

7 Privacy and confidentiality of data

7.1 Privacy—an introduction

Privacy and confidentiality must be considered whenever data about individuals, service provider organisations or funding departments are collected or disseminated. Privacy legislation is concerned with the handling of personal information. Personal information includes an opinion, whether true or not, no matter how it is recorded, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

The *Privacy Act 1988* (the Act) requires Commonwealth public agencies to comply with specific standards when handling personal information. Commonwealth agencies include Ministers, Departments, the Australian Federal Police, the Federal Court etc. The Act also applies to Australian Capital Territory government agencies. The standards for the handling of personal information by Commonwealth agencies are contained in the 11 Information Privacy Principles (IPPs) in the Act.

The *Privacy Amendment Act, 2000* came into operation on 21 December 2000. It introduced similar provisions for private sector organisations which, from 21 December 2001, also have to comply with personal information standards. For private sector agencies, 10 National Privacy Principles (NPPs) generally apply. Or, a private sector organisation may be subject to an Industry Approved Privacy Code, which must deliver a level of protection no less than that provided by the NPPs.

There are also special requirements in respect of ‘sensitive information’ and ‘health information’ (which is both sensitive and personal). See Appendix D for the full listing of the IPPs and NPPs.

Some states and territories also have legislation governing the handling of different types of personal, health or sensitive information.

Summary of requirements for Commonwealth agencies (IPPs) and private organisations (NPPs)

The IPPs and NPPs set out rules relating to the collection, use and disclosure, storage and handling, quality and security of personal information by Commonwealth agencies and private sector organisations.

The IPPs and NPPs give individuals the right to ascertain what information an agency holds about them and the right to ensure the information is accurate.

The IPPs and NPPs can be summarised by 3 basic principles:

1. Agencies/organisations must tell people what information they are collecting and what they will do with it (i.e. the purpose and uses of that collection).
2. Whenever possible, agencies/organisations should get an individual’s consent or give them an opportunity to ‘opt out’ before collecting, using or disclosing information about them.
3. Agencies/organisations should give people confidence that they respect their personal information and will treat it accordingly.

7.2 Privacy and the AIHW

The AIHW's functions are to:

- identify and meet the information needs of government and the community to enable them to make informed decisions to improve the health and welfare of Australians;
- provide authoritative and timely information to the Commonwealth, state and territory governments and non-government clients through the collection, analysis and dissemination of national health, welfare, housing assistance and community services data; and
- develop, maintain and promote, in conjunction with stakeholders, information standards for health, welfare, housing assistance and community services data.

As a Commonwealth agency, the AIHW must comply with the IPPs set out in the Act. The AIHW is **also** bound by its own legislation, the *Australian Institute of Health and Welfare Act 1987*, which contains a section on confidentiality (s29).

In summary s29 states:

- A person who holds any information concerning another person, due to their employment at the AIHW, or due to the fact they are performing a duty or function for the AIHW, or doing any act as a result of any arrangement entered into by the AIHW, shall not directly or indirectly:
 - divulge that information to any person
 - give a document containing that information to any person
 - be required to divulge that information to a court
- Nothing prohibits a person holding information concerning another person (as stated above) from:
 - divulging information to the Minister if it does not identify the information subject
 - divulging information to the information provider
 - divulging information to a person specified in writing by the Ethics committee if to do so is not contrary to the written terms upon which the information was divulged initially by the information provider (only applies to health related statistical information)
 - publishing conclusions based on statistics derived from the work of the AIHW if to do so is not contrary to written terms upon which the information provider divulged the information directly to the AIHW.

AIHW policy and procedures on information security and privacy

(Excerpt from *AIHW Information Security and Privacy Policy and Procedures* document).

The provisions of the *Privacy Act 1988* and the Information Privacy Principles establish the framework for the collection, storage, use and release of all personal information in the public sector. The AIHW policy complies with the requirements of the *Privacy Act 1988* and in addition, covers issues of specific relevance to the AIHW, including s29 on confidentiality contained in the *AIHW Act 1987*.

