Privacy and Confidentiality Policy

Document ID	POL-007	**Version**	1.0
Owner	Director	**Approved by**	Daniel Patterson, Director
Issue date	1 November 2025	**Last revised**	5 September 2026

Policy statement

Northern Rivers Toxicology (NRT) protects personal information, sensitive information, customer information and laboratory information against unauthorised collection, use, disclosure, alteration, loss or access. NRT manages information in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), applicable data-breach obligations, legally enforceable confidentiality commitments and the confidentiality, records and information-management requirements relevant to ISO/IEC 17025:2017.

NRT is a non-clinical analytical service. Consistent with POL-001, human drug-testing services are performed for a requesting authority under an agreed non-clinical purpose and donors are not treated as patients. This does not reduce the protection afforded to personal, sensitive, or health information under applicable privacy law.

Purpose

This policy establishes the minimum requirements for collecting, handling, securing, using, disclosing, retaining, correcting, and disposing of information handled by NRT. It also establishes confidentiality obligations for laboratory activities and controls for laboratory information systems, technical records and external service providers.

Scope

This policy applies to all NRT directors, employees, contractors, consultants, temporary personnel and any other person given access to NRT information or systems. It applies to information in any form, including electronic records, paper records, emails, images, laboratory instrument data, chain-of-custody records, reports, specimens where linked to an identifiable person, customer records, financial records, and quality-management records.

The policy applies to information obtained from customers, donors, requesting authorities, collection providers, employers, laboratories, legal representatives, regulators, courts and other sources, as well as information created by NRT during laboratory activities.

Definitions

- **Personal information:** information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or recorded in a material form.
- **Sensitive information**: includes health information and other categories of information treated as sensitive under the Privacy Act.
- **Health information:** information or an opinion about an individual's health, disability, health services or related matters, where the statutory definition applies. Toxicology information may constitute health information even though NRT does not provide clinical care or health services.
- **Customer information:** information obtained from, concerning, or created for a customer or requesting authority in connection with laboratory activities.
- **Laboratory information:** analytical data, technical records, chain-of-custody information, reports, quality records, instrument records, and other information obtained or created in laboratory activities.
- **Authorised recipient:** a person or entity authorised by the customer, contract or law to receive specified information.
- **Privacy incident:** an actual or suspected loss, unauthorised access, unauthorised disclosure, misuse, interference, alteration or compromise of personal information.

Governance and responsibilities

- The Director is accountable for privacy governance and for ensuring that appropriate practices and systems are maintained.
- The Director acts as NRT Privacy Officer unless another person is formally appointed.
- All personnel must preserve confidentiality, access information only for authorised work, follow information-security controls, and promptly report suspected privacy or security incidents.
- System owners must ensure that access, validation, backup, change control, and auditability requirements are implemented for systems used to acquire, process, record, report, store, or retrieve laboratory information.
- Managers engaging external providers must assess confidentiality, privacy, security, data-location, and access risks before the provider is given NRT information.

Privacy management and APP compliance

NRT will take reasonable steps to implement practices, procedures and systems that support compliance with the APPs and enable privacy enquiries and complaints to be handled appropriately. NRT will maintain an up-to-date public privacy notice or privacy policy containing the matters required by APP 1.

Privacy controls must be proportionate to the nature, sensitivity, volume, and consequences of misuse of the information. Sensitive laboratory and donor information is to be treated as high-sensitivity information.

Collection of personal and sensitive information

NRT will collect only information reasonably necessary for its functions or activities and will collect sensitive information only where consent or another lawful basis permits collection. Information may be collected directly from an individual or from a requesting authority, employer, collector, laboratory, practitioner, legal representative, government body, or other authorised source.

- Collection must be relevant to the requested analytical or administrative purpose.
- Staff must not seek medical or personal information that is unnecessary to perform, verify, or interpret within NRT's non-clinical scope, or report the requested laboratory activity.
- Where reasonably practicable, individuals must be provided with an appropriate collection notice or otherwise informed of the matters required by APP 5.
- If unsolicited personal information is received, NRT must determine whether it could lawfully have been collected. If not, it must be destroyed (or de-identified) where lawful and reasonable to do so.

