

POLICY

SCDC POL 04 Privacy Policy

SCDC POL 04

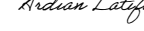
Status: FINAL

Version: 1.0

Page 1 of 13

Valid from: 2026-08-10

Expiry date: 2029-08-10

	Name and Position	Signature	Date
Prepared by:	Khalid Abubaker Chief Operating Officer	 Electronically signed by: Khalid Abubaker Reason: Approver Date: 07-Aug-2026 13:28:24 GMT+10	07-Aug-2026
Reviewed by:	Karin Gruber Head of Quality Assurance	 Electronically signed by: Karin Gruber Reason: Reviewer Date: 07-Aug-2026 15:43:04 GMT+12	07-Aug-2026
Reviewed by:	Nikita Nazareth Group People and Culture Manager	 Electronically signed by: Nikita Nazareth Reason: Reviewer Date: 07-Aug-2026 13:40:03 GMT+10	07-Aug-2026
Approved by:	Ardian Latifi Chief Executive Officer	 Electronically signed by: Ardian Latifi Reason: Approver Date: 07-Aug-2026 12:50:26 GMT+10	07-Aug-2026

Revision history

Version	Reason for Change	Date
0.1	Initial draft issued for review	2026-08-05
1.0	Initial Version	2026-08-10

This document belongs to Southern Clinical Development Consulting and cannot be changed or copied without the agreement of Southern Clinical Development Consulting.

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL		Version: 1.0	Page 2 of 13
Valid from: 2026-08-10			Expiry date: 2029-08-10

TABLE OF CONTENTS

1.0 PURPOSE

2.0 SCOPE

3.0 RESPONSIBILITIES

4.0 ABBREVIATIONS

5.0 POLICY

5.1 What personal information means

5.2 The personal information SCDC collects and holds

5.3 Sensitive information and consent

5.4 How SCDC collects personal information

5.5 Telling you when SCDC collects your information

5.6 Dealing with SCDC anonymously

5.7 Why SCDC collects, holds, uses and discloses personal information

5.8 Who SCDC discloses personal information to

5.9 Direct marketing

5.10 Where information is held and overseas disclosure

5.11 Keeping information accurate

5.12 Security, retention and destruction

5.13 Data breaches

5.14 How SCDC manages privacy risk

5.15 Training and awareness

5.16 Accessing your personal information

5.17 Correcting your personal information

5.18 Complaints

5.19 How to contact us

5.20 Availability and review of this policy

6.0 DOCUMENTATION AND RECORDS

7.0 REFERENCES

Southern Clinical Development Consulting				
POLICY				
SCDC POL 04 Privacy Policy			SCDC POL 04	
Status: FINAL		Version: 1.0		Page 3 of 13
Valid from: 2026-08-10			Expiry date: 2029-08-10	

1.0 PURPOSE

Southern Clinical Development Consulting (SCDC) provides regulatory, quality and clinical development consulting services to sponsors, biotechnology companies and research institutions. Doing that work means SCDC collects and holds personal information about the people it deals with.

This policy sets out what personal information SCDC collects, why it collects it, how it holds and protects it, who it may be given to, and what a person can do if they want to see their information, correct it, or complain about the way it has been handled.

It is published to meet SCDC's obligation under Australian Privacy Principle 1 to maintain a clearly expressed and current policy on the management of personal information. It is available free of charge at www.southerncdc.com, and in another form on request to the Privacy Officer.

SCDC handles personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles, together with applicable State and Territory health records legislation.

2.0 SCOPE

This policy applies to all personal information SCDC collects, holds, uses or discloses, across every part of the business and every system, whether that information is held electronically or on paper. It binds all SCDC personnel, including employees, contractors, secondees and consultants.

The policy sits above SCDC's controlled procedures for information security, system access, record retention and personnel management. Those procedures set out how personnel must do the work. This policy is the public statement of what SCDC does and why.

