Australian Government | National Statistical Service

Statistical Data Integration involving Commonwealth Data

Application for accreditation as an Integrating Authority against the interim accreditation scheme

Summary version

Applicant:	Australian Institute of Health and Welfare
Auditor:	Protiviti
Date accredited:	28 June 2012

The Australian Institute of Health and Welfare (AIHW) provides reliable, regular and relevant information and statistics on Australia's health and welfare. It is an independent statutory authority governed by a management Board, and accountable to the Australian Parliament through the Health and Ageing portfolio.

The AIHW has about 400 staff skilled in statistical analysis, epidemiology and demography, information development, data management, communication and public sector administration. Collaborating units based at universities bring specialist knowledge to areas such as asthma, dental health, injury, and perinatal and maternal health.

The summarised application can be found on the following pages of this file. For further information about the application contact:

The Cross Portfolio Data Integration Secretariat

Phone (02) 6252 7198

Email: statistical.data.integration@nss.gov.au

Criterion I – Ability to ensure secure data management

Auditor rating against criterion I – compliant

I(a) How does your agency adhere to the separation principle? Provide details of how only that information, from datasets to be linked, that is required to perform specific tasks is made available to those people performing the tasks. Specifically:

- linking separation (where those people performing the linking of the datasets can only access those parts of the datasets to be linked that are required to complete the linkage)
- analysis separation (where those people performing analysis of the lined datasets can only access those parts of the datasets required for the analysis).

Important Note. Unless otherwise specified, the responses to this and all other questions refer to high risk data integration projects involving Commonwealth data.

In order to apply the separation principle, data integration in AIHW is undertaken in 3 distinct stages:

- Separation
- Linkage
- Merging (or integration)

Data Integration Services Centre (DISC) staff only have access to those data sets required for the particular operation they are undertaking at any point in time. Staff undertaking linkage can only access identifying variables (such as names and dates of birth); staff undertaking merging can only access content variables; and staff undertaking data analysis can only access de-identified and appropriately confidentialised integrated datasets.

In addition, a further extension of the separation principle can be achieved using combinations of 'external' and 'internal' separation and merging. External separation and internal merging (in conjunction with controlled data access such as a data laboratory) provides the strictest control over privacy and data access. Note that the AIHW offers the various separation options to data custodians during project initiation.

External Separation

In external separation, the data custodians identify, with assistance from DISC, linkage and content fields and separate the data into a linkage file and a content file. The linkage file is then delivered to the project-specific linkage domain within DISC and the content file is delivered to the DISC project-specific merging domain. This means that DISC staff can only access either the identifiers OR the content but never both.

External separation can be further enhanced by data custodians exercising an option to withhold the provision of content fields until after the linkage has been undertaken. In this case, project specific record identifiers for linked records (i.e. those likely to be matches) are passed back to data custodians to attach to the content fields. The data custodians need only then forward content for matches likely to be linked. Post-linkage content provision is only appropriate if the integrated dataset comprises only linked records (rather than linked and unlinked records).

Internal Separation

In internal separation the linkage and content fields are separated within DISC. To maintain privacy, separation is only carried out in a separate domain by staff with a project specific data separation role.

Linkage Separation

Linkage is conducted using the linkage fields only and is undertaken in a project specific linkage domain only accessible by DISC staff with a linker role for that project.

Merging Separation

Merging (or integration) brings together content fields using project-specific linkage keys so that identifiers are never exposed.

Analysis Separation

Analyses of integrated data will only be undertaken by DISC staff that have been granted an Analyst role or approved researchers who have been granted a Data Laboratory User role. DISC staff who have had a project specific Linker, Separator or Merger role for a high risk integration project will not be granted an Analyst role within that project.

For analyses within DISC by DISC staff a project specific analysis domain will be set up for the project. This domain will only be accessible (apart from auditing purposes) to DISC staff with an Analyst role for that project.

For analyses within the Data Laboratory a project specific and researcher specific domain will be set up for the project and researcher. For the same project a separate domain is set up for each individual researcher and is only accessible (apart from auditing purposes) to that researcher.

Only output that has been cleared of statistical disclosure risk by the DISC Data Laboratory Output Reviewer and approved for release by the project manager can be released from the Data Laboratory or the analysis domain (see Criterion II).