Anonymity and pseudonymity

A person is not permitted to maintain anonymity or use a false name (pseudonym) when dealing with NRT. Whilst NRT can avoid disclosing your identity, if we cannot verify a persons identity as being that of a natural person we may refuse to deal with them until such time as they provide unequivocal proof of their identity.

This also applies to complainants, a complaint cannot be considered or investigated if not connected to a natural person.

Use and disclosure

Personal information may only be used or disclosed for the primary purpose for which it was collected, for a related secondary purpose reasonably expected by the individual where permitted by law, with valid consent, or where another lawful authority applies.

- Laboratory results must be released only to an authorised recipient through an approved release process.
- Personnel must verify recipient identity and authority where appropriate before releasing sensitive or confidential information.
- Information must not be discussed in public areas, with unauthorised colleagues, or with any person whose role does not require access.
- Donor or customer information must not be used for curiosity, personal purposes, training examples, presentations, marketing, or research unless authorised and lawful, with de-identification used where appropriate.
- NRT will not use sensitive donor information for direct marketing.

ISO/IEC 17025 confidentiality requirements

NRT treats all information obtained or created during laboratory activities as confidential unless it has been made publicly available by the customer, the customer and NRT have agreed that it may be public, or release is otherwise authorised or required by law. Confidentiality obligations form part of the legally enforceable commitments applicable to NRT personnel and relevant external providers.

- If NRT intends to place customer information in the public domain, the customer must be informed in advance unless the information is already public or another lawful basis applies.
- Where NRT is required by law, subpoena, warrant, court order or authorised contractual arrangement to release otherwise confidential information, NRT will notify the affected customer or individual of the information released unless notification is prohibited by law or the relevant authority.
- Information about a customer obtained from a source other than the customer remains confidential. The identity of the source must also remain confidential to NRT unless the source agrees to disclosure or disclosure is required by law.
- Personnel, committee members, contractors, external bodies and persons acting on behalf of NRT must keep confidential all information obtained or created during laboratory activities except where disclosure is authorised or required by law.

Laboratory results, technical records and chain of custody

Laboratory information must be created, maintained and amended in a way that preserves traceability, integrity and accountability. Technical and evidentiary records must enable reconstruction of the laboratory activity to the extent required by the applicable method, quality system, contract and ISO/IEC 17025 requirements.

- Specimens, worksheets, instrument files, chromatograms, calculations, review records and reports must use controlled identifiers sufficient to prevent misidentification.
- Changes to technical records must not obscure the original entry. The change must be traceable to the person making it and, where applicable, the date and reason for the change.
- Corrections to personal details must not destroy the historical integrity of laboratory records or audit trails.
- Results must not be altered, reissued or withdrawn except through an authorised amendment, correction or report-control process.
- Chain-of-custody information must be protected against unauthorised alteration and must be available only to personnel and recipients with a legitimate need to access it.

Data quality and correction

NRT will take reasonable steps to ensure that personal information it collects is accurate, up to date and complete and that information used or disclosed is accurate, up to date, complete and relevant for the purpose. Where an individual requests correction, NRT will assess the request under APP 13 and any applicable contractual, evidentiary and laboratory-record requirements.

A privacy correction request does not itself require NRT to change a scientifically valid analytical result. Where a request disputes the technical validity or interpretation of a result, the matter must be managed through the applicable complaints, technical review, nonconformance or report-amendment process.

Information security

NRT must take reasonable steps to protect personal and confidential information from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure. Controls are to be selected having regard to the sensitivity and consequence of compromise.