Two things are dealt with elsewhere:

- Information about SCDC personnel handled for employment purposes. Employee records are largely exempt from the Australian Privacy Principles under section 7B(3) of the Privacy Act, so this information is governed instead by the Employee Privacy Policy contained in the Employee Handbook and the Personnel Handbook. This policy still describes, at a general level, the personnel information SCDC holds
- Personal information SCDC handles for a client under a contracted engagement. Where SCDC works on a clinical trial for a sponsor, the sponsor determines what is collected and for what purpose. That collection is governed by the trial protocol, the participant information and consent form, the approving Human Research Ethics Committee, and the services agreement between SCDC and the sponsor. SCDC handles the information on the sponsor's instructions and applies the security and handling standards in this policy.

Where a client requires a privacy statement specific to an engagement, that statement sits alongside this policy. It does not displace it.

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL		Version: 1.0	Page 4 of 13
Valid from: 2026-08-10			Expiry date: 2029-08-10

3.0 RESPONSIBILITIES

Role	Responsibility
Privacy Officer	- Owns this policy and is the contact point for all privacy matters. - Handles enquiries, access and correction requests, and complaints, and maintains the register of those requests. - Issues and maintains the collection statements used for SCDC engagements. - Coordinates the assessment of, and response to, any suspected data breach. - The role is held by the Chief Operating Officer, or a delegate appointed by the CEO.
Chief Executive Officer	- Approves this policy and is accountable for privacy compliance at company level. - Approves notification decisions under the Notifiable Data Breaches scheme.
Head of Quality Assurance	- Maintains this policy as a controlled document and schedules its periodic review. - Confirms that personnel have completed privacy training and reports completion to management. - Oversees corrective and preventive actions arising from privacy incidents, complaints or audit findings.
Head of IT	- Maintains the technical safeguards described in this policy, including access control, encryption, monitoring, backup and recovery. - Assesses privacy and security risk in new systems and tools before they are approved for use.
Project Managers and Department Heads	- Confirm that the personal information handled by their teams is limited to what the work requires and is held only in approved systems. - Confirm that a collection statement has been issued where personal information is collected for an engagement.
People and Culture Team	- Issues collection statements to candidates at the application stage. - Limits recruitment and onboarding data collection to what the role requires. - Coordinates contractor access and correction requests with the Privacy Officer. - Handles employee record requests under the Fair Work Regulations.
All personnel	- Handle personal information only for a proper purpose connected to their role. - Complete privacy, information security and system use training as required. - Report any suspected privacy breach, loss of information or unauthorised access to the Privacy Officer immediately on becoming aware of it.

4.0 ABBREVIATIONS

Abbreviation	Definition
APP	Australian Privacy Principle
CTMS	Clinical Trial Management System

Southern Clinical Development Consulting					
POLICY					
SCDC POL 04 Privacy Policy				SCDC POL 04	
Status: FINAL		Version: 1.0		Page 5 of 13	
Valid from: 2026-08-10				Expiry date: 2029-08-10	

GCP	Good Clinical Practice
HREC	Human Research Ethics Committee
LMS	Learning Management System
MFA	Multi-Factor Authentication
NDB	Notifiable Data Breaches
OAIC	Office of the Australian Information Commissioner
POL	Policy
RBAC	Role-Based Access Control
SCDC	Southern Clinical Development Consulting
SOP	Standard Operating Procedure
SSO	Single Sign-On

Abbreviations and acronyms and their meaning are explained in the [Master Abbreviations Log](#).

5.0 POLICY

5.1 What personal information means

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not it is true and whether or not it is recorded in a material form.

Sensitive information is a category of personal information that attracts a higher standard of protection. It includes health information, and information about a person's racial or ethnic origin, political opinions, religious beliefs, sexual orientation and criminal record.

5.2 The personal information SCDC collects and holds

SCDC collects personal information only where it is reasonably necessary for one or more of its functions or activities. In practice what it collects falls into the following categories.

