel data is shared with Alithia Clients eg, as part of a feasibility assessment and discussion of potential sites
- Clinical trial participant information may be disclosed to regulatory agencies as part of an individual case safety report or to a laboratory vendor for the purposes of sample collection information
- External databases, with strict security controls, that Alithia uses for the management of clinical trials including electronic data capture systems, radiology images etc
- Third parties that provide commercial, legal, financial, marketing and regulatory services

8. Data Security

Alithia take all reasonable steps to ensure security and confidentiality of Personal Information processed, including robust security measures to protect from unauthorized access, disclosure, alteration and destruction. The measures include physical and electronic measures, such as encryption, secure data storage and restricted access to authorized personnel only.

Where third parties and contractors have access to Personal Information, Alithia requires their protection of this information in a manner consistent with this policy. For example, this includes:

- not using the information for any purpose other than to carry out the services they are performing
- ensuring access to Personal Information is limited only to those personnel who require access to achieve the business objective

Alithia requires that third parties and contractors go through a process of qualification and review to become an approved vendor. This includes review of information on Data Security and Privacy controls where applicable. Alithia requires all Vendors to have a legal contract in place for service delivery with Alithia, or with Alithia's Clients, that documents/assures compliance with the applicable privacy laws for the required information processing.

9. Data Retention

Alithia retains Personal Information in the following ways:

- As long as necessary to fulfil the purposes outlined in this policy
- A longer period to comply with legal and regulatory requirements
- To ensure the integrity of clinical trial data

Once the retention period expires, Alithia will securely delete the data (if paper based by shredding or secure waste) and if electronic by double delete method (ie, delete primary file and also any back-up copy).

10. An Individual's Rights

Depending on geographic location and applicable data protection laws, an individual may have the following rights:

Access	To request a copy of your Personal Information
Correction	To request corrections to any inaccurate or incomplete data
Deletion	To request deletion of your Personal Information, subject to legal and contractual obligations
Objection	To object to the processing of your data in certain circumstances
Restriction	To request restrictions on the processing of your data
Portability	To allow your data to be directly transferred to another party
Withdrawal	To withdraw consent to data processing

For Australia the process for access and correction falls under the Freedom of Information Act 1982.

To exercise individual rights, contact the Alithia Privacy Officer at the address as per Section 11.

11. Alithia Contact for Privacy Information Requests

Any questions or concerns about this Privacy Policy, or Alithia's data practices, should be made in writing and directed to:

Alithia Privacy Officer
privacy@alithialifesciences.com
PO Box 5096, Moreland West VIC 3055 AUSTRALIA

If dissatisfied with the outcome of a privacy complaint, the Alithia Founder and Director, Dr Tina Soulis (tina.soulis@alithialifesciences.com) should be contacted.

Alithia will treat your request or complaint confidentially. The Alithia Privacy Officer will contact you within a reasonable time after your request or complaint is received to discuss the matters raised in your correspondence and outline options for resolution.

12. Reporting a Data Breach

A notifiable Data breach occurs when it is likely to result in serious harm to an individual whose Personal Information is involved.

A data breach occurs when Personal Information that an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with Client's Personal Information is lost or stolen
- a database with Personal Information is hacked
- Personal Information is mistakenly given to the wrong person.

If a notifiable privacy breach has occurred, immediately notify Alithia Privacy Officer on: privacy@alithialifesciences.com

The breach will be reviewed and assessed by Alithia management to determine if it meets the criteria for Notifiable Data Breach and if so, the Office of the Australian Information Commissioner (OAIC) and affected individual(s) will be promptly notified by Alithia in accordance with legislative requirements.

Alithia holds insurance for any data breach caused by unauthorised access due to cybersecurity incident(s). Alithia management will notify the Cybersecurity Insurers of any such breach resulting from unauthorised access to Alithia IT systems.

13. References

- *Privacy Act 1988 (Cth)*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*
- *Australian Privacy Principles, administered by the Australian government's Office of the Australian Information Commissioner. (https://www.oaic.gov.au/)*
- *Data Breach Reporting https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach*
- *POL-IT-001 Technology and Equipment Use*
- *POL-IT-003 Data Security and Protection*
- *General Data Protection Regulation (GDPR) EU (https://gdpr-info.eu/)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Freedom of Information Act 1982 (Cth)*

14. Policy Updates

Alithia may change this Privacy Policy from time to time. Any updates to this policy will be made available on the Alithia website.

15. Version History

Version	Date	Summary of changes
1.0	29 Nov 2024	N/A, First release