

# Data Collection Monitoring Report and Checklist

## Purpose of this form

In December 2019, the Ethics Committee agreed to the merging of the Ethics Committee: Data collections annual monitoring report with the Data custodian self-assessment checklist. This combined Data Collection Monitoring Report and Checklist is used to record progress and compliance for data collections approved by the AIHW Ethics Committee.

Data custodians are required to complete and submit a *Data Collection Monitoring Report and Checklist* for each data collection listed in the data catalogue for which they are responsible. This form serves three functions. It provides:

1. the Ethics Committee assurance that the collection continues to meet the terms and conditions of Committee approval as stated in the Committee’s approval letter
2. data custodians with additional guidance on the Data Collection Management Principles (DCMPs) against which data collections are audited, and enable them to assess their collections' readiness for audit, and
3. the AIHW with summary information regarding conformance with the DCMPs to aid in identifying key risks and any systemic issues.

## Structure of this form

The form comprises two parts:

1. the data collection monitoring report – addresses the first function by seeking data custodian assurances against specific compliance requirements. This part is reviewed by the Ethics Secretariat and satisfactory receipt of the report is advised to the AIHW Ethics Committee for noting. Overdue monitoring reports are also brought to the attention of the Ethics Committee. Continued approval from the Ethics Committee is subject to submission of the *Data Collection Monitoring Report and Checklist* by the due date.
2. the data collection checklist – addresses the remaining two functions. This self-assessment checklist is based on the seven AIHW [Data Collection Management Principles](http://bruce.aihw.gov.au/Governance/Documents/Data%20collection%20management%20principles%20FINAL.docx) (‘the Principles’) and assists data custodians to self-assess compliance of their management of each data collection with the Principles. This part is reviewed by Ethics Privacy & Legal Unit (EPLU) and any areas of concern will be discussed with the data custodian. EPLU prepares an annual summary report for the Data Governance Committee highlighting strengths and opportunities for improvement in AIHW’s management of data collections, based on an analysis of all submitted checklists.

There are certain conditions where a data collection checklist (Part B) is not yet required, such as when a collection is established but data are yet to be received. In these instances, only the data collection monitoring report section (Part A) is to be completed.

## Submission of this form

A *Data Collection Monitoring Report and Checklist* is due for each collection listed in the Data Catalogue on or before the end of each financial year (30 June) unless the following apply, in which case it is to be submitted every two years:

* the data are not identified or reasonably identifiable/re-identifiable, and there are no or limited stakeholder requirements above standard legal and AIHW policy or guideline requirements; and/or
* the data are archived, not accessed or very rarely accessed.

Approval should be sought from Head EPLU that a data collection meets the criteria for biennial submission. Data custodians with more than six collections are encouraged to spread submissions over the financial year.

The *Data Collection Monitoring Report and Checklist* is to be submitted **by the data custodian** through the EthOS monitoring reports section of the EthOS entry for the data collection. EthOS records the name of the user lodging the form, and this method is used in lieu of a signature to authenticate data custodian approval of the form. The form can be submitted as a word document and does not need to be printed, physically signed or scanned to pdf.

An automated reminder will be sent to each data custodian six weeks before the form is due.

In the event that a data collection listed in the data catalogue does not have a corresponding entry in EthOS, this *Data Collection Monitoring Report and Checklist* is to be lodged directly with EPLU. (EPLU is working with data custodians to progressively eliminate these instances.) Data custodians should read the *Data Collection Monitoring Report and Checklist* FAQs, which provide extensive information on completing and submitting the checklist, before attempting to complete and submit their first form. If data custodians have any concerns or additional queries after reading the FAQs, they should contact Head EPLU.

**Note** This document will be refined and updated based on:

* recommendations or issues identified by data custodians,
* results of internal audits and/or
* additional guidance, clarifications and/or decisions made by the AIHW Board, the Risk Audit and Finance Committee, the Ethics Committee, the Executive Committee and/or the Data Governance Committee.

