

6 AODTS–NMDS privacy and data principles

6.1 Introduction

All people participating in the AODTS–NMDS collection are urged to read the AODTS–NMDS privacy and data principles and undertake their role in the collection in accordance with these principles. The principles draw heavily on legislation and standards designed to protect the rights of all involved.

The privacy and data principles are designed to apply to data collected for the AODTS–NMDS collection, from alcohol and other drug treatment agencies, that are transmitted to health authorities in each jurisdiction and to the AIHW for national collation and analysis. Similar principles could be used, however, in data collections more generally.

Under National Privacy Principle 5.1 of the *Privacy Amendment (Private Sector) Act 2000* relevant agencies must set out in a document, clearly expressed policies on their management of personal information. For agencies that have not developed such a policy, the AODTS–NMDS privacy and data principles may be a useful basis or starting point.

Section 6.2 first presents relevant background material and Section 6.3 draws on this material to outline privacy and data principles for the AODTS–NMDS collection.

6.2 Relevant background material

The Privacy Act and Information Privacy Principles

The *Privacy Act 1988* contains 11 Information Privacy Principles (IPPs) which govern the conduct of Commonwealth and ACT Government agencies in the collection, management, use and disclosure of records containing personal information. These principles have stood the test of time in a decade of rapid technical development (see Appendix F for a ‘plain English’ copy).

The *Privacy Amendment (Private Sector) Act 2000* came into effect on 21 December 2001. This Act extends the coverage of the Privacy Act to protect personal information in the private sector. The Amendment Act includes 10 National Privacy Principles (NPPs) which set base line standards for privacy protection by private sector (and non-government) organisations. The Act provides for the development and approval, by the Federal Privacy Commissioner, of sector-specific codes. A working group of the Australian Health Ministers’ Advisory Council (AHMAC) is currently developing a national health privacy code that could operate in the public and private sectors.

The Privacy Commissioner has issued guidelines to explain in a clear and simple way how the NPPs work in practice. Acknowledging that personal health information is generally considered to be amongst the most sensitive and intimate of personal information, the Office of the Federal Privacy Commissioner has issued health privacy guidelines which complement the general NPP guidelines and provide specific guidance on how the NPPs

operate in the private health sector. The Act defines health information as including information or an opinion about the health or a disability (at any time) of an individual (see Appendix G for an information sheet developed by the Office of the Federal Privacy Commissioner). Further information on privacy can be obtained from the Federal Privacy Commissioner's website <www.privacy.gov.au>.

Relevant AIHW data policies

The AIHW operates under the *AIHW Act 1987*, which has strong confidentiality provisions (refer to S29a). Confidentiality principles are documented in the AIHW policy as are procedures in relation to information security and privacy, approved by the Institute's Board, and related data custodianship procedures. These policies and procedures seek to operationalise the principles set out in Appendix F, as well as the AIHW policy and other legislation. The Institute's Ethics Committee approves access to databases under certain conditions.

Some of the AIHW principles relating to data custodianship complement the other material quoted in this paper. Further information on AIHW policy and procedures on information security and privacy is included in Appendix G.

Relevant State and Territory policies and practices

New South Wales

NSW Health is committed to safeguarding the privacy of client information, and has implemented a number of measures to comply with its obligations set out in the *Health Records and Information Privacy Act 2002* (HRIP Act) and the *Privacy and Personal Information Protection Act 1998* (PPIP Act). Generally, individuals should be informed as to what information is being collected, what agency is collecting the information, how it will be used, and their rights in relation to it. Further information on NSW Health's privacy principles and procedures can be found at: <www.health.nsw.gov.au/policies/pd/2005/pdf/PD2005_593.pdf>.

Victoria

The Victorian Department of Human Services is committed to protecting the privacy of personal information and is bound by the Victorian privacy laws, the *Information Privacy Act 2000* and the *Health Records Act 2001*, as well as other laws which impose specific obligations in regard to handling information. Further information on the Department's privacy principles can be found at: <www.dhs.vic.gov.au/privacy/public/index.htm>.

Queensland

Queensland Health respects the privacy of patients and clients, their families, staff members and business partners. Privacy is broader than the traditional concept of confidentiality and includes the collection, use, disclosure, security, quality, access, correction and openness of information. It includes such things as informing individuals when information is collected about them and informing the community about the types of information collected.

Further information on Queensland Health's privacy standard IS42A can be found at: <www.health.qld.gov.au/privacy/>.

Western Australia

The Western Australian Drug and Alcohol Office is committed to ensuring that the confidentiality of patient information is protected and that it meets its legal and ethical obligations to protect the privacy of individuals. It is anticipated that information privacy legislation will shortly be introduced in Western Australia which will contain principles applicable to personal health information. Until state legislation is enacted government policy requires that information sharing by state government organisations complies with appropriate minimum privacy standards such as the Commonwealth National Privacy Principles.