Privacy ethos

1. All AIHW and Collaborating Unit staff must have a knowledge of section 29 and a good understanding, in relation to the work they do, of the implications of:

- The *Australian Institute of Health and Welfare Act 1987*, section 29
 - The Information Privacy Principles.
2. All AIHW and Collaborating Unit staff must sign the Institute's *Undertaking of confidentiality – Employees*.
 3. The Institute will ensure that its various Collaborating Units maintain a consistent privacy and security ethos.
 4. All work performed by consultants, contractors, seconded staff, visiting fellows and students working under supervision of the Institute which involves access to information collected under the AIHW Act and other identifiable information, must be authorised by contracts which impose information and privacy security requirements at least as stringent as those applying to Institute employees.

Information gathering and receipt

5. Information may only be collected and held for the purpose of AIHW activities.
6. Identifiable information may only be collected and held with the approval of the Institute's Ethics Committee.
7. Any information collected must be limited to that directly relevant to the aims and objectives of an approved project.
8. All data holdings containing identifiable information must be recorded and managed in accordance with the Institute's *Guidelines for custody of AIHW data*.
9. Except as outlined in paragraphs 10 and 11 below, the consent of information subjects for the use of their information should be obtained when the identifying information is in the form of identified records held indefinitely on registers used to contact the information source for research purpose (all such research must be approved by the Ethics Committee).
10. Otherwise, consent should not be required provided that appropriate guarantees are given that the information will be handled in a secure environment, the public good benefits of the research are clear and its use will have no impact on those individuals whose information is being used. As far as is possible, an opt out option should be provided.
11. Regardless of whether consent needs to be obtained, information subjects should be advised, by whatever mechanism is appropriate, why their information is being collected, how it is to be used, who will be using it, the type of access that will occur and how it will be protected.

Information storage, retention and destruction

12. Data must be stored to meet the storage and archival requirements of the National Archives of Australia, and in accordance with the Institute's *Guidelines for custody of AIHW data*.
13. Data Custodians are responsible for ensuring their data holdings are protected from unauthorised access, alteration or loss.
14. Paper-based identifiable information must be kept securely locked away when not in use. The minimum requirement is that, outside normal working hours, the information must be stored in locked drawers or cabinets.
15. Particular care must be taken regarding the print out and photocopying of paper-based information. Users must stand by printers and photocopiers while this material is being printed or copied.

16. Information users must follow normal practice for the use of IT systems (see the IT Security Manual) to ensure the security and privacy of in-confidence information stored on computer systems.
17. Identifiable information must not be copied to or held on workstation hard disks.
18. Wherever possible, identifiable information and associated attribute information should each be stored separately in databases to minimise any risk from unauthorised access.
19. Identifiable information must not be copied or removed from Institute premises without specific approval from the relevant Data Custodian.
20. Normally, data holdings used in support of the Institute's Work Program must be retained for a specified period in order to allow later verification of the research, and in accordance with undertakings given to data providers.
21. Decisions regarding retention of databases lies with Data Custodians, and must be taken in accordance with the Institute's *Guidelines for custody of AIHW data*.
22. The Institute will maintain a physical security system, which provides reasonable and properly enforced measures to protect both staff and its repositories of personal information.

Information transmission

23. If identifiable information is sent by post, registered or certified mail or safe hand delivery must be used.
24. The electronic transmission of identifiable information must apply procedures for the certification of transmission and the encryption of information which are at least commensurate with that used for transmission by post.

Information retrieval and use within the Institute

25. Rather than treating ownership (of data) as an indivisible entitlement, it should be treated as a 'basket of rights' in relation to the information concerned, and there should be acceptance that different parties may have different entitlements. The 'basket of rights' would include the right to do the following, for statistical purposes:
 - gain access to information;
 - amend the information;
 - use the information;
 - disclose the information; and
 - control who can do these things and under what conditions.
26. Data Custodians may approve use, within the Institute, of identifiable information for purposes consistent with those for which it was collected, in accordance with the Institute's *Guidelines for the custody of AIHW data*.
27. In published tables, the amount of information in small cells should be reduced to minimise the potential for identification. Aggregations of data with small cell sizes, which may enable inferences about or identification of individual entities, should not be published.