- Business contact and professional details. Name, job title, employer or institution, business email address, business telephone number, business address, and professional qualifications or registrations. This covers client and sponsor personnel, principal investigators and site staff, research governance and ethics contacts, Institutional Biosafety Committee members, regulator contacts, and vendor and subcontractor personnel.
- Information required for regulatory submissions. The names, positions, qualifications and experience of individuals who must be identified in an application, license, notification or item of regulatory correspondence, together with any curriculum vitae or training certificate supplied in support.
- Training and competency records. Attendance, completion and assessment records for training SCDC delivers or oversees, including training delivered to clinical site staff on the conditions of a license.

Southern Clinical Development Consulting			
POLICY			
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL	Version: 1.0	Page 6 of 13	
Valid from: 2026-08-10			Expiry date: 2029-08-10

- Records of dealings. Correspondence, meeting records, file notes, and records of instructions, decisions and approvals.
- System account and audit information. User names, business email addresses, access rights, log-in records and audit trail entries generated by SCDC business systems.
- Contract and payment information. What is needed to enter into and administer an agreement, raise a purchase order, or make or receive a payment.
- Personnel information. Information about employees, contractors and candidates collected for recruitment, engagement and employment purposes. This is described in the Employee Privacy Policy in the Employee and Personnel Handbooks.
- Clinical trial information. Where an engagement requires it, SCDC may handle coded clinical trial data on behalf of a sponsor. During site monitoring, SCDC personnel may view identifiable participant records at a clinical site to verify data against source records, as Good Clinical Practice requires. SCDC does not remove identifiable participant records from the site and does not hold them, unless the protocol and the participant's consent expressly permit it and the sponsor has instructed SCDC to do so.
- Website and electronic communications information. SCDC's website may record standard technical information such as internet protocol address, browser type and pages visited. Information a person submits through an enquiry form or by email is held so that SCDC can respond and keep a record of the exchange.

SCDC does not collect government related identifiers such as tax file numbers except where the law requires it for employment, payment or taxation purposes, and does not adopt a government related identifier as its own identifier for a person.

5.3 Sensitive information and consent

SCDC collects sensitive information only where the individual has consented and the information is reasonably necessary for SCDC's functions, or where the collection is required or authorised by law.

Where consent is needed, SCDC seeks it before the information is collected, explains what the person is agreeing to, and records the consent. Consent is not bundled with unrelated matters. A person may withdraw their consent at any time by contacting the Privacy Officer, although a withdrawal does not require SCDC to delete records it is required by law, by a regulator or by a client agreement to retain.

Health information handled in the course of a clinical trial engagement is collected by the sponsor under the trial protocol and the participant's consent, and reviewed or held by SCDC only to the extent the engagement requires. SCDC uses it for the contracted purpose and for nothing else. It is never used for marketing, and it is not disclosed except as set out in section 5.8.

5.4 How SCDC collects personal information

Southern Clinical Development Consulting				
POLICY				
SCDC POL 04 Privacy Policy			SCDC POL 04	
Status: FINAL		Version: 1.0		Page 7 of 13
Valid from: 2026-08-10			Expiry date: 2029-08-10	

SCDC collects personal information directly from the individual where that is reasonable and practicable. This happens when a person contacts SCDC, attends a meeting, audit or training session, applies for a role, or supplies their details for a regulatory application.

SCDC also receives personal information from other sources, including clients and sponsors, clinical trial sites and their institutions, ethics and biosafety committees, regulators, vendors and subcontractors, publicly available registers and professional directories, and recruitment agencies.

If SCDC receives personal information it did not ask for and could not have collected under this policy, it destroys or de-identifies that information where it is lawful and reasonable to do so.

5.5 Telling you when SCDC collects your information

SCDC takes reasonable steps to tell a person, at or before the time their personal information is collected, or as soon as practicable afterwards:

- who SCDC is and how to contact us;
- that the information has been collected, and where it was collected from, if the person may not be aware SCDC holds it or that it came from someone else;
- whether the collection is required or authorised by law, and which law requires or authorises it;
- the purposes for which the information is being collected;
- what is likely to happen if the information is not provided;
- the types of organisations SCDC usually discloses that kind of information to;
- that this policy explains how a person can access and correct their information, and how to make a complaint; and
- that SCDC may disclose the information to recipients outside Australia, and where those recipients are located.