I(b) How does your agency's audit program (internal and external) ensure the continued security of data? *NOTE: If your agency complies with the Australian Government Protective Security Policy Framework (and can demonstrate this to the auditor) the remaining questions under criterion I do not need to be answered so proceed to question IIa. Otherwise, please complete the following questions.*
The AIHW has three levels of auditing to ensure the security of data. (1) Internal Audit The AIHW Board is the governing body of the Institute and is accountable to the Parliament of Australia through the Minister for Health and Ageing. A subcommittee of the AIHW Board, the Audit and Finance Subcommittee, authorises and oversees the AIHW's audit program and reports to the AIHW Board on financial and data audit matters. (2) Data integration-specific audits and reviews A regular program of data-integration specific audits has also been established by DISC with a similar ongoing program established within the AIHW internal audit program. (3) 'Ethics Committee' audits The AIHW Ethics Committee and Board have agreed that a program of audits of 'critical data sets' be developed and implemented based on the level of risk and significance of each collection.
I(c) Do employees (including contractors) undergo police checks upon employment?
Yes, as a condition of employment at the AIHW all new employees (including contractors) engaged for more than six weeks must complete a police records check. Employees or contractors that have not completed a police check cannot be employed in the Data Integration Services Unit under any circumstances.
I(d) How is access to the agency's premises controlled? Provide details.
Access is controlled via swipe card to the AIHW buildings. Visitors are escorted at all times (and must wear a 'Visitor' pass). Access to the DISC is controlled via a further layer of swipe cards issued to DISC staff only, visitors to the secure area must sign in and be accompanied at all times.

I(e) How is your agency's Internet gateway secured?
AIHW connects, via the Intra Government Communications Network (ICON), to a Defence Signals Directorate (DSD) - accredited internet gateway provider. As such, AIHW 's internet gateway is certified to the PROTECTED level. Further, DISC projects are undertaken on a separate secure network.
I(f) Does your agency have an Information Security Policy and procedural plan (including protective control of data, secure ICT access and documented procedures)? Please specify key elements of your Information Security protocols.
Yes, the AIHW has an Information Security Policy that covers: • Privacy Ethos • Information Gathering and Receipt • Information Storage, Retention and Destruction • Information Transmission • Information Retrieval and Use Within The Institute • Conditions Applying To Data Linkage Projects • Information Release and Disclosure Outside The Institute • Monitoring and Audits • Breaches and Sanctions

Criterion II – IAs must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users

Auditor rating against criterion II – compliant

II(a) How will safe data access be provided?

Please provide details of the proposed method. For example:

- providing access to data that are not likely to enable identification of individuals or organisations via on site data laboratories
- providing access to data that are not likely to enable identification of individuals or organisations via secure remote access facilities
- review of data by appropriately skilled internal staff to ensure data is appropriately confidentialised before release
- provision of only confidentialised files to users (e.g. using formal algorithms to apply confidentiality)
- other - specify.

As an extra protection, in addition to one of the methods above, IAs may also restrict access to endorsed applicants (similar to the restrictions placed on access to Confidentialised Unit Record Files by the ABS, for example).

NOTE: Any of these options is acceptable provided the applicant can demonstrate safe practices. The application will need to include details of how the IA confidentialises data.

The AIHW has six protective protocols aimed at ensuring that information that is likely to enable identification of individuals or organisations is not disclosed.

First, approval to access unit record files (always de-identified and confidentialised where appropriate) is only ever granted by an independent body – the AIHW Ethics Committee. This ensures that AIHW staff and users and potential users are at arms-length and that staff cannot be unduly influenced. The Ethics Committee is established according to the AIHW Act. The AIHW Director is one of the members, the remaining members are independent of the AIHW.

Second, access to these files is only ever granted to users for purposes agreed to by the Ethics Committee.

Third, users are subject to the penalties for disclosure laid out in the AIHW Act (a fine of $2,000 or imprisonment for 12 months, or both) and must sign the undertakings contained in the Ethics Committee application form at http://www.aihw.gov.au/ethics/

Among other things, these undertakings aim to ensure that:

- 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 to identify an individual be made
- the person/organisation will not disclose or release the information to any other person or organisation, except as statistical information that does not identify an individual

- access to the unit record file will be restricted to only those employees of the organisation who are directly responsible to the Principal Investigator. The Principal Investigator will explain to any employees granted access to the information the provisions of the AIHW Act prohibiting release of the information to others
- access will not be granted to any other organisation without specific approval of the AIHW Ethics Committee
- the information will be used for statistical purposes in health and/or welfare research
- the information will not be used as a basis for any legal, administrative or other actions that could directly affect any particular individuals or organisations as a result of their identification in this project
- the recipient will cooperate with any surveillance procedures established by the Institute or its Ethics Committee and advised to the recipient in writing.

