

7 Privacy and data principles

7.1 Introduction

Preliminary work on the CSDA MDS redevelopment in 1999 established the importance of developing and refining data principles for the CSDA MDS collections in the course of the redevelopment. Final CSTDA NMDS Privacy and Data Principles are included in the CSTDA NMDS Data Guide, along with practical guidance for agencies about the ethical collection and transmission of service user data. Further privacy procedures are also included in the Network Guide, for use by jurisdiction and AIHW staff.

This chapter outlines the methodology for developing the collection's privacy and data principles, before presenting the principles themselves. The chapter closes with a brief summary of the additional procedural guidelines for funded agencies, jurisdictions and the AIHW.

7.2 Developing the privacy and data principles

The April 2000 planning workshop identified a number of issues that were likely to arise in the course of the CSTDA NMDS redevelopment project. For instance, the disability standards require that information not be sought from clients unless it is necessary for service delivery purposes. The workshop asked: Does the information have to be directly relevant to the immediate service? Or could it also be primarily of policy relevance to the funding body, which cannot justify its expenditure without being able to report on the information? Country of birth is an example of a data item where these questions could arise.

As a result, the project plan stated that issues such as these should be addressed by establishing operational data principles early in the life of the project. These principles could be expanded or revised in the course of the project. They would address:

- privacy and confidentiality principles;
- relevance;
- responder burden and the 'minimum' data set;
- consistency with jurisdictional reporting;
- national consistency, its benefits and the costs of changes to national standards;
- linkage keys and identifiers; and
- data ownership, transmission, storage and release.

These principles might influence what data items are required for different service types.

Relevant source material was identified and included:

- privacy legislation, including the *Privacy Act 1988* (and associated Information Privacy Principles) and *Privacy Amendment (Private Sector) Act 2000* (and associated National Privacy Principles);¹
- the Disability Service Standards; and
- relevant AIHW data policies.

Draft privacy and data principles, based on the above documents, were prepared for FIG comment in December 2000. Jurisdiction FIG representatives were asked to provide both general comment and to investigate the principles in relation to local legislation and procedures (e.g. departmental guidelines in relation to privacy). Following a number of rounds of comment, draft principles were placed on the public AIHW redevelopment web site for public comment in mid-2001. The draft principles were also included in the draft Data Guide, used in Round 3 field testing in late 2001.

7.3 The CSTDA NMDS Privacy and Data Principles

The CSTDA NMDS Privacy and Data Principles, as they appear in the final Data Guide, are included below. Further background detail, including extracts from source documents, is included in the Data Guide.

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 CSTDA NMDS collection should respect the rights to privacy, dignity and confidentiality of the service user.
- Funded 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.

¹ During the course of the project, the *Privacy (Private Sector) Amendment Act 2000* was passed, with legislation effective from December 2001. This legislation extended the *Privacy Act 1988* (covering most government service providers) to non-government or private service providers. The CSTDA NMDS collection draws on data supplied by government and non-government disability service providers and is therefore subject to the eleven Information Privacy Principles (IPPs) for Commonwealth and Australian Capital Territory agencies and the ten National Privacy Principles (NPPs) for private (including non-government) providers. According to the privacy legislation, data collected under the CSTDA NMDS are health information and therefore personal information that is also sensitive in nature.

E2. Fairness and transparency

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

- Funded agencies should ensure that service users are aware of the data being recorded, the purpose of recording, and which data will be transmitted to other bodies, including funders and national statistical agencies, and for what purpose.²
- Service users should be made aware of their right 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 agencies are aware of the data being recorded, the purpose for recording them, and which data will be transmitted to other bodies including national 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 CSTDA NMDS, and the purpose of data collection and jurisdictional and national collation, 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 origin may or may not be directly relevant to the provision of a service to a service user on a particular day.