This is done through a collection statement. Where SCDC collects personal information for a specific engagement, including from principal investigators, study staff, institutional and research governance contacts, ethics or biosafety committee members and client personnel, a collection statement covering the matters above is issued for that engagement and provided at or around the point of collection, either directly or through the client or site that makes the introduction.

For clinical trial participants, the collection notice is given by the sponsor through the participant information and consent form approved by the Human Research Ethics Committee. SCDC does not collect personal information directly from trial participants.

5.6 Dealing with SCDC anonymously

A person may deal with SCDC anonymously or under a pseudonym where it is lawful and practicable, for example when making a general enquiry. In most other situations it is not practicable. Regulatory applications,

Southern Clinical Development Consulting			
POLICY			
SCDC POL 04 Privacy Policy		SCDC POL 04	
Status: FINAL	Version: 1.0	Page 8 of 13	
Valid from: 2026-08-10		Expiry date: 2029-08-10	

contracts, dealings with sites and institutions, training records and employment matters all require SCDC to know who it is dealing with.

5.7 Why SCDC collects, holds, uses and discloses personal information

SCDC handles personal information for the following purposes:

- to provide the services SCDC has been engaged to provide;
- to prepare, lodge and manage regulatory applications, licenses, notifications and correspondence, and to respond to regulator queries;
- to identify, assess, contract with and oversee clinical trial sites, investigators, vendors and subcontractors;
- to deliver and record training, and to show that required training was completed;
- to communicate with clients, sites, institutions, committees and regulators about a project;
- to meet obligations under Good Clinical Practice, the trial protocol and applicable regulatory requirements, including safety reporting;
- to negotiate, administer and enforce agreements, to raise and pay invoices, and to keep accounting records;
- to recruit, engage and employ personnel and administer that relationship;
- to respond to enquiries, requests and complaints;
- to keep SCDC systems and records secure, accurate and available;
- to support audits and inspections by clients, regulators and SCDC's own quality function; and
- to meet a legal or regulatory obligation, or to establish, exercise or defend a legal claim.

SCDC uses and discloses personal information for the purpose it was collected for, for a directly related purpose the person would reasonably expect, with the person's consent, or where the law requires or authorises it.

5.8 Who SCDC discloses personal information to

SCDC may disclose personal information to:

- clients and sponsors, and their affiliates, agents and other service providers involved in the project;
- regulators and government bodies, including the Office of the Gene Technology Regulator and the Therapeutic Goods Administration;
- Human Research Ethics Committees, Institutional Biosafety Committees and research governance offices;
- clinical trial sites and the institutions that host them;
- vendors, subcontractors and service providers engaged by SCDC, including information technology, hosting, learning management and professional services providers, each of whom is bound by contract to protect the information and use it only for the purpose it was supplied for;
- professional advisers, auditors and insurers;

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL	Version: 1.0	Page 9 of 13	
Valid from: 2026-08-10			Expiry date: 2029-08-10

- a purchaser or prospective purchaser in connection with a sale, merger or restructure of the business, under confidentiality obligations; and
- any person where the disclosure is required or authorised by law, or is reasonably necessary to prevent a serious threat to life, health or safety.

SCDC does not sell, rent or trade personal information.

5.9 Direct marketing

SCDC does not disclose personal information to third parties for their marketing purposes. SCDC may contact business contacts about its services, industry developments or events. Every such communication includes a way to opt out, and SCDC acts on an opt-out request promptly.

A person may ask SCDC at any time to stop sending them marketing material, and may ask SCDC to tell them where it obtained their information. Requests should go to the Privacy Officer.

5.10 Where information is held and overseas disclosure

Most personal information SCDC holds is stored in its Microsoft 365 environment, which resides at rest in Microsoft's Australian data centres.

Two systems hold a limited set of personal information outside Australia:

- SCDC's Learning Management System is hosted in the European Union. It holds the names, business email addresses and job titles of SCDC personnel and contractors.
- SCDC's Clinical Trial Management System is hosted in the Republic of Korea. It holds account details, being the names and business email addresses, of the personnel who use the system.