# Part A: Data Collection Monitoring Report

Part A is used to record the progress of data collections approved by the Australian Institute of Health and Welfare Ethics Committee (the Committee). Projects approved by the Committee require a different form which is available [here](https://www.aihw.gov.au/getmedia/83fbefac-a4ee-473d-bdd3-a429f475716e/AIHW-ethics-projects-annual-monitoring-form.doc.aspx) or from [ethicssec@aihw.gov.au](mailto:ethicssec@aihw.gov.au)

Consistent with the legislative and ethical requirements set out in [*Australian Institute of Health and Welfare Act 1987*](https://www.legislation.gov.au/Details/C2016C01008)*,* the [*Australian Institute of Health and Welfare (Ethics Committee) Regulations 2018*,](https://www.legislation.gov.au/Details/F2018L00317) the [*National*](https://www.nhmrc.gov.au/guidelines-publications/e72)[*statement on ethical conduct in human research*](https://www.nhmrc.gov.au/guidelines-publications/e72)and AIHW’s [*Data Governance Framework,*](http://bruce.aihw.gov.au/Stats/Pages/Data-governance.aspx)reporting on progress for Committee approved data collections is normally on an annual basis.

The Data Custodian (as Principal Investigator) is responsible for ensuring that the collection continues to meet the terms and conditions of Committee approval as stated in the approval letter from the Committee. Please consult your own records for details (unless otherwise requested, approval letters are sent to the data custodian nominated on the application form).

The due date for annual monitoring reports is 30 June. Six weeks prior to the due date, the EthOS system will send the Data Custodian an email request to submit an Annual Monitoring Report. Continued approval from the Committee is subject to submission of the annual monitoring report by that due date.

NOTE: This form will not be accepted if it is incomplete or used for another purpose (e.g. to request an amendment). For assistance please contact the Ethics Manager: [ethicssec@aihw.gov.au](mailto:ethicssec@aihw.gov.au) or   
(02) 6244 5004.