² In accordance with AIHW Ethics Committee guidelines, each jurisdiction has provided written confirmation that:

1. Agencies participating in the CSTDA NMDS collection will be informed of the collection's Privacy and Data Principles, which outline their legal obligations under the *Privacy Act 1988* and the *Privacy (Private Sector) Amendment Act 2000*, and refer them to the Acts themselves.
2. The 'information subjects' (people with a disability who are the service consumers) will be informed about the information being recorded and its purpose, as well as their right to access the information and update or correct it. The following paragraph has been approved for this purpose:
 - Please note that <agency name> is required to release information about service users (without identifying you by full name, or address) to <CSTDA funding dept name>, and to the Australian Institute of Health and Welfare, to enable statistics about disability services and their clients to be compiled. The information will be kept confidential. This information is used for statistical purposes only and will not be used to affect your entitlements or your access to services. As a user of CSTDA-funded services you have the right to access your own files and to update or correct information included in the CSTDA NMDS collection.
3. The unit record file will not be matched, in whole or in part, with any other information for the purposes of attempting to identify individuals, nor will any other attempt be made to identify an individual.
4. The person/organisation will not disclose, release or grant access to the information to any other person or organisation, except as statistical information that does not identify an individual.
5. The information will be used only for statistical purposes and will not be used as a basis for any legal, administrative or other purpose.
6. Any deviations from the standards are detailed below, including how alternative arrangements accord with relevant privacy legislation.

However this information is regarded as crucial to the effective delivery of the CSTDA program, by establishing the accessibility and equity of the program, and hence ensuring its continuing financial support by governments.)

E3. Custodianship as a principle

- Funded agencies, jurisdictions and the AIHW are the custodians of information collected from service users and funded agencies. They do not 'own' data, but are responsible for the protection, storage, analysis and dissemination of the data in accord 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. CSTDA 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 CSTDA NMDS should contribute to the goals and objectives of the CSTDA.

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 reporting procedures; and able to be efficiently 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 CSTDA NMDS should be: based on national and international standards where appropriate; defined clearly, concisely and comprehensively; in accord 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 agency, the jurisdictional administration and the AIHW.

Q2. Quality of data capture and collection methods

- Funded agencies should attempt to align data items on their administrative forms (e.g. age, sex and Indigenous origin) as closely as possible to the CSTDA NMDS items, especially where these conform to national standards for community service data definitions.
- Jurisdictions should attempt to ensure related new policy and service developments (e.g. service definitions and assessment methods) can be mapped to the information framework of the CSTDA NMDS data concepts, to promote quality, consistency and continuity of national data.

Q3. Custodianship standards: security of storage and access procedures

'Identifiable information' is defined here to be: individual records containing age, sex and statistical linkage key components 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 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 their 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, the 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 IT 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 agencies must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information was collected.
- In relation to the collection of the statistical linkage key components, the AIHW Ethics Committee has recommended protocols which are in place by agreement between all jurisdictions and the AIHW. These protocols include advising the service user that information about them will be released to the relevant funding body and the AIHW. However, this information will not identify the service user by full name or address and will be kept confidential, i.e. securely stored and released in a non-identifiable form (see also previous footnote).

Q4. Dissemination and use

- Dissemination and use of the data should be in accord with these CSTDA 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 CSTDA 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 agencies) and data subjects (e.g. CSTDA service users).

7.4 Statistical linkage key

The statistical linkage key is made up of a number of components collected in the CSTDA NMDS:

- selected letters of surname;
- selected letters of given name;
- date of birth; and
- sex.

These components are combined into a 14-character key that is used in analysis to statistically reduce the incidence of multiple counting of service users across CSTDA-funded service types, and to enable an estimate of the actual number of service users at a point in time to be obtained. (Further information on the use of the statistical linkage key can be found in AIHW 2002a, Appendix 4). The statistical linkage key used in the CSTDA NMDS was initially developed for the Home and Community Care (HACC) Minimum Data Set.