The fourth protective arrangement is to release data in such a way that identification is unlikely. De-identification automatically occurs as part of the data integration process and confidentialisation of researcher output is achieved by first undertaking, on a case-by-case basis, a statistical risk assessment and then applying appropriate disclosure control techniques such as limitation of detail, top/bottom coding, field suppression, value substitution, rounding and the addition of noise. The arrangements are described in more detail in the DISC Operations manual.

Fifth, access to confidentialised, de-identified microdata is only possible in the DISC Data Laboratory as described below.

The final and sixth layer of protection is screening of the output produced by researchers. This ensures that unit records are not removed from the Data Laboratory and only aggregate data that does not pose a statistical disclosure risk is removable.

DISC Data Laboratory

The DISC Data Laboratory provides a secure access environment for researchers to perform analysis on de-identified and appropriately confidentialised datasets.

Researchers can access the datasets provided and use familiar analytical packages (e.g. SAS, SPSS, Stata, R) but they cannot remove files from the laboratory without these being cleared for statistical disclosure risk by DISC staff.

Data Laboratory Security/Researcher Oversight

The Data Laboratory is a physically secure room within the AIHW. Access to the room is controlled by key carded entry, which is restricted to DISC personnel and approved AIHW facilities and ICT Operations staff. All other staff and external data laboratory users (ie researchers) must sign in to gain entry and must be supervised by DISC staff.

Result Screening and Statistical Disclosure Review of Researcher Output

All analytical output is vetted using appropriate disclosure control methodologies by a DISC staff member who has been allocated a Data Laboratory Output Reviewer role for the specific project.

DISC Mobile Data Laboratory

Where approved by the data custodians, de-identified and confidentialised integrated data may also be migrated to the DISC Mobile Data Laboratory.

The DISC Mobile Data Laboratory is a secure laptop with all contents encrypted using very strong encryption. Two factor authentication is required to access the Mobile Data Laboratory. All input and outputs, including floppy disc drives, optical disc drives, input and output ports (including serial, parallel, USB, video), except for keyboard, mouse and monitor are disabled for all user accounts excluding for those persons with a DISC System Manager role.

The Mobile Data Laboratory can be transported by DISC to staff to an offsite location for use by approved researchers. An approved researcher will be assigned a Data Laboratory User role. While being transported the Mobile Data Laboratory must be stored in a locked case.

DISC staff must ensure that no one tampers with or attempts to remove any data from the Mobile Data Laboratory. No DISC System Manager will access the Mobile Data Laboratory while it is away from AIHW premises.

After cleared output has been removed the Mobile Data Laboratory is completely and securely wiped according to AIHW IT security policy and reimaged before use.

Criterion III – Availability of appropriate skills

Auditor rating against criterion III – compliant

III(a) What expertise and experience does the agency have to undertake high risk data integration projects?

If your agency does not have this expertise or experience, what strategies are in place to acquire the necessary expertise to undertake a high risk integration project?

NOTE: Relevant skills to consider include: expertise in linkage and merging functions; expertise in privacy; expertise in confidentiality; information management skills; ability to provide useful metadata to data users; and appreciation of data quality issues.

Unit Capability

The AIHW has been undertaking data integration projects since the mid-nineties. Both the number of projects undertaken per year and the size and complexity of individual projects has grown substantially since that time. Projects involving the linkage of millions of records and data flows between researchers and custodians, including Medicare and DoHA, are now routinely undertaken.

In the 2010-2011 financial year 87 data integration projects were undertaken by the Institute and it is now recognised as a centre of excellence in national-level data integration projects. The team has demonstrated the capability to apply a broad set of data integration methodologies from probabilistic techniques to the self-developed and ground-breaking techniques for linkage using the community services statistical linkage key.

The AIHW has demonstrated:

- rigorous processes and controls for the protection of privacy and confidentiality;
- detailed knowledge of, and experience with many, national datasets that are already held by the Institute;
- strong information governance (including the ethics committee and other approval processes) and client management (particularly with State and Territory data custodians);
- expertise and experience in the integration of both health and community services data using a variety of methods; and
- technical capability and resources for the manipulation and storage of large complex datasets

Individual capabilities

The team is very highly qualified and experienced with an average of 13 years experience per person undertaking functions relevant to data integration such as statistical methodology and analysis, disclosure control, metadata management and production, computer programming etc.

It is also worth noting that membership of Population Health Research Network (PHRN) confers the benefit of being able to call on other experts if necessary.

The AIHW is always able to attract skilled staff and will look to engage others as required.

III(b) What documentation and training is available to ensure staff have the appropriate skills and knowledge required in high risk data integration projects?