- Access must be limited to authorised personnel on a least-privilege and need-to-know basis.
- Each user must use an individual account where the system supports individual authentication. Shared credentials are prohibited unless technically unavoidable and formally risk-assessed.
- Strong authentication, including multi-factor authentication where reasonably available and appropriate, must be used for systems holding sensitive information or remote access.
- Passwords, tokens, cryptographic keys and other authentication secrets must not be shared or stored insecurely.
- Sensitive information must be transmitted using an approved secure method. Staff must verify email addresses and recipients before sending reports or other sensitive material.
- Portable media and local copies must be minimised. Where used, they must be controlled and protected against unauthorised access.
- Paper records containing sensitive information must be stored in controlled areas and disposed of securely.
- Systems and devices must be maintained, patched and protected in accordance with NRT information-security procedures and risk assessments.
- Backups must be sufficient to protect required records against loss and must be protected against unauthorised access or alteration.
- Access must be removed or changed promptly when personnel leave, change roles or no longer require access.

Control of data and information management systems

Systems used for the collection, processing, recording, reporting, storage or retrieval of laboratory data must be suitable for their intended purpose and controlled to preserve data integrity. This applies to computerised and non-computerised systems.

- Laboratory information systems and relevant interfaces must be validated or otherwise verified as fit for purpose before introduction and following significant changes, to the extent required by the quality system.
- Changes to software, configurations, calculations, interfaces and reporting templates that may affect laboratory information must be authorised, documented and tested before use.
- Systems must be protected against unauthorised access, tampering, loss and corruption and must maintain appropriate audit trails or equivalent traceability where required.
- Where an external provider manages or hosts laboratory information systems, NRT remains responsible for ensuring that applicable ISO/IEC 17025, privacy, confidentiality and record-control requirements are addressed through due diligence and contractual controls.
- Manual calculations, spreadsheets or other user-developed tools affecting reported results must be appropriately controlled, checked and protected from unauthorised alteration.

External service providers and cross-border disclosures

Before providing personal or confidential information to an external service provider, NRT must determine what information is necessary, whether the provider requires access, where information will be stored or accessed, and what contractual and technical safeguards are appropriate.

- Only the minimum information reasonably necessary for the service is to be disclosed.
- Contracts or other enforceable arrangements should address confidentiality, authorised use, security, breach notification, return or destruction of information and access by subcontractors where relevant.
- Cross-border disclosures must be managed in accordance with APP 8 and applicable Privacy Act requirements. NRT must maintain sufficient knowledge of likely overseas recipients or locations to support the disclosures required in its public APP privacy policy.
- Remote support access by an overseas provider is to be treated as a potential cross-border disclosure and assessed accordingly.

Government-related identifiers

NRT must not adopt a government-related identifier, such as a Medicare number or driver licence number, as its own identifier for an individual unless permitted by law. Government-related identifiers may only be used or disclosed where authorised by APP 9 or another applicable law.

Access to personal information

Individuals may request access to personal information held about them. Requests must be referred to the Director or delegated Privacy Officer and handled in accordance with APP 12. NRT may verify identity and authority before providing access and may refuse or limit access only where a lawful exception applies.

Where access is refused or limited, NRT will provide written reasons and information about available complaint mechanisms where required by law. Access to laboratory materials may be provided in a form that preserves third-party confidentiality, chain-of-custody integrity, legal privilege, and evidentiary requirements.

Retention, destruction and de-identification

Personal and laboratory information must be retained for the period required by applicable law, contract, accreditation requirements, evidentiary needs, the quality system and NRT's records-retention schedule. Information must not be destroyed while it is subject to a complaint, investigation, legal hold, subpoena, court proceeding, accreditation requirement or other known preservation obligation.

When personal information is no longer required for any authorised purpose and no legal or operational retention requirement applies, NRT will take reasonable steps to destroy or de-identify it in accordance with APP 11. Destruction must be secure and appropriate to the medium and sensitivity of the information.

Biological specimens are managed under applicable specimen-retention and disposal procedures. The retention period for a specimen may differ from the retention period for the records associated with that specimen.