Conditions applying to data linkage projects

28. Ethics Committee approval is required for record linkage projects. Before granting such approval, the Committee must be satisfied that:

- the 'public good' benefits to be reasonably expected from them will be significant; and
 - 'best practice' procedures will be adopted throughout the conduct of the studies
29. It is not necessary for the Institute to obtain the consent of information subjects for the use of their information in record linkage studies if:
- their identity is irrelevant (except to facilitate the linkage process);
 - the objective is data analysis;
 - no administrative action will be taken in relation to the individuals concerned.
30. The Institute will not permit its data to be linked for client management or regulatory purposes.

Information release and disclosure outside the Institute

31. The AIHW Act allows the Institute to release or disclose identifiable health information to third parties, subject to s29 of the AIHW Act.
32. Requests for access to, or release of identifiable information from a database must be in writing. Any person or organisation wishing to access an Institute database for research purposes should prepare an adequate written proposal for the study following the Institute's *Guidelines for the preparation of submissions for ethical clearance*.
33. Any requests for release or disclosure of identifiable information must be scrutinised by the appropriate Data Custodian in accordance with the Institute's *Guidelines for custody of AIHW data*.
34. If the information requested can be provided under the information provider's constraints, and its release would not contravene s29 of the Act, but the information cannot be provided under an existing Ethics Committee approval, then an opinion must be obtained from the Committee. In this case the appropriate Data Custodian should provide the information requested with documentation necessary for submissions to the Committee.
35. The Institute should endeavour to identify potential disclosure requirements at the commencement of a project and, where appropriate, to build these into the agreements with information providers and into submissions to the Institute's Ethics Committee. Such action can be used to obtain information provider and ethical approval in advance, thereby streamlining the release process.
36. Staff should take particular care to ensure that no release, publication or public presentation or discussion of individual records or results of research could breach the requirements of this Policy. Results shown in tables with small cell values often need special attention (see paragraph 25.)

The Institute in an agency role

37. Data providers, such as Registrars of Births, Deaths and Marriages in states and territories, supply data to the Institute for the Institute's purposes. The Institute reformats these data and produces national data sets. These data sets may be returned to the Registrars.
38. Should Registrars wish to furnish the national lists of births and deaths to other agencies for their own purposes, Institute staff may assist the Registrars with these tasks, acting as the Registrar's agent.
39. At all times, it must be clear that the work is being undertaken as an agent of the Registrars.

Monitoring and audits

40. The Institute's Board requires that security audits be carried out as part of the Institute's audit program.
41. Compliance and quality control will be assessed by routine data audits. Results will be reported to the Board's Audit and Finance Committee.

Breaches and sanctions

42. The Institute relies on the diligence of all staff in preventing breaches of information security.
43. If a breach is thought to have occurred it should be reported immediately to the Director through normal Divisional/Collaborating Unit reporting channels.
44. The Director may appoint a person to investigate the circumstances of a suspected breach. If a breach is proven the Director may initiate disciplinary or legal action under the relevant legislation.
45. Details of suspected breaches will be treated as STAFF-IN-CONFIDENCE information at all times.
46. The Institute's Fraud Control Guidelines and Plan (available to staff on the Intranet) are also relevant.

AIHW Ethics Committee

(Excerpt from *Guidelines for the preparation of submissions for ethical clearance* document)

The AIHW Ethics committee (appointed under s16(1) of the *Australian Institute of Health and Welfare Act*) may, under strict conditions, allow the release of information to researchers proposing studies judged to have scientific merit and that meet the required data confidentiality standards. The following criteria upon which the submissions will be evaluated include:

Purpose of the proposal

- The Committee will only approve use of information for research purposes. A key criterion is that the research output is to be put in the public domain. Regulatory, legal and administrative purposes are not acceptable, unless there is an overriding public good and no detriment to the information subject.

Research focus of the proposal

- The Committee will only approve research that has recognition of relevant ethical considerations, including social and cultural factors, by all involved in the conduct of the activity, and their commitment to upholding ethical standards.
- The Committee will also take into consideration a project's overall value to society and the predicted outcome of activities in relation to possible risks such as the comfort and privacy of information subjects.