The AIHW provides an active learning and development program with a focus on supporting relevant statistical, analytical and writing skills. There is an emphasis on participation in learning activities that have a clear connection with the Institute's overall work program, have a link to Unit work plans and priorities, assist employees' ongoing skill and career development and assist employees to develop skills in general management matters including workplace relations. Learning and Development is broadly defined as any activity that develops the skills and knowledge of staff and it is recognised that learning and development needs and opportunities will differ for each individual.

DISC-Specific Documentation and Training

On commencement with DISC, staff are given a checklist of competencies to achieve in the first six months. For new staff this is integrated with the six-month probation period process, for other staff it is integrated with the standard AIHW six-monthly performance review. The staff member will work with their immediate supervisor to ensure that they receive sufficient on-the-job training, materials, courses and other opportunities to develop the required competencies. The areas in which DISC staff need to be proficient are listed below.

- Project management processes;
- Ethics, Privacy and Confidentiality;
- Technical skills;
- Business and workflow processes; and
- Client relationships

The DISC Operations Manual details competencies in these areas and identifies a number of means of achieving these.

On-the-job training

All new staff are mentored by their immediate supervisor. As well, all staff work with other senior DISC staff in a variety of cross-cutting projects and as far as possible in different roles. This provides the opportunity to learn from other experienced staff with a range of skills. Where possible, new staff are involved in projects being undertaken with other areas of AIHW so as to increase understanding of the range of AIHW work. They may also be involved in systems development. Staff recruited as graduates are encouraged to take part in the Institute's graduate projects, which gives them experience in researching and discussing a particular topic under the guidance of the AIHW Statistical Adviser.

AIHW Induction

All staff undertake the general AIHW induction course, which provides a general understanding of the Institute's work, the AIHW Act and the privacy regime.

Reference and study material

Consistent with the Learning and Development policy, all staff are given sufficient time and opportunity during working hours to read and discuss reports, articles and other study material. These include:

1. DISC Operating Manual
2. Previous AIHW reports and papers by AIHW staff on both techniques of data linkage, and the analysis of linked data
3. Reports and papers by outside researchers that involve data integration by the AIHW

4. Standard references on data linkage held in the DISC library
5. Training material from PHRN and other sources

PHRN courses

All staff are able to undertake PHRN courses as available.

Other courses

Staff are able to undertake courses given within the AIHW and by other organisations as available and appropriate. These include specialist data linkage and statistical courses, as well as courses in the use of particular relevant software packages.

Internal and external seminars

AIHW has irregular seminars with internal and external speakers that all staff can attend. Staff are also able to attend relevant seminars at other organisations such as ABS, other government departments, ANU and the University of Canberra.

Conferences

All staff have the opportunity to attend one conference per year and present at conferences where possible. Specialist data linkage conferences are not frequent and attendance at these, along with the PHRN Technical Forums, is rotated. Staff may also present at conferences in other health and welfare areas, where the results of a data linkage project are relevant. All new staff are able to attend either the *Australia's Health* or *Australia's Welfare* conferences.

Criterion IV – Appropriate technical capability

Auditor rating against criterion IV – compliant

IV(a) Does your agency have secure IT infrastructure, including hardware and software systems, and the capacity to support the potentially large and/or complex files associated with high risk data integration projects? Give a brief evidentiary statement.

Dedicated DISC infrastructure capabilities replicate the hardware that has already been used with success on other large data integration projects across the AIHW. The benefit of replicating this hardware is that it is tried and trusted; the hardware will however have a higher specification to ensure that future needs can be met. The PCs in the Data Lab will be networked to this hardware, but the environment will be completely separate from any other AIHW systems.

The AIHW uses best practice technology, procedures and policies to protect its ICT assets. A layered system of security is in place with different technologies and techniques used at different levels. In line with the PSPF:

- Passwords are changed regularly
- Accounts are locked out after three failed attempts
- Operating System patching of desktops, networking equipment and servers are done in line with DSD guidelines
- Application software updates are tested and applied as soon as practical after release
- Access to the data centre is controlled by swipe card
- The network is protected by a state of the art firewall to protect against external intrusion, beyond which the accredited gateway has their firewalls
- Anti-virus software is constantly updated
- Regular backups are taken, including rotation to a secure off-site storage facility
- Desktops have been hardened to prevent users from installing software or tampering with the system