Privacy incidents and notifiable data breaches

All suspected privacy or information-security incidents must be reported to the Director immediately. Personnel must not conceal, independently investigate beyond their authority, or communicate externally about an incident unless authorised.

- NRT will take prompt steps to contain the incident, preserve evidence, identify affected information and systems, and reduce the risk of further access or disclosure.
- The Director will assess whether the incident is an eligible data breach under the Privacy Act, including whether unauthorised access, disclosure or loss is likely to result in serious harm and whether remedial action prevents that outcome.
- Where notification is required, NRT will prepare the required statement and notify the Office of the Australian Information Commissioner and affected individuals in accordance with the Notifiable Data Breaches scheme.
- Incidents must be documented, investigated to an appropriate level and considered for corrective action, risk treatment and management-system improvement.

Privacy complaints and enquiries

Privacy enquiries, access requests, correction requests and complaints are to be directed to the Director or delegated Privacy Officer using NRT's published contact details. Complaints must be acknowledged, investigated fairly and documented. NRT will provide a response within a reasonable period and advise the complainant of external review avenues where applicable, including the Office of the Australian Information Commissioner.

Personnel must not disadvantage or retaliate against a person for making a privacy complaint or exercising a privacy right.

Automated processing and decision-making

Laboratory instruments, software and information systems may perform automated calculations, flagging, data processing or workflow functions. Such automation must remain subject to validation, technical review and authorised reporting controls where it can affect laboratory outcomes.

Before NRT introduces a computer program that uses personal information to make, or substantially and directly assist in making, a decision that could reasonably be expected to significantly affect an individual's rights or interests, the Director must assess the applicable Privacy Act requirements and ensure NRT's public privacy policy is updated before the relevant statutory obligations commence or the arrangement is used, whichever is later.

Training, confidentiality undertakings and access review

- Personnel must receive privacy, confidentiality and information-security instruction appropriate to their role before or promptly after being given access to sensitive information.
- Employment, contractor or other enforceable arrangements must include confidentiality obligations appropriate to the information accessible to the person.
- Confidentiality obligations continue after a person ceases employment, engagement or association with NRT.
- Access rights are to be reviewed periodically and whenever roles or responsibilities change.
- Privacy and confidentiality requirements are to be included in relevant internal audits, management review inputs, corrective actions and risk assessments.

Breach of this policy

Unauthorised access, use, disclosure, alteration, copying or removal of personal or confidential information may constitute misconduct and may result in withdrawal of access, disciplinary action, termination of engagement, contractual remedies, notification to regulators or law-enforcement authorities, or other action appropriate to the circumstances.

Review and legal escalation

This policy must be reviewed at planned intervals and whenever there is a material change to privacy law, NRT services, information systems, laboratory accreditation requirements, outsourcing arrangements or information-handling practices. The Director must obtain legal advice where a proposed practice raises uncertainty about statutory privacy obligations, cross-border disclosure, compulsory disclosure, health-information regulation, surveillance, automated decision-making or other material privacy risk.

This policy is an operational control document and does not itself determine whether a particular statutory definition, exemption or jurisdiction applies. Where requirements conflict, NRT will comply with the applicable law and preserve ISO/IEC 17025 confidentiality and record-integrity requirements to the maximum extent lawfully possible.

References

- *Privacy Act 1988* (Cth)
- Australian Privacy Principles - Schedule 1 to the Privacy Act 1988 (Cth)
- Office of the Australian Information Commissioner - Australian Privacy Principles Guidelines
- Privacy Act 1988 (Cth) - Notifiable Data Breaches scheme
- ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories
- ISO/IEC 17025:2017 clauses 4.2 (Confidentiality), 7.5 (Technical records), 7.11 (Control of data and information management) and 8.4 (Control of records)
- NATA ISO/IEC 17025 Assessment Worksheet and applicable accreditation criteria
- POL-001 - Non-Clinical Scope and Service Boundary
- PRO-005 - Complaints

Revision history

Version	Date	Change	Approved by
1.0	1 November 2025	Initial issue	Daniel Patterson, Director