South Australia

Drug and Alcohol Services of South Australia respects confidential information obtained in the course of professional practice and refrains staff from disclosing such information without the consent of the client, except where disclosure is required by law, (e.g. child protection, notification of infectious diseases, an Order of a Court) or is necessary in the public interest.

Tasmania

In Tasmania, Client Information Guidelines have been created to ensure the protection of individual privacy. The Guidelines constitute a set of specific rules which apply to the collection and management of client information by all service providers who deal directly or indirectly with client information and/or have access to the Department of Health and Human Services (DHHS) client information. This includes contracted services, Non-Government Organisations and other agencies that utilise DHHS client information. The client information referred to is that collected, used, held and disclosed by service providers.

Australian Capital Territory

ACT Health has a legislative responsibility to protect the confidentiality of data, to respect the privacy rights of the individuals to whom it relates and to ensure appropriate security arrangements are in place to safeguard the confidentiality of the information provided. ACT Health actively promotes management of personal and sensitive information within privacy guidelines and ensures that data is managed pursuant to legislation in controlled and approved process.

Northern Territory

The Northern Territory Government is committed to ensuring that the confidentiality of client information and the respect and privacy rights of the individual are protected. The Northern Territory is governed by the *Northern Territory of Australia Information Act* as in force 5 May 2004. The Department of Health and Community Services has an Information and Privacy Unit through which any unusual requests for data can be cleared as compliant with the legislation.

Treatment agencies provide client and episode data to the Alcohol and Other Drugs Program (AODP), Department of Health and Community Services. To ensure client confidentiality, names are not requested and a client identifier is used to allow for repeat clients to be monitored. De-identified data is then passed on to the AIHW annually. It is the treatment agency's responsibility to ensure that their client is aware that information recorded will be used, in a de-identified format, for statistical purposes.

Access to the Northern Territory AODP data collection is generally restricted to the AODP

Research and Information Officer and the AODP Research Coordinator. Requests for data must come through to the AODP Research and Information Officer.

Services provided under the Non-Government Organisation Treatment Grants Programme

Services provided under the National Illicit Drug Strategy Non-Government Organisation Treatment Grants Programme (funded by the Australian Government) are required to comply with all relevant Commonwealth, State and Local Government statutes, regulations and by-laws as they apply to their particular Project circumstances.

6.3 Privacy and data principles for the AODTS–NMDS

It is important to note that the people and organisations involved in the AODTS–NMDS collection are custodians of data provided by individuals and agencies. Thus, treatment agencies, jurisdictions and the AIHW do not ‘own’ data. They are, however, responsible for the protection, storage, analysis and dissemination of the data in accord with the purposes for which they were collected.

This section begins by providing a basic outline of the responsibilities of treatment agencies, jurisdictions and the AIHW.

Responsibilities of the treatment agencies

It is the responsibility of each treatment agency to inform every client that data about them will be sent to the Health Authority responsible for the AODTS–NMDS, and then on to the AIHW to become part of a national data set. It is important that the clients of each agency are made aware not only that data are being transmitted to the funding department and the AIHW, but that these data will be used only for statistical purposes and will not be used to affect individual treatment or entitlements.

Treatment agencies are thus responsible for ensuring that all clients whose data are included in the collection are informed of their rights.

Responsibilities of the jurisdictions

Jurisdictions are responsible for ensuring that:

- Treatment agencies are informed that the data they supply to the jurisdiction (Health Authorities) will be passed on to the AIHW for inclusion in the AODTS–NMDS.
- Relevant state/territory or Commonwealth legislation as well as local policies and procedures are referred to when responding to queries in relation to privacy and confidentiality.
- Data dissemination is carried out without compromising confidentiality.

Responsibilities of the AIHW

All AIHW staff with access to AODTS–NMDS data have signed a confidentiality undertaking, which is consistent with the *AIHW Act 1987* and the *Privacy Act 1988*.

For jurisdictions as well as the AIHW, data dissemination must be carried out without compromising confidentiality. Cell sizes of less than 2 or 3 should be thoroughly vetted to see if they compromise confidentiality – at a national level they may not, but with small groups (e.g. main treatment type or with jurisdictions) they may.

The AIHW may release national data, in response to special requests. The following protocols are observed in relation to requests for specific tables from the national database:

- Where national tables are requested from the AIHW, they are vetted to ensure that there are no small cell sizes and copies of the requested tables are sent to all jurisdictions for their information.
- Where tables are requested that require a national breakdown by State/Territory, or where State/Territory only tables are requested, a requestor must make a formal request for access to the AODTS–NMDS. This ‘request for data access’ form is then forwarded to all contributing jurisdictions for approval. If approved by all jurisdictions the requestor will be able to access the data after signing the AIHW confidentiality undertaking signed by all AIHW staff. (See also AODTS–NMDS data access protocols for further information.)

Principles

The following privacy and data principles are based on the key material outlined above and are designed to be consistent with this key material and draw together the material into a concise and holistic document.

The privacy and data principles are drafted under three main headings: ethos, purpose and content, and quality, methods and procedures.