IV(b) How does the system track access and changes to data to allow audits by date and user identification? Does the system 'footprint' inspection of records and provide an audit trail?
This is based around tightly controlled separate information domains (staging, linking and consolidation domains) that exist for each stage of creating the project data for researchers to use in the Data Laboratory. Each project in each information domain is in a separate storage location, with access limited by user (different users in different information domains for separation requirements). This architecture determines who can access what data at any time and access is therefore predetermined and logged. In addition, work logs are generated when code is run against the data; these provide basic information about who ran the job and when. These will be stored as part of the audit trail. Once the data is ready for a researcher to use, and it has been confirmed by DISC staff that the dataset (i) only contains variables agreed with the data custodian, and (ii) has had 'first level' confidentiality protection applied (eg collapsing values on certain variables) as agreed with data custodians, it will be moved to the data lab and usage restricted to a researcher. Data can be freely manipulated in this area, producing output in the formats that they require. All output is stored in a temporary work area for the duration of the session. When the researcher is confident that he has produced the output required, the data will be moved to a checking area where it becomes only available to an AIHW user who will ensure that the data is as confidentialised and suitable for release. In summary, access is provided to individuals for each stage of a project. This allows the AIHW to determine and log all access rights to the data throughout the process.
IV(c) What IT support is in place for staff?
AIHW is comprehensively supported by an IT Service Desk between the hours of 7.30am and 5.30 pm Monday to Friday. This service desk is further supported by a range of infrastructure and network specialists, Data Base Administrators, data managers and a highly skilled SAS development team, who will assist in the resolution of issues.

Criterion V – Lack of conflict of interest **Auditor rating against criterion V – compliant**
V(a) Does the agency have a compliance monitoring or regulatory function? If yes, describe how this function will be separated from integration projects undertaken for statistical and research purposes to avoid this conflict of interest.
No. The AIHW operates under the provisions of the Australian Institute of Health and Welfare Act 1987 which establishes the AIHW to undertake statistical, methodological and research functions only.

Criterion VI – Culture and values that ensure protection of confidential information and support the use of data as a strategic resource

Auditor rating against criterion VI – compliant

VI(a) How is an appropriate culture and values embedded in the agency's corporate plan/mission statement/policies etc?

The AIHW's Corporate Plan, *Strategic Directions 2011 – 2014*, emphasises both the importance of maintaining information quality, data privacy and confidentiality and the need to continually improve the availability of information for the community and stakeholders. To achieve the twin goals of continuously improving data privacy and confidentiality and maintaining high standards of information quality, the Corporate Plan places particular emphasis upon:

- the AIHW playing a leadership role in data integration work
- working closely with the community, data suppliers and data users
- improving the quality and timeliness of information
- promoting national standards in information provision and reporting through the Institute's METeOR information standards repository
- ensuring continuing compliance with privacy legislation and frameworks while continuing to ensure that data are as accessible as possible.

AIHW's policies emphasise the importance of all staff in taking responsibility for maintaining the privacy and confidentiality of data. The AIHW has an *Information Security and Privacy Policy and Procedures* document which requires all staff to be familiar with their legislative obligations under the Privacy Act and AIHW Act.

The AIHW's legislation requires the formation of an Ethics Committee to assess the ethical acceptability of AIHW's work.

Specific data related responsibilities are formally delegated to internal AIHW data custodians to ensure that experienced staff members are held responsible for maintaining information security. The responsibilities of data custodians are set out in the *Guidelines for the Custody of AIHW Data*. These guidelines require data custodians to collaborate closely with information governance and ICT areas within the Institute, and emphasise the importance of maintaining information security.

The AIHW has a number of internal mechanisms designed to support information sharing and collaboration in support of the objectives outline above. A data custodian's forum has been established to assist data custodians in sharing experiences and maintaining best practice. The Institute's Statistical and Analytical Methods Advisory Committee (SAMAC) is a cross-institutional Committee chaired by the Group Head of the Information and Statistics Group and convened to promote shared statistical processes across the Institute and examine emerging literature and technology. The Committee hosts frequent and well attended 'conversations' (seminars) which provide useful learning and development opportunities for staff.

AIHW's policies also emphasise the importance of ensuring that data released by the Institute are freely available to stakeholders and the community. The AIHW is committed to releasing all work into the public domain. The AIHW was the first *Commonwealth Authorities and Companies Act* agency to universally adopt Creative Commons, a licensing scheme that increases the ability of consumers to reuse published material.

VI(b) How have staff been trained in requirements for protecting personal information and how are they made aware of policies regarding breaches of security or confidentiality?

The AIHW ensures that all staff are made aware of and comply with, the Institute's privacy requirements. Staff, are initially made aware of the confidentiality requirements of section 29 of the AIHW Act upon commencing employment, at which time they are required to sign a confidentiality undertaking which outlines their legislative obligations and responsibilities relating to privacy and confidentiality. New starters are required to attend a presentation on privacy as part of their induction. The privacy induction presentation outlines internal policies and procedures and external legislative requirements.