Scientific validity of the proposal

- The Institute has the responsibility only to submit to the Committee proposals that it considers as scientifically valid.

- The Committee has the right to raise queries about scientific validity if it sees fit, and to refer them to the Institute.
- The submission should be signed off by the responsible Data Custodian.

Approval by the applicant's own institutional ethics committee

- All applications other than applications by the Institute before the Committee need to be approved by the applicant's own institutional ethics committee.

Organisational framework of the researcher

- Consideration will be given to whether there is an established accountability mechanism, [e.g. an institutional ethics committee], that can impose sanctions if necessary.
- The Committee may approve an agreement between the Institute and other organisations for the use of the Institute's data in classes of research projects so that the organisation can release identifiable AIHW data subject to the approval of its own Ethics Committee.

Credentials and technical competence of the researcher

- The qualifications, competence and expertise of personnel engaged in the activities will be considered.

Extent to which privacy and consent issues have been addressed

- The Committee will take into account the privacy provisions contained in *Minding our own business* which is the privacy protocol for Commonwealth agencies in the Northern Territory handling personal information of Aboriginal and Torres Strait Islander people.
- The Committee will only approve research projects where the protection of the wellbeing and privacy of the subjects, and also of persons who collect, communicate, work with or have access to the information about them is assured.
- The Committee will be mindful of legal requirements, in particular the pertinent sections of the AIHW Act, and the *Privacy Act 1988* and the current *Guidelines for the protection of privacy in the conduct of medical research* as approved by the Privacy Commissioner.
- If further information is needed from information subjects, the Committee will seek their consent to an approach by the principal investigator.
- The Committee will not require informed consent where this is not necessary.

Adequacy of researcher's data security protection mechanisms

- The Committee must be assured that the maintenance of adequate degrees of confidentiality of information about identifiable persons (and, in certain cases, of groups of persons) is enforced.
- The Committee must also be assured of the physical security of data, covering the security access system to the building, storage rules for hard copy of data, computer security procedures and the disposal of data when no longer required.

Commitment to, and method of publishing results of research

- The Committee considers it important that the results of research are disseminated to the appropriate groups, communities and individuals. Therefore, the dissemination plan will be carefully considered in each submission. The Committee requests that a copy of the

published work be made available to it and may also request that a summary of the research be made available on the AIHW web site.

- The Committee does not give approval to projects where there is no intention to publish results. The 'Undertaking' signed by researchers, allowing for legal disclosure of information by the AIHW, specifies that the AIHW must be acknowledged as the source of data in any publication, and that a copy of any published material must be supplied to the AIHW.

Transfer of data out of Australia

- This will not normally be approved, but can be on a case by case basis where the overseas data holder and their organisations are of undoubted quality.

For more information on the AIHW Ethics Committee, refer to <http://www.aihw.gov.au/committees/ethics/index.html>.

Data Custodians at the AIHW

(Taken from *Guidelines for custody of AIHW data* document)

Whilst all staff at the AIHW share responsibility for maintaining the security of AIHW data, data custodians have overall responsibility for the security of specified data collections. Once the *data custodian delegation* instrument is signed, the custodians assume the responsibility of the director in regard to the data in their custody. The relevant unit head is given the responsibility of data custodian. The custodianship is vested in a position rather than a named person.

Data Custodians ensure that data holdings within their unit are properly documented, maintained and controlled, and ensure an appropriate level of consultation with other units regarding the data resources within the Institute. This includes responsibility for:

- Recognising and abiding by all limitations placed on data.
- Maintaining up-to-date documentation, including Datacatalogue entries, of the content and format of the data holding and of the constraints applying to its use and/or release.
- Authorising and recording users of the data within the AIHW, and providing advice and assistance to new users on any constraints which apply.
- Assisting potential users wishing to access identifiable data in the preparation of their proposals for submission to the Health and Welfare Ethics Committees (see *Guidelines for the preparation of submissions for ethical clearance*).
- Following Ethics Committee approval, arranging for the secure transfer of data to recipients in accordance with constraints imposed regarding the use of data. Working with the Ethics Committee Secretariat with their monitoring processes.
- Ensuring, when required, the appropriate destruction (or return to the original information provider) of the data holding.