The information held in those two systems is limited to user account and directory information. It does not include client confidential information or clinical trial data.

Separately, where a client is part of a global group, information SCDC provides to that client during an engagement may be accessed by that client's personnel or affiliates located outside Australia. Where a regulatory submission requires it, information may be provided to a regulator outside Australia.

Before disclosing personal information to a recipient outside Australia, SCDC takes reasonable steps to satisfy itself that the recipient will handle the information in a way consistent with the Australian Privacy Principles. This is ordinarily done by contract.

5.11 Keeping information accurate

SCDC takes reasonable steps to make sure the personal information it collects, uses and discloses is accurate, current and complete. If a person tells SCDC that their information is wrong or out of date, SCDC will correct it. Telling SCDC when contact details or roles change is the fastest way to keep records right.

5.12 Security, retention and destruction

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL	Version: 1.0	Page 10 of 13	
Valid from: 2026-08-10			Expiry date: 2029-08-10

SCDC protects personal information from misuse, interference, loss, and unauthorised access, modification or disclosure using a combination of technical, physical and organisational controls. These include:

- multi-factor authentication and single sign-on for access to business systems;
- role-based access control applied on a least-privilege basis, with project information restricted to the personnel assigned to that project;
- encryption of information in transit and at rest;
- endpoint protection, email filtering and threat detection across SCDC devices and accounts, with logging and alerting;
- routine backup, tested restoration, and a documented disaster recovery process;
- controlled physical access to SCDC premises, visitor sign-in and supervision, and secure handling of anything held in hard copy;
- assessment of vendors and systems before they are approved for use, and contractual confidentiality and security obligations on vendors and subcontractors; and
- confidentiality obligations, a code of conduct, and mandatory training binding on all personnel.

SCDC keeps personal information only for as long as it is needed for the purpose it was collected for, or for as long as a law, a regulatory requirement or a client agreement requires it to be kept. Clinical trial and regulatory records are subject to long retention periods. Once information is no longer needed and is no longer required to be kept, SCDC destroys it or de-identifies it.

5.13 Data breaches

SCDC maintains a documented data breach response process aligned to the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

Personnel must report a suspected breach to the Privacy Officer as soon as they become aware of it. SCDC then contains the breach, assesses it as quickly as it can and in any event within 30 days, decides whether the eligible data breach threshold has been met, notifies where it has, and reviews the cause so it can be addressed.

Where an eligible data breach occurs, SCDC notifies the Office of the Australian Information Commissioner and the affected individuals as soon as practicable. Where a breach affects information SCDC holds for a client, SCDC notifies that client in accordance with the applicable services agreement.

5.14 How SCDC manages privacy risk

Privacy risk is managed inside SCDC's quality management system rather than as a separate exercise. In practice:

- new systems, tools and vendors are assessed for privacy and security risk before they are approved for use, and are subject to contractual protections;
- artificial intelligence tools are separately governed, and no client data or client deliverable is processed by a public or unapproved artificial intelligence tool;

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL	Version: 1.0	Page 11 of 13	
Valid from: 2026-08-10			Expiry date: 2029-08-10

- changes to processes and systems go through change control, with an impact assessment that considers privacy and regulatory compliance;
- the personal information collected for an engagement is kept to what that engagement actually requires, a collection statement is issued, and access is limited to the personnel who need it;
- privacy incidents, complaints and audit findings are investigated and, where warranted, managed through corrective and preventive action; and
- this policy and the procedures supporting it are reviewed on a set cycle, and sooner if something material changes.

5.15 Training and awareness

Privacy, information security and system use training forms part of onboarding for all SCDC personnel and must be completed before or at the point system access is granted.

Personnel complete refresher training at least annually, and additional training whenever a relevant policy or procedure changes materially. Training is recorded, records are retained, and completion is monitored by Quality Assurance and reported to management.