The DSSC first discussed the statistical linkage key in relation to the CSDA MDS collection in June 1998. From these discussions it was decided to pilot test the linkage key in selected jurisdictions in the 1998–99 CSDA MDS snapshot collection

For the original pilot of the statistical linkage key in 1998–99, the AIHW prepared a submission to the Institute’s Ethics Committee for consideration. The Ethics Committee approved the submission subject to each participating jurisdiction providing written conformation that:

- the ‘information subjects’ (people with a disability who are the service users) will be informed about the information being recorded and its purpose.
- the unit record file will not be matched, in whole or in part, with any other information for the purposes of attempting to identify individuals, nor will any other attempt be made to identify an individual.
- the person/organisation will not disclose, release or grant access to the information to any other person or organisation, except as statistical information that does not identify an individual.
- the information will be used only for statistical purposes and will not be used as a basis for any legal, administrative or other.

Following a successful pilot, the linkage key became an ongoing feature of the collection, and these conditions remained in place for all participating departments. All departments confirmed their conformity with these conditions, with variations depending on jurisdictional arrangements, particularly concerning client information and ‘opt out’ arrangements.

The linkage key has been an invaluable tool with the collection, not only for its original purpose of removing double counting and enabling more precise estimates of client numbers to be made – an essential capacity for analysis of the extensive new data in the redeveloped collections. It has also enabled analysis of patterns of multiple service use to be carried out (see AIHW 2002a). Moreover, the linkage key has identified some data inconsistencies in near-matching records, thereby enabling data quality to be enhanced.

The statistical linkage key is a probabilistic linkage mechanism, with a small but non-zero error rate. It is not a unique personal identifier.

7.5 Privacy procedures

The CSTDA NMDS Privacy and Data Principles were developed by the AIHW, in consultation with the FIG, to ensure that privacy issues are adequately addressed in the redeveloped CSTDA NMDS collection. This section provides a basic outline of the responsibilities of funded agencies, jurisdictions and the AIHW.

It is important to note that the people and organisations involved in the CSTDA NMDS collection are custodians of data provided by individuals and funded agencies. Thus, funded 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 as well as the principles of respect and fairness and the quality standards outlined in the CSTDA NMDS Privacy and Data Principles.

Responsibilities of funded agencies

It is the responsibility of each CSTDA-funded agency to inform every service user that data about them will be sent to the CSTDA funding department, and from there to the AIHW to become part of a national data set. It is important that the service users 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 entitlements.

Funded agencies are thus responsible for ensuring that all service users included in the collection are informed of their rights and shown the client rights statement (see footnote on page 58).

Responsibilities of jurisdictions

All jurisdictions have signed an undertaking agreeing to the privacy arrangements established for the CSTDA NMDS (see footnote on page 58 for an example undertaking).

Jurisdictions are also responsible for ensuring that:

- all jurisdiction staff involved in the CSTDA NMDS collection are familiar with the collection's Privacy and Data Principles, including the client rights statement and the jurisdiction undertaking;
- the CSTDA NMDS Privacy and Data Principles are included in the Data Guide sent to each funded agency;
- information about the principles and procedures is included in training for funded agencies;
- 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; and
- data dissemination is carried out without compromising confidentiality.

Responsibilities of the AIHW

All AIHW staff with access to CSTDA NMDS data have signed a confidentiality undertaking, which is consistent with the *AIHW Act 1987* and the *Privacy Act 1988*. In addition to adhering to the CSTDA NMDS Privacy and Data Principles, the AIHW has its

own policy and procedures on information security and privacy. Excerpts from this document are provided in Section 6 of the Data Guide.

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. disability groups 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.
- Where tables are requested that require a national breakdown by State/Territory, tables are sent to jurisdictions before going to the requestor.
- Where State/Territory-only tables are requested (i.e. jurisdiction-specific data), people are referred to the relevant jurisdiction for provision of the data.

Access to the national database is only provided under strict conditions. A potential researcher must make a formal request for access to CSTDA NMDS. This 'request for access' form is then forwarded to all contributing jurisdictions for approval. If approved by all jurisdictions the researcher will be able to access the data after signing the AIHW confidentiality undertaking signed by all AIHW staff.