Ethos

E1. Respect: privacy, dignity and confidentiality

The national minimum data set should be defined and collected in a climate of mutual respect:

- All participants in the AODTS–NMDS collection should respect the rights to privacy, dignity and confidentiality of the service user.
- Funded treatment agencies should be respected for their role in providing a valued service and for their need to operate cost effectively and competitively in a mixed economy.
- Service funders should be respected for their role in policy, administration and high level advocacy in the sector, and their associated need to monitor the activities and outcomes of services and the profile and needs of service users.

E2. Fairness and transparency

Data should be collected in accordance with the privacy principles attached:

- Funded treatment agencies should ensure that service users are aware of the data being recorded, the purpose of the recording, and which data will be transmitted to other bodies, including funders and national statistical agencies, and for what purposes.
- Service users should be made aware of their rights to seek access to their records and to correct or update information about them, if it is incomplete, inaccurate or out-of-date.
- Funding departments should ensure that, similarly, funded treatment agencies are aware of the data being recorded, the purpose of recording them, and which data will be transmitted to other bodies including statistical agencies.

- Fairness and openness concerning purposes, data, procedures and release: Jurisdictions and the AIHW should publish clear statements about the purpose of each data item in the AODTS–NMDS, and the purpose of data collection and jurisdictional and national collection, analysis and dissemination. The purpose of data may legitimately extend to the collection of information that, while not immediately related to the service a person receives at a point in time, relates to the continued availability of that service. (For example, the collection of information on ethnicity or Indigenous status may or may not be directly relevant to the provision of service to a service user on a particular day. However this information is regarded as crucial to the effective delivery of the alcohol and other drug treatment service, by establishing the accessibility and equity of the program, and hence ensuring its continuing financial support by governments.)

E3. Custodianship as a principle

- Funded treatment agencies, jurisdictions and the AIHW are the custodians of information collected from service users and funded treatment agencies. They do not ‘own’ data, but are responsible for the protection, storage, analysis and dissemination of the data in accordance with: the purposes for which they were collected; the principles of respect and fairness outlined above; and the quality standards outlined below.

Purpose and content

P1. AODTS National Minimum Data Set principles

- The data items included in a national minimum data set should be nationally relevant and important, and able to be collected consistently and interpreted meaningfully.
- The AODTS–NMDS should contribute to the goals and objectives of the National Drug Strategy.

P2. Cost effectiveness

Including or changing data items imposes costs on all participants in a national collection:

- Data items should, as far as possible, be: consistent with agency and jurisdictional administrative procedures; and able to be effectively collected and transmitted.
- The costs of change to data items or collection methods should be weighed up against the desire for continued improvement in content.

Quality, methods and procedures

Q1. Quality of data items

Data items in the AODTS–NMDS should be: based on national and international standards where appropriate; defined clearly, concisely and comprehensively; in accordance with national information priorities; tested for meaning and feasible collection in the field; and collected and maintained accurately, with opportunities for correction by the service user, the funded treatment agency, the jurisdictional administration and the AIHW.

Q2. Quality of data capture and collection methods

- Funded treatment agencies should attempt to align data items on their administrative forms (e.g. age, sex and Indigenous status) as closely as possible to the AODTS–NMDS items, especially where these conform to national standards for health data definitions.

Q3. Custodianship standards: security of storage and access procedures

'Identifiable information' is defined here to be: individual records containing age and sex that could be related back to an individual (or could enable an individual's identity to be reasonably ascertained), and agency records that could be used to identify an individual funded treatment agency. 'Identifiable information' is different from 'identifying information' where individual names and other identifiers are included (i.e. the individual is identified uniquely and with certainty).

Data custodians are responsible for ensuring data holdings are protected from unauthorised access, alteration or loss.

- Paper-based identifiable information should be kept securely locked away when not in use. The minimum requirements are that information must be accessible only to those who are authorised, and that outside normal working hours, information must be stored in locked drawers or cabinets.
- Particular care must be taken regarding the printout and photocopying of paper-based information – users should stand by printers, photocopiers and fax machines while this material is being printed, copied, sent or received.
- Information users should follow normal practice for the use of UT systems to ensure the security and privacy of in-confidence information stored on computer systems including, but not limited to:
 - user account and password protection, use and management; and
 - automatic screen shutdown or automatic log-off in place on all PCs.
- Identifiable information should not be copied to or held on workstation hard disks, or copied and removed from the data holding without permission of the data custodian.
- Funded treatment agencies must take reasonable steps to destroy or permanently de-identify personal information if it is not longer needed for any purpose for which the information was collected.

Q4. Dissemination and use

- Dissemination and use of the data should be in accordance with these AODTS–NMDS privacy and data principles and those relating to the purpose of the collection.
- Data should be carefully interpreted, and any conclusions drawn based on rigorous and balanced analysis of the AODTS–NMDS data and other relevant information.
- In published tables, the amount of personal information in small cells should be reduced to decrease the potential for identification.
- Published data should be made available, in suitable formats to data providers (e.g. funded treatment agencies) and data subjects (e.g. service users).