

Document Number:	5.1
Document Name:	Ethics and privacy policy
Version Number:	2019.1
Effective Date:	14/02/2019

1.0 Purpose

To describe the consent process for data collection and how the privacy of patient information collected by ANZDATA is ensured.

2.0 Policy Details

2.1 Background

On the 12th March 2014, the Australian Privacy Principles (APPs) replaced the National Privacy Principles in providing guidance to Australian Government agencies and private sector and not-for-profit organisations through 13 principles concerning the handling, management and use of personal information. These principles include:

Part 1: Consideration of personal information privacy

APP 1 — Open and transparent management of personal information

APP 2 — Anonymity and pseudonymity

Part 2: Collection of personal information

APP 3 — Collection of solicited personal information

APP 4 — Dealing with unsolicited personal information

APP 5 — Notification of the collection of personal information

Part 3: Dealing with personal information

APP 6 — Use or disclosure of personal information

APP 7 — Direct marketing

APP 8 — Cross-border disclosure of personal information

APP 9 — Adoption, use or disclosure of government related identifiers

Part 4: Integrity of personal information

APP 10 — Quality of personal information

APP 11 — Security of personal information

Part 5: Access to, and correction of, personal information

APP 12 — Access to personal information

APP 13 — Correction of personal information

ANZDATA is committed to acting in accordance with these principles, and is open and transparent about the collection, management and usage of information. ANZDATA's policies and procedures are consistent with the privacy principles outlined in the APPs.

The information provided below gives specific details of ANZDATA's privacy policies not covered elsewhere. Additional information relevant to the APPs can be found in other policy and procedure documents:

- 1.1 Mission, vision and values statement
- 2.1 Data collection policy
- 2.2 Data custodianship and release policy
- 2.3 Data requests standard procedure
- 2.4 Quality assurance procedures
- 2.5 Data linkage request procedure
- 2.6 Current data collection
- 3.1 Security compliance policy
- 4.1 Outputs and publications
- 5.2 Complaints policy
- 6.1 Freedom of information policy

While ANZDATA's internal policies are consistent with the APPs, where issues arise that are not specifically covered in internal documents, the Executive will refer to the APPs for guidance.

Detailed information on the APPs can be found here:

<https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>

2.2 Opt-out Consent

- Following extensive consultation in 2002 ANZDATA adopted an opt-out consent process for data collection.
- Patients are distributed information outlining the nature and purpose of the information collected, offered an opportunity to view that data and ask questions, and the opportunity to request withdrawal of part or all of their data.
- This approach is that endorsed by the Safety and Quality Commission for Clinical Quality Registries (<http://www.safetyandquality.gov.au/our-work/information-strategy/clinical-quality-registries/strategic-operating-principles-for-clinical-quality-registries/>).
- ANZDATA circulates patient information sheets to all participating hospitals, for each unit to use to inform patients if they wish
- Specific age appropriate and pictorial information sheets have been developed for children, adolescents and patients with limited English literacy
- Many hospitals have developed their own sheets to meet local needs
- Contact details of the registry are provided for patients to discuss any queries that are not covered in the patient information sheets
- Patients who elect to opt-out of data collection are not included in the registry

2.3 Summary of Privacy Policies

- Patients are entitled to view the information the Registry holds about them, and request alterations if the data is thought to be inaccurate
- Patient names are not included in the locked analysis data set that is used for reporting and data extraction
- Files containing patient names are stored in a separate password protected location with access limited to essential staff members only
- All ANZDATA staff are required to sign a confidentiality agreement, confirming that data will only be accessed for purposes directly related to their work within the registry and that identifiable data will only be accessed when essential
- All staff are required to be familiar with and act in accordance with both the Australian and the New Zealand National Privacy Principles
- All ANZDATA published reports present summary data only in tabular or graphic format.
- ANZDATA does not release data identifiable by patient name except to the patient's treating unit with the expressed approval of the unit's Director or for the purposes of data linkage with specific HREC approval
- All data linkage projects must adhere to strict ethical standards and administrative processes that protect patient privacy
- On occasion, when data identifying particular hospitals is involved, consent from the Director of the relevant renal unit is sought prior to the release of information
- At the time of data collection each unit is asked to certify that they have complied with measures under the relevant privacy measures
- Use and release of tissue typing data, transplant waiting list data, and peritoneal dialysis data provided to ANZDATA by the Australian National Organ Matching System (NOMS) database, the New Zealand Blood Services (NZBS) and Baxter Healthcare require approval by NOMS, the New Zealand Transplant Leadership Team or Baxter Healthcare in accordance with agreements between ANZDATA and these three parties

2.4 Data Security

- Details of ANZDATA's physical and information technology security measures are outlined in policy 3.1 Security Compliance Policy

2.5 Breaches in Privacy

- Any breaches in data security or patient privacy, or near misses, are required to be reported to the ANZDATA executive
- All breaches in security or privacy, the underlying causes and the actions taken to address these, will be reviewed at the monthly ANZDATA Executive meeting
- Where appropriate, the ANZDATA Steering Committee and relevant Heads of Units will be notified of details of a privacy or security breach and actions taken to address this.



ANZDATA Registry
C/O SAHMRI, PO Box 11060
SAHMRI Building, Level 4 South, North Terrace
Adelaide, South Australia 5001
Ph: +61 8 8128 4758 | Fax: +61 8 8128 4769

3.0 Exhibits / Appendices / Forms

4.0 Document History

Revision	Date	Description
2017.1	21/09/2017	Creation
2017.2	15/11/2017	Updated Background to explicitly reference 2014 APPs
2019.1	14/02/2019	Updated 'Summary of Privacy Policies' to capture the use and release of peritoneal dialysis data from Baxter Healthcare