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **CURRENT COLLECTION DETAILS:** | **Refer to the Committee’s collection approval letter in your files** | | **Please provide responses in this column** |
| (a) EC or EO reference number |  | |  |
| (b) Title of collection  (as approved by the Committee) |  | |  |
| (c) Data Custodian: | Name and title: | |  |
| Group/Unit: | | Choose an item. |
| Email: | |  |
| Ph: | |  |
| (d) Contact person **if different to Data Custodian** | Name and title: | |  |
| Group/Unit: | | Choose an item. |
| Email: | |  |
| Ph: | |  |
| 1. **STATUS OF THE APPROVED COLLECTION:** | **mark N/A to any that do not apply** | |  |
| (a) Approvals up to and including data destruction | Date the Committee originally approved the collection | |  |
| Approved data retention date (if applicable)  ***NOTE****: if a collection is approved for a defined period, at data destruction time a separate Final Monitoring report is submitted.* | |  |
| (b) Collection commencement | If the approved collection has not yet commenced, please provide brief **reasons** and attach any supporting documentation (e.g. changes to funding). | |  |
| (c) Human Research Ethics Committee (HREC): approvals from another HREC (**if applicable**) | Full name of the other HREC (please do not use unexplained abbreviations) | |  |
| Chair of the other HREC | |  |
| Please provide brief **reasons** for the need to obtain approval from that HREC | |  |
| Date the approval from that HREC **expires** | |  |
| If the approval (from another HREC) has expired, please briefly explain how it has been renewed including (indicative) date | |  |
| (d) Changes to the collection (amendment requests) | Has the Committee approved any amendments to the collection? | | Choose an item. |
| *There is no need to attach the original application or any amendment requests* | If YES, please briefly describe the nature of those approved amendments, e.g. an extension of time (see 2 (b) above) | |  |
| Date the amendment request was approved (see approval letter) | |  |
| 1. **COMPLIANCE INCLUDING DATA STORAGE:** | **refer to collection approval letter for details** | |  |
| (a) Data storage and security  *A* ***NO*** *answer* ***must*** *be discussed with the Ethics Secretariat via* [*ethicssec@aihw.gov.au*](mailto:ethicssec@aihw.gov.au)*.* | The data storage and security arrangements approved by the Committee continue to be met. | | Choose an item. |
| **If NO**, | please briefly outline the **reasons** |  |
|  | and **what has been done** to address the issue/s, including any amendments approved by the Committee (attach any supporting documentation) |  |
| (b) Confidentiality and privacy (e.g. a waiver of consent)  *A NO answer* ***must*** *be discussed with the Ethics Secretariat via* [*ethicssec@aihw.gov.au*](mailto:ethicssec@aihw.gov.au)*.* | The confidentiality and privacy provisions approved by the Committee have been implemented and continue to be met. | | Choose an item. |
| **If NO**, | please briefly outline the **reasons** |  |
| and **what has been done** to address the issue/s including any amendments approved by the Committee (attach any supporting documentation). |  |
| (c) General compliance  *Refer to the Chapter 5.5 of the* [*National*](https://www.nhmrc.gov.au/guidelines-publications/e72)[*Statement*](https://www.nhmrc.gov.au/guidelines-publications/e72)*, AIHW Ethics Committee approval and data supply arrangements.* | All Ethics Committee and data supplier conditions for the collection continue to be observed and applied. | | Choose an item. |
| **If NO**, | please briefly outline the **reasons** |  |
| and **what has been done** to address the matter (attach any supporting documentation) |  |
| 1. **DISSEMINATION OF RESULTS:** | **refer to collection approval letter for details** | |  |
| (a) Approved method of dissemination of results | The method/s of dissemination approved by the Committee continue(s) to be met.  . | | Choose an item. |
| **If NO**, | please briefly outline the reasons |  |
|  | and any future plans for dissemination including indicative timelines |  |
| **If YES** please provide citation details (including web-links) for any publications arising from the collection, e.g. a report to government | |  |
| 1. **OTHER:** | **Mark N/A if not applicable** | |  |
| (a) Other  *Do not use this section to request an amendment* | Please briefly outline **other matters** that have arisen in the reporting period which directly relate to the approved collection but are not covered in any of the above fields (attach any supporting documentation). | |  |
| 1. **DECLARATION:** | **Data Custodian to complete** | |  |
| I confirm that the details in this report are a true and accurate record of the above-named collection as approved by the AIHW Ethics Committee. | Name & Title: | |  |
| Group/Unit: | | Choose an item. |
| Date: | | Click or tap to enter a date. |

# Part B: Data Collection Checklist

## Context

This self-assessment checklist is based on the seven [Data Collection Management Principles](http://bruce.aihw.gov.au/Governance/Documents/Data%20collection%20management%20principles%20FINAL.docx) (‘the Principles’) approved by the AIHW Ethics Committee in 2012 and endorsed by the AIHW Board in 2013. It is further informed by results of data collection audits conducted by the AIHW’s internal auditors.

The checklist assists Data Custodians to self-assess compliance of their respective data collection(s) with the Principles as well as their readiness for internal audits, with a focus on key controls that are managed by data custodians and their units, with some reference to other procedures that may for example be conducted by IT but of which data custodians should be aware.