Staff are kept aware of contemporary developments in privacy and confidentiality, and also reminded of their current obligations at privacy seminars which are conducted regularly throughout the year. The Institute's Statistical and Analytical Methods Advisory Committee (SAMAC) also frequently presents learning and development seminars on contemporary developments in the privacy space as they relate to statistical methods. Updates to existing policies and procedures are well advertised through notices in AIHW's weekly all staff email and in 'update emails' circulated by AIHW's Director.

Staff members of the Information Governance Unit, the business area of the Institute tasked with enforcing privacy compliance across the organisation, regularly attend external learning and development sessions such as Information Contact Officer Network meetings, hosted by the Office of the Australian Information Commissioner and events sponsored by the International Association of Privacy Professionals.

Each year, the AIHW is a keen participant in Privacy Awareness Week, conducted under the auspices of the Office of the Australian Information Commissioner. This year the AIHW registered as a Privacy Awareness Week partner and reinforced its ongoing commitment to honouring its privacy-related obligations. A staff seminar entitled 'Privacy Fundamentals' focused on the need to recognise and apply privacy considerations in the Institute's day-to-day work, and on potential reforms to Australia's privacy laws.

VI(c) Do staff sign undertakings related to secrecy and fidelity?

The *Information Security and Privacy Policy and Procedure* document requires all AIHW employees and staff at partner institutions to sign an undertaking of confidentiality. The undertaking is based on section 29 of the AIHW Act, and reiterates the legal obligations and criminal penalties that may apply for breach of the Act. The AIHW also requires external contractors, students and other parties to sign confidentiality undertakings where they may be exposed to either confidential or in confidence information.

The *AIHW Ethics Committee – Guidelines for the Preparation of Submissions for Ethical Clearance* document stipulates the form of undertakings for researchers in receipt of identifying, identifiable or potentially identifiable AIHW data. The principal investigator along with any individual that may have access to the data, along with an individual responsible for the organisation as a whole, are required to sign an undertaking that specifies that all professional standards will be adhered to and that the research will conform with the Privacy Act and any other relevant privacy frameworks. The Agreement also reiterates that the criminal penalties of the AIHW Act apply where data is misused or where confidentiality is breached.

VI(d) What mechanisms are in place to engage with stakeholders to maximise the usefulness of the data holdings?

The AIHW has a number of mechanisms in place, both technical and procedural, to assist stakeholders in maximising the usefulness of data.

METeOR is Australia's repository for national metadata standards for the health, community services, early childhood and housing and homelessness sectors. The system was developed by the Institute and came online in 2005. METeOR provides users with a suite of features and tools. These include online access to a wide range of nationally endorsed data definitions and tools for creating new definitions based on existing already-endorsed components. It has a strong focus on providing comprehensive user support and assistance.

METeOR enables a variety of stakeholders, including data suppliers and users, understand the data definitions of a wide variety of health and welfare related data. The registry is a large repository of metadata for different data collections. A diverse number of stakeholders participate in METeOR including jurisdictional departments and the New Zealand Government. The information held on METeOR is accessible to the public via the AIHW website. The usefulness of the metadata contained on METeOR is further enhanced by publically available data dictionaries covering diverse terms in the Health, Community Services and Housing sectors. Metadata are held online for 4160 standard metadata items.

The AIHW has developed a publically available Guide to Data Development designed to provide comprehensive information to stakeholders on using metadata, the arrangements and mechanisms for national data collections, data development principles and data development methodology.

The AIHW Ethics Committee plays a role in data development by monitoring the activities of partner institutions in receipt of AIHW data to ensure legal and governance requirements are maintained. In relation to external stakeholder involvement with the Ethics Committee the initial review function of the Ethics Committee takes place when they consider a proposal for a data integration project AIHW proposes to release identifiable data to a third party, or when the AIHW collaborates with partners in data integration work or in the creation or modification of a data

set. The Ethics Committee adds significant value by ensuring that initial proposals comply with privacy and governance requirements and ensuring that in cases where proposals fail to meet these requirements, providing practical advice to ensure that they are developed to meet those standards.

The AIHW is also involved in over 20 jurisdictional committees, where it acts to provide advice to jurisdictional and other external stakeholders on the development of national data collections and standards.

As well as direct consultations between the AIHW and user organisations, companies with particular expertise (eg market research agencies) are often engaged to undertake specific research and consultation work with government and non-government organisations and user groups in all jurisdictions.

Most importantly, one of the key responsibilities of the AIHW in regard to its role as a node of the PHRN is to design collaboration mechanisms to 'create the best possible channels for researchers to access Commonwealth data and to be responsible for providing researcher access to Commonwealth data' (the PHRN Integrated Health Systems Education Investment Fund Project Plan).

