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

Document Number:	3.1
Document Name:	Security compliance policy
Version Number:	2017.2
Effective Date:	15/11/2017

1.0 Purpose

Description of steps taken to ensure physical, operational and technological security of the data collected by ANZDATA.

2.0 Policy Details

2.1 Security measures

Measures put in place to ensure the security of all collected information include the following:

Physical Security

- restricted access to SAHMRI building, floor and offices requiring access cards
- paper forms are in locked storage rooms when archived
- network data is stored on physically secure and separate servers with protective firewalls
- access keys, codes, cards and passwords are controlled by defined and enforced security procedures

Operational Security

- users as part of their employment contract agree to privacy and confidentially standards
- permission levels are restricted to position, with lists maintained
- education and training of new users is anonymised when dealing with patient or unit level information
- procedures are in place for employees leaving the Registry for logins, password and pass cards etc to be cancelled
- passwords are changed regularly and must maintain a level of strength to reduce hacks or reproduction
- deidentification practices are in place for any research or project work

Technical Security

- validation of data is performed to ensure integrity and accuracy
- business continuity is regularly audited and updated
- system software and licenses are maintained, ensuring certification, authenticity, security, anti-theft and anti-virus needs are functioning and up to date

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

Data Transfer Security

- fax location is secure with restricted use and accessibility; confirmation reports and information control procedures are in place
- email guidelines are in place for the transfer of information; lists maintained; encryption and enforced security engaged for transmitting information
- couriered track and trace procedures are used for physical delivery and receipt of paper forms and items are wrapped and boxed for damage control
- secure depot service is used for data/report transfers which meet AUS and NZ information standards

Disposal and destruction

- Paper forms are kept for a maximum of 2 surveys only (the current survey and the one prior) and are destroyed thereafter
- Physical records are destroyed using a secure destructive service
- Computer records are kept indefinitely and hardware physically wiped and destroyed when decommissioned

Data Security Breaches

- An audit tool has been built to track all user activities in accessing the database and entering data. All user activities can be reviewed in the event of a data security breach.
- An error log is produced that records all potential attempts at fraudulent access to the database and other access errors. This error log is reviewed regularly by the Registry manager to detect potential security risks.
- All security breaches and near misses must be reported to the Executive and dealt with in line with ANZDATA's Ethics and Privacy Policy (Document 5.1)

3.0 Exhibits / Appendices / Forms

Nil

4.0 Document History

Revision	Date	Description
2017.1	21/09/2017	Creation
2017.2	15/11/2017	Minor revision regarding auditing trail

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