## Instructions

* This checklist should be completed by Data Custodians for each data collection in the data catalogue for which they are responsible. If you have any questions or require assistance in completing the checklist, please contact the Head, Ethics, Privacy and Legal Unit.
* Where a Principle is marked with \*\* Asterisks, this denotes that some components of the Principle will be separately assessed as part of a broader assessment of AIHW institutional controls (for example IT controls).
* Please assess each component under each of the 7 Principles and indicate your assessment of compliant (‘Yes’), non-compliant (‘No’) or, if the component is not applicable for the data collection being assessed, indicate ‘Not Applicable’. Where a component is determined to be ‘Not Applicable’, and/or where further explanation would assist an understanding of the assessment, or of activities being undertaken to action an aspect which is not yet fully compliant, please complete the ‘Comments’ section adjacent by inserting the basis or bases for this assessment.
* Upon completion of all components, the data custodian should personally upload the form through the EthOS monitoring reports section of the EthOS entry for the data collection.
* Data custodians may choose to update a previous version of this form in preference to populating a completely new form. When taking this approach, please ensure you meet the requirements of the most recent version of the form, which are detailed in the Frequently Asked Questions.

| **Principle** | **Q #** | **Compliance with components of the principle** | **Sub- principle** | **Additional Guidance / Compliance indicators** | | | **Choose from menu/ Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Compliance Principle 1** | 1 | Is a custodian for this data collection clearly identified? | 1.7 | In accordance with the AIHW Director delegation, a data custodian must be identified in the AIHW Data Catalogue for all data that comprises a ‘data collection’.  Compliance indicators include:   * The individual (not just position) is accurately identified. * The person nominated on the Data Catalogue is the *current* custodian. * If custodianship has changed hands, appropriate handover regarding the data and its controls/obligations occurred upon commencement of a new custodian. | | | Choose an item. |
| **Data collections are established and managed effectively, appropriately, and consistently, with clear accountability requirements and governance arrangements.** |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 2 | Are details of the data collection recorded in the AIHW [Data Catalogue](http://bruce.aihw.gov.au/Data-Catalogue/Lists/DataCatalogue/Data%20custodians.aspx) and are they up to date? | 1.1 | Compliance indicators include:   * information is accurate * information is current * all fields relevant to the collection are complete (including e.g. release externally field and approver when set to ‘no’ or ‘yes - restricted access’, information about identifiability, data limitations/use, temporal/geographic coverage, data availability, terms and conditions of access and use, metadata information, Ethics committee approval reference/no. etc) | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 3 | Has the data collection been approved by the Ethics Committee? | 1.1, 1.2, 1.3, 1.6 | All data collections must be approved by the Ethics Committee.  Approval of the Ethics Committee is current and details of the approval are entered in the Data Catalogue.  Any modifications made to the collection (including e.g. manner of collection, data description, retention and/or dissemination) have been notified to the Committee and those changes approved.  Collection, retention, use, dissemination and/or destruction is consistent with the terms of the Ethics Committee approval. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 4 | Are there documented processes and procedures for this data collection?  Are these adequately accessible to all staff responsible for maintaining this data collection? | 1.1, 1.8 | Compliance indicators include:   * Procedures are documented. * Procedures are current and sufficiently detailed to enable new staff to effectively manage and support the collection. * Procedures are easily locatable by staff that maintain the data (and, as relevant, intended users). * The existence of the procedures and need for compliance have been communicated to the data custodian team and intended users by the data custodian.   Version controls should be applied (e.g. Prepared By, Date Prepared, Date Last reviewed, and Approved By) so that staff can be confident they are referencing current procedures. | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 5 | Do the procedures adequately detail the objectives of the data collection, how data are collected, key collection dates and processes for collection? | 1.1, 1.3, 2.1 | Compliance indicators include ensuring that procedures and related documentation explain all relevant aspects. For example:   * the purpose of the collection, including whether data is collected under a broader government policy or program * if the data collected under an Agreement/MOU, the relevant agreement(s) is specified, staff are informed about it and have ready access so that they understand its terms * how the data are obtained and from which party(ies) (Note: Direct data suppliers are particularly relevant to legislative considerations such as those in the s. 29 of the AIHW Act.) * relevant collection period(s) and whether the data are part of longitudinal collections (to ensure consistency between data items and definitions) * fields/data items relevant to the collection * when data are collected and the reason for this timing/intervals * quality assurance and other processes applied * key stakeholders and communication strategies * persons/positions e.g. in data provider organisations who must be consulted or from who permissions should be sought * who outside AIHW is allowed to access data (aggregate or unit record) and data products.   