VI(e) How does your agency provide for valuable use of the data i.e. how does it maximise the value of data for users by providing them with access to as much data as possible while still protecting confidentiality?

The AIHW has a number of strategies and policies in place to balance the competing priorities of maintaining access to data and protecting the privacy of individuals.

The AIHW's legislation requires the formation of an Ethics Committee to assess the ethical acceptability of the AIHW's work. The Committee reviews all internal work involving data integration, creation of data sets, modification of existing data sets or work that may result in the release of identifiable information. The Committee has played a key role in overseeing the work of the AIHW and represents an important safeguard that ensures that data are used ethically and appropriately.

Under the *Guidelines for Custody of AIHW Data* certain senior and experienced staff members are given formal delegated responsibility to maintain datasets that are identified, identifiable or potentially identifiable. These staff members are known as data custodians. Data custodians have responsibility for cataloguing all data holdings in the Institute's data catalogue. The system lists all staff members who have access to the data sets, and allows the Institute's information governance unit to perform an audit role to ensure that data integrity is maintained.

Data custodians are also responsible for managing data requests from external researchers. Where a request is made for identified, identifiable or potentially identifiable information, data custodians forward the request to the AIHW Ethics Committee. The Committee then makes a determination on the ethical acceptability of the research and the proposed use of the data within the research. Both data custodians and the Ethics Committee add value by ensuring that research complies fully with legislative requirements and ethical requirements promulgated by the National Health and Medical Research Council.

In this context, it is important to note the innovative approaches undertaken by AIHW to maximise the usefulness of data through the use of new technologies. In addition to its ongoing publication program, the Institute is continuously improving its online data dissemination, visualisation and decision support services.

Criterion VII – Transparency of operation **Auditor rating against criterion VII – compliant**
VII(a) Are data retention and data disposal statements publicly available? Provide details.
Yes, the Data Integration section of the AIHW website contains this information. See http://www.aihw.gov.au/data-integration/
VII(b) Are details of governance arrangements publicly available? Provide details.
Yes, the Data Integration section of the AIHW website contains this information. See http://www.aihw.gov.au/data-integration/
VII(c) Where are details of data integration projects published?
In the data integration section of the AIHW website. See http://www.aihw.gov.au/data-integration/
VII(d) What other relevant material is published? Examples include data protocols such as microdata access protocols, confidentiality protocols, protocols for linking and protecting privacy; and data integration manuals.
The data integration http://www.aihw.gov.au/data-integration/ and privacy of data http://www.aihw.gov.au/privacy-of-data/ sections of the AIHW describe AIHW privacy protection and protocols. Details of confidentialisation processes applied to particular datasets are not publicly available as an additional security precaution.

Criterion VIII – Existence of an appropriate governance and institutional framework

Auditor rating against criterion VIII – compliant

VIII(a) What are the institutional and project-specific governance arrangements for data integration? (Provide attachment or link to where published.)

There are five inter-related sets of governance arrangements relevant to data integration:

1. Over-arching AIHW governance and executive management arrangements as set out in the AIHW Act and the annual report (see pp xiv of the 2010-2011 Annual Report and the accountability framework set out on pp 28 of that report).
2. Ethical oversight. The Australian Institute of Health and Welfare Ethics Committee is established under section 16(1) of the *Australian Institute of Health and Welfare Act 1987*. The Committee is required to advise on the ethical acceptability of AIHW activities involving information which can identify a person ('identifiable data'). The Ethics Committee considers applications:
    a. by AIHW units and collaborating units to commence new collections of unit record data or to change the scope of content of existing collections;
    b. by AIHW units and collaborating units to link datasets (ie undertake data integration) for the purposes of analysis; and
    c. by external researchers for access to identifiable data held by the AIHW which they wish to link with their research data.
3. High-level consultative and governance arrangements specific to data integration. The key arrangement here is the Data Integration Advisory Committee (DIAC) which has the following role:
    - Assisting the AIHW to fulfil its functions as an integrator of Commonwealth data - in particular, providing advice that helps:
        - support appropriate institutional and project-specific arrangements to enable data custodians to fulfil their responsibilities in regard to their data, and to ensure that researchers provide and uphold appropriate undertakings in regard to integrated data provided to them; and
        - gain and maintain full accreditation as an Integrating Authority
    - Assisting the AIHW to fulfil its functions as a node of the PHRN – in particular, helping to:
        - provide researcher access to Commonwealth data;
        - design collaboration mechanisms in consultation with PHRN to create the best possible channels for researchers to access Commonwealth data; and
        - influence Commonwealth and PHRN governance processes to ensure that, where appropriate, PHRN and Australian Government policies and protocols are consistent and mutually reinforcing
    - Providing advice on the implementation, operation, improvement and extension of data integration services provided by the AIHW, including arrangements for handling complaints and conducting investigations; and