5.16 Accessing your personal information

A person may ask for access to the personal information SCDC holds about them by contacting the Privacy Officer. SCDC will ask for enough information to confirm the person's identity before releasing anything.

There is no charge for making a request. SCDC may charge a reasonable amount for the cost of retrieving and supplying the information, and will tell the person what that cost will be before it is incurred. SCDC responds within 30 days.

If SCDC refuses access, or provides it in a different form to the one requested, it will explain the reasons in writing and set out how the person can complain.

5.17 Correcting your personal information

A person may ask SCDC to correct personal information they believe is inaccurate, out of date, incomplete, irrelevant or misleading. SCDC will make the correction within 30 days, or explain in writing why it will not and how the person can complain.

Where SCDC has already disclosed the information to someone else, the person may ask SCDC to notify that recipient of the correction, and SCDC will take reasonable steps to do so unless it is impracticable or unlawful.

Some records cannot be altered once they are created. Clinical trial and regulatory records are held under audit trail and controlled document requirements. Where a correction cannot be made by amending the original record, SCDC will attach a statement of the correction to the record so that anyone reading it sees the correction.

5.18 Complaints

Southern Clinical Development Consulting			
		POLICY	
SCDC POL 04 Privacy Policy			SCDC POL 04
Status: FINAL	Version: 1.0	Page 12 of 13	
Valid from: 2026-08-10			Expiry date: 2029-08-10

A person who believes SCDC has mishandled their personal information, or has breached the Australian Privacy Principles, should contact the Privacy Officer in writing, setting out what happened and what outcome they are seeking.

SCDC acknowledges a privacy complaint within 5 business days, investigates it, and responds within 30 days. If a complaint is complex and needs longer, SCDC will say so and give a revised date.

If a person is not satisfied with SCDC's response, they may refer the complaint to the Office of the Australian Information Commissioner:

Website	www.oaic.gov.au
Phone	1300 363 992
Email	enquiries@oaic.gov.au
Post	GPO Box 5288, Sydney NSW 2001

5.19 How to contact us

Privacy enquiries, access and correction requests, opt-out requests and complaints should be directed to:

Attention	Privacy Officer
Entity	The Trustee for Southern Clinical Development Consulting Trust trading as Southern Clinical Development Consulting Pty Ltd
ABN	68 157 645 360
Post	Level 17, 60 City Road, Southbank VIC 3006, Australia
Email	privacy@southerncdc.com
Website	www.southerncdc.com

5.20 Availability and review of this policy

This policy is published on SCDC's website and is available free of charge. A copy in another form can be requested from the Privacy Officer.

SCDC reviews the policy at least every three years, and sooner if the law, SCDC's systems, or the way SCDC handles personal information changes materially. The version published on the website is the current version.

6.0 DOCUMENTATION AND RECORDS

- The register of privacy enquiries, access and correction requests, opt-out requests and complaints, maintained by the Privacy Officer on the SCDC SharePoint.
- Collection statements issued for SCDC engagements, and records of consent where consent has been obtained, held with the engagement records.

POLICY

SCDC POL 04 Privacy Policy		SCDC POL 04
Status: FINAL	Version: 1.0	Page 13 of 13
Valid from: 2026-08-10		Expiry date: 2029-08-10

- Data breach records, including the assessment, the notification decision and the reasons for it, maintained by the Privacy Officer.
- Training records, held in the Learning Management System and monitored by Quality Assurance.
- Vendor and system assessment records, and the approved tools register maintained under POL 02.
- This policy, held as a controlled document on the SCDC SharePoint and published at www.southerncdc.com. Superseded versions are retired and archived in accordance with SOP 004.

7.0 REFERENCES

- Privacy Act 1988 (Cth), including the Australian Privacy Principles at Schedule 1 and the Notifiable Data Breaches scheme at Part IIIC
- Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines
- Office of the Australian Information Commissioner, Data Breach Preparation and Response Guide
- Applicable State and Territory health records legislation, including the Health Records Act 2001 (Vic)
- ICH Guideline for Good Clinical Practice
- NHMRC National Statement on Ethical Conduct in Human Research