Data Quality Statements (DQS), Ethics Committee approvals, user guides and data collection shopfronts may address some of these indicators.  Consider providing some guidance to the data custodian team on data requests as distinct from privacy queries or complaints, FOI requests etc. The distinction is not always clear. Queries on the latter should be discussed with the Ethics, Privacy and Legal Unit. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 6 | Do the procedures cover key controls/steps for data collection storage, security, integrity, manipulation and dissemination? | 1.1, 1.3 | Procedures and controls are consistent with, and adequately address matters required under:   * legislation (e.g. Privacy Act, AIHW Act) * the Ethics Committee approval * policy (e.g. AIHW Data Governance Framework, Guidelines for the Custody of AIHW Data, confidentialisation policies) and * relevant institutional procedures and guidance (e.g. AIHW statistical manual and quality assurance processes) | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 7 | Are there additional specific procedures or compliance requirements that have been agreed with data providers? Are these clearly defined and documented? | 1.1, 1.3, 1.4 | Compliance indicators include:   * Source documents detailing these requirements are specified, including information on where they are kept and relevant staff know where to locate them. * Updated signed copies of agreements and/or other source documents are stored appropriately and maintained for currency, including contacts for the other party(ies) * Documentation and practice is consistent with current Ethics Committee approvals. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 8 | Are the data collected and stored with appropriate metadata and associated with appropriate data dictionaries to accurately define and describe the collection? | 1.5 | Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. The level/type of metadata may depend upon the nature of the collection.  Compliance indicators of appropriate metadata management include:   * accuracy - the characteristics of the resource are correctly reflected * availability – the metadata can be accessed now and into the future * completeness – to the extent necessary and economically feasible, all relevant characteristics of the resource captured * conformance with accepted standards – e.g. a specific metadata standard or application profile * consistency – absence of contradictions, ambiguities or other non-adherences to accepted standards * credibility and provenance – metadata is based on trustworthy sources * ease of processing – e.g. software-defined, machine-readable or use of dynamic encoders or decoders * relevance – contains the right information for the task * timeliness – corresponds to current characteristics of the resource and published at the right time   METeOR entries and DQS may be sources of evidence for auditing purposes. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 9 | Are roles, responsibilities and accountabilities relevant to this data collection, including data custodian responsibilities, clearly defined? | 1.1, 1.3, 1.8 | Whilst AIHW policies and guidelines establish baseline requirements for defined roles such as data custodians, consider defining collection-specific decision making points and clearly assigning responsibilities for preparation, review and approval of key task. For example, procedures outline:   * which position(s) are responsible for various data-related activities * who has authority to make various decisions * written records are kept of data custodian decision- making   Procedures/processes are in place to ensure that replacement/back-filling staff are appropriately trained and knowledgeable. | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 10 | Are monitoring controls in place to ensure adherence to internal procedures and specific compliance requirements of data providers? | 1.4 | The effectiveness of monitoring controls are generally assessed as part of auditing general organisational activities, along with additional separate specific evaluations, if necessary.  Consider in respect of this particular collection:   * What are the monitoring controls? * Are the controls part of the procedures for the collection (i.e. easily identified/located)? * How often must certain things occur? Are they occurring at the intervals specified? * Have any issues been found? * What action(s) were taken in respect of identified issues? Are those actions appropriately documented?   