- Facilitating the development and maintenance of relationships with data custodians and users of data integration services provided by the AIHW

The committee consists of:

- Group Head Information and Statistics Group, AIHW (Chair)
- A representative of the PHRN
- A representative from a state or territory government
- Head AIHW Business Group
- Unit Head Information Governance
- A representative of the data custodian community
- A representative of the user community

4. DISC-specific governance arrangements to ensure operational processes and project-specific operations and processes are appropriate. These arrangements need to be approved by an AIHW internal committee known as the DISC Steering Committee (DISC SC) with the following responsibilities:

   - To consider systems and process design and policy proposals
   - To ensure that issues raised by the DIAC are being responded to appropriately
   - To recommend DISC-related proposals and other material for consideration by higher level governance bodies processes as necessary; and
   - To ensure that directions set by external influences, including DIAC are being progressed appropriately

   The committee consists of:

   - Group Head Information and Statistics Group (Chair)
   - Unit Head Data Linkage Unit
   - Unit Head Data Integration Service Centre
   - Principal Data Analyst Data Linkage Unit
   - Unit Head ICT Operations
   - Unit Head Information Governance

5. Project-specific governance and control arrangements. There is an array of mechanisms to ensure that data integration projects are appropriately resourced, managed and controlled. The DISC Operating Manual is project oriented (ie it is structured around four project phases (1) Project Negotiation and Definition, (2) Project Initiation and Management, (3) Project Operations and; (4) Project Finalisation). Each of these phases incorporates document templates, workflows, control points and checklists embodying governance and control arrangements appropriate for that phase.

VIII(b) What framework is in place to conduct investigations and handle complaints?

The AIHW Ethics Committee has an appeals process codified within the *Guidelines for the Preparation of Submissions for Ethical Clearance*. The process allows either data subjects or researchers to appeal decisions made by the Committee, requiring the Committee to reconsider their decision. If the applicant receives an unsatisfactory outcome, they may write to the Chairman of the AIHW Board who will then appoint an independent person to assess the applicant's claim.

In addition, one of the key tasks of the Data Integration Advisory Committee is 'Providing advice on the implementation, operation, improvement and extension of data integration services provided by the AIHW, including arrangements for handling complaints and conducting investigations.'

AIHW has adopted *a Customer Care Charter* which outlines the Institute's commitment to its stakeholders in terms of levels of service, privacy protections and so on, and provides contact details to assist users to take matters up with Institute management.

Under the *Ombudsman Act 1976*, the Commonwealth Ombudsman may investigate the activities of the AIHW either following a complaint by a member of the public or on his own motion. The Ombudsman has strong powers allowing him to examine witnesses, enter premises and require the furnishing of documents. Depending on the circumstances of the misconduct being investigated, if the Ombudsman is satisfied that misconduct has occurred, they must either inform the AIHW's Minister or the AIHW's principal officer.

The AIHW is also bound by the requirements of the Commonwealth *Privacy Act 1988*. While the secrecy provisions in the AIHW Act prevent the release of personal, identifiable or potentially identifiable information to individuals lodging FOI requests, individuals are able to obtain administrative documents, for example, by lodging an application through the FOI process.

The Office of the Australian Information Commissioner (OAIC) also has the power to conduct investigations in relation to privacy matters under Part V of the *Privacy Act 1988*. The OAIC may conduct investigations following a complaint or on its own motion. Where the OAIC finds a privacy breach to have occurred, they may issue a declaration recommending a form of reparation, such as an apology or monetary compensation.

It is also of relevance to note that incident management and response is undertaken independently of the DISC. The following extract from the DISC Operations Manual sets out the arrangements:

> 'Staff must report actual or suspected incidents that are likely to impact the DISC infrastructure and data integration activities to their supervisor as soon as they are identified…….
>
> 'If a breach of privacy or confidentiality is confirmed, subsequent actions are the responsibility of Governance and Communications Group. These actions may include the following:
>
> - Escalation, investigation, containment and management;
> - Consultation with external parties who may be affected by the incident (eg the data custodian) or have some relevant responsibilities (eg the Privacy Commissioner, the Minister);
> - Recovering from an information security incident (rebuilding and restoration, closure); and
> - Post incident activities (root cause analysis, investigation into control effectiveness and reporting to stakeholders)'.