Indicators of compliance (examples) include:   * Evidence based monitoring controls are used to ensure that key tasks have been completed as expected. * Protocols are reviewed at regular intervals to ensure currency, and collection processes, data elements, use and dissemination by the data custodian team remain consistent with agreed arrangements with data provider requirements (as evidenced by correspondence, contracts, agreements and/or MOUs) and Ethics Committee approvals. Amendments are submitted to the Committee where processes have changed or it is anticipated they will change. Users outside the team are provided with appropriate information and guidance to aid compliance with requirements for the data collection. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 11 (a) | Are the data collected identified, reasonably identifiable, or used for/ the product of data linkage? | 1.6 | Data comprising ‘personal information’ and/or ‘information concerning another person’ must be collected, used and disclosed only in accordance with the Privacy Act 1988 and AIHW Act.  Indicators of compliance include:   * data are collected in identified/identifiable form only as needed to achieve collection objectives and commensurate with required approval(s) * Ethics Committee approvals have been obtained prior to collection and/or linkage activities being conducted * Adherence to Privacy Act APPs, AIHW Act and AIHW policies and procedures (e.g. AIHW *Data Governance Framework*, *Guidelines for the Custody of AIHW data*, *Privacy Policy*, *Information security policy*, data linkage protocols, ICT policies, statistical manual, publications policies etc) as supported by documentary evidence of practices and activities. | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 11 (b) | If yes, do your data collection procedures adequately cover risks in that regard? |  |  | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 12 (a) | If the collection has been audited, have any audit recommendations been actioned? |  | Indicators of compliance include:   * Evidence of action taken * If action has not been taken, comment on any issues & timeframe/plan for action | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 12 (b) | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance assessment – Principle 2**  **Data receipt processes ensure the security and integrity of the data during transfer.** | 13 | Are there adequate checks to ensure that data transmitted by data suppliers are received without degradation/corruption? \*\* | 2.1 | Data transmission controls ensures the security, accuracy and completeness of data received. Controls that aid in minimising loss or alteration of data include: | | | Choose an item. |
| * Encryption of data * Call-back * Echo check | * Bit recognition * Feedback   Private lines | |  |
| Whilst some functions may be conducted via ICT systems and controls, the data custodian should at a minimum check that such systems appear to be working properly, to enquire if uncertain, and/or ensure that data suppliers do not submit data in a manner that is contrary to AIHW policies and protocols.  Liaison with ICT may be required to inform these aspects.  Use of Validata may be a source of documentary evidence regarding compliance. | | |  |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 14 | Is information about secure transmission of data known to the data custodian team and adequately communicated to data suppliers and adhered to in all data transmissions? | 2.2 | Indicators of compliance may include:   * emails or other correspondence with data suppliers * manuals or protocols made available to data suppliers which cover processes for data supply and receipt * information provided to data suppliers at point of entry on data portals * use of Validata * ICT protocols / manuals and system checks * documentary evidence of data supply and monitoring of compliance | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 15 | Are all collection data received assigned to the data custodian? | 2.3 | Data received must be stored in the correct storage locations for collections per Institute guidelines. No data should be retained in Outlook (e.g. as attachments) or on discs or computer/shared drives such as G drive. (Data may be stored in T drive with restricted user access whilst under analysis). | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 16 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance assessment – Principle 3\*\***  **Data are stored securely and regularly backed up.** | 17 | Standard processes are in place to back up AIHW’s data – do current processes meet the needs of your data collection? \*\* | 3.3, 3.4,  3.5 | Data collection procedures should note what back-ups are conducted and how to access backed-up data in the event of need.  At a minimum, data custodian involvement in back-up processes includes:   * a basic understanding of the standard back-up procedures conducted by ICT * obtaining confirmation from ICT that regular back-ups are being carried out and tested * ensuring standard back-up procedures are fit-for-purpose for the relevant collection and * the ability to access backed-up data if required. Liaison with ICT may be required to obtain this information. | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 18 | Are there adequate controls to prohibit/control the use of shared or personal drives to store data collection material? \*\* | 3.1, 3.2 | Shared and personal drives are typically less controlled in terms of access and therefore represent a control risk for AIHW data. As a general rule, AIHW shared drives such as G drive and personal drives should not be permitted locations for extracts or analyses of data. This applies in particular (but not solely) to identified/reasonably identifiable data. (Data may be stored in T drive with restricted user access whilst under analysis).  Examples of controls:   * advice and/or request for confirmation from data users * prohibitions contained in protocols/procedures for the data collection * logging/tracking data access, copying and storage * restriction of access to shared or personal drives * Automated restrictions on saving certain types of information such as data to shared or personal drives. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 19 | Are there adequate controls over the use and storage of spreadsheets including data collection information that are used by the data custodian team as part of data aggregation and/or analysis? | 3.1, 3.2 | As above | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 20 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance Assessment – Principle 4**  **Integrity of the data is maintained** | 21 | Are there adequate documented controls for processing and manipulation of the data including data storage, migration, editing and protecting the integrity of the data during analysis? | 4.1 | Data integrity is the state of completeness, consistency, timeliness, accuracy and validity that makes data appropriate for a given use. Procedures/protocols should describe controls on data-related activities (refer to guidance on elements of ‘well- designed better practice procedures’ in Principle 1). | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
|  | 22 | Are all employees that have access to and/or manage the data appropriately trained and qualified and are they subject to appropriate confidentiality requirements? | 4.2 | Compliance indicators include:   * Training and qualifications of the data custodian and data custodian team are relevant and adequate for activities to be undertaken (can include formal training, accreditation and/or on-the-job training). * Critical training/skills are current and recorded (Consider maintaining records of lesson plans/PowerPoint presentations where skills are particularly relevant to roles.) * Staff, consultants and contractors have signed confidentiality undertakings. Documentary evidence of undertakings is maintained. Staff are reminded of their confidentiality obligations at appropriate intervals. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 23 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance Assessment – Principle 5\*\***  **Controls for persons/entities having access to the collection exist and are implemented.** | 24 | Is access limited to a needs basis and are permission levels granted commensurate with roles played/activities performed by those with access? | 5.1, 5.3 | Compliance indicators include:   * Data custodian can identify with confidence (and provide documentary evidence) of all those with access to the data and permission levels granted * Permissions granted correspond with staff roles in respect of the data * Highest level permissions (unfettered access) is strictly confined to those in identified critical positions. * Access to staff not directly involved in the collection is restricted to a set period (e.g. 6 months).   Consider: Do you request (and review) a regular (e.g. monthly) list from IT including all user names of individuals who have access to the database, the level of access? A regular access list can be prepared by ICT and tailored at the request of the data custodians. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 25 | Is all access to the data collection database documented and approved by the data custodian? | 5.1, 5.2 | Compliance indicators include:   * Documentary evidence is readily available\*\*. * Access reports are run and reviewed on a regular basis and appropriate action taken if required. Actions taken are recorded. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
|  | 26 | Is the access to the database time-limited to prevent individuals, who are not primary users of the database, from getting unnecessary extended access? | 5.4, 5.5 | Compliance indicators include:   * Time limits are specified where applicable (e.g. commensurate with contract/consultancy period. * Exit forms/end of contract forms contain a requirement for cease of access to be noted by the data custodian. * Access reports are run and assessed on a regular (e.g. monthly) basis and appropriate action taken if required. Actions taken are recorded. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 27 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance Assessment – Principle 6**  **Data transmission or dissemination from the collection to any source (internal or external) is conducted in a manner which ensures its accuracy, integrity and security.** | 28 | Do procedures for the collection clearly describe data dissemination strategies and processes | 6.1 | Documented procedures for the collection clearly detail any collection-specific requirements about:   * what data may be divulged/disseminated * when and how the data should be divulged/disseminated and * why it should be sent (including in the manner specified).   Additionally, project documentation should include any project- specific limitations. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 29 | Do procedures specify measures to ensure the data are sent intact, non- degraded/uncorrupted and securely? | 6.4, 6.5 | Compliance indicators include:   * Procedures/protocols describe requirements and processes clearly and unambiguously (see also guidance regarding ‘well-designed better practice procedures’ in Principle 1 and FAQ). * Security, data governance, ICT and quality assurance policies and protocols, including use of ASM are adhered to. * If data are classified, they are marked, stored and managed in accordance with PSPF requirements | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 30 | Are adequate controls regarding transmission or dissemination of the data applied to ensure compliance with any conditions imposed by the Ethics Committee and/or data supplier(s) of the data being transmitted or disseminated? | 6.2 | Information on Ethics Committee approvals and data provider requirements are clearly documented in the Data Catalogue and procedures/protocols for the collection.  Documentary evidence indicates compliance with requirements (e.g. checklists. See additional examples in FAQ)  Special considerations and controls are applied to sensitive and identifiable data. | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 31 | Are any additional specific conditions or compliance requirements imposed by Ethics Committee being appropriately managed? | 6.3 | Information on Ethics Committee requirements are clearly documented in the Data Catalogue and procedures/protocols for the collection.  Documentary evidence indicates compliance with requirements  Special considerations and controls are applied to sensitive and identifiable data. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 32 | Are you complying with monitoring requirements of the Ethics Committee? | 6.2, 6.3 | Regular monitoring forms must be submitted for Ethics Committee approved data collections. Reminders are sent by the Ethics Secretariat. Compliance indicators include:   * Compliance with annual (or such other timeframe as specified by the Committee) monitoring reporting requirements. * Records are maintained of completed monitoring and other relevant reports. In particular, recent forms should be readily accessible. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 33 | Are appropriate key controls applied to ad hoc data requests? | 6.6 | Procedures/protocols for the collection include clear information about management of requests including the decision-making process.  Consider establishing a control checklist for all ad hoc requests received and processed including supporting documentation of key compliance requirements (e.g. approvals from data suppliers for the release of requested data). Entries in the data request checklist on Bruce may assist with and/or provide evidence about this. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 34 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Compliance Assessment – Principle 7**  **End of data lifecycle/use is appropriately managed.** | 35  (a) | Is there a limited duration for the use of the data? | 7.1, 7.2 | Contracts, agreements, correspondence, protocols and/or Ethics Committee approvals related to the data may specify constraints/time limits on data retention. These limitations should be identified early and contained in procedures and other documentation for the collection.  Obligations should be adhered to, or alternative/extended arrangements negotiated and documented in an accessible location. | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 35  (b) | If yes, do procedures for the collection adequately address what happens to the data at the end of its use? | 7.1,7.2 |  | | | Choose an item. |
|  |  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 36 | Data are required to be destroyed, returned to data supplier (for example, in compliance with contractual obligations), or de-identified (per Privacy Act requirements) or archived in a secure environment, as appropriate, when no longer needed. Do procedures/protocols adhere to these requirements? | 7.2 | Procedures/protocols for the collection should specify whether there are contractual, Ethics Committee approval or other requirements relating to retention or disposition of data at the end of the project/contract.  Contractual provisions relating to the return, retention or other disposition of data must be adhered to or alternative/extended arrangements negotiated and documented in an accessible location.  (Note: Data custodians must be mindful of records retention notices and notices of disposal freeze as issued by National Archives Australia). | | | Choose an item. |
|  | Comments |  | Comments are mandatory where No or N/A is selected | | |  |
| 37 | How do you rate your compliance with the components of this Principle? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| **Overall compliance** | 38 | How do you rate overall compliance of your data collection with the requirements of the seven Data Collection Management Principles? |  | (Note: If any answers above indicate non-compliance then assessment rating will be either partially or not compliant.) | | FC – Fully compliant  P or NC – Partially or not compliant | Choose an item. |
| 39 | Actions and timeframes to address non- compliance. |  | List actions and timeframes to address non-compliance.  Timeframe for completion: | | |  |