Northern Territory Health Data Release Guideline

25/07/2018

Version: 3.1

|  |  |
| --- | --- |
| Acronyms The following acronyms are used in this document | |
| **Acronyms** | Full form |
| ABF | Activity Based Funding |
| AHKPI | Aboriginal Health Key Performance Indicator |
| AIHW | Australian Institute of Health and Welfare |
| BP3 | Budget Paper 3 |
| CAHS | Central Australia Health Service |
| CFO | Chief Finance Officer |
| CHO | Chief Health Officer |
| COO | Chief Operating Officer |
| DM&SR | Data Management and System Reporting |
| DSS | Data Set Specification |
| FOI | Freedom Of Information |
| HREC | Health Research Ethics Committee |
| HRN | Health Record Number |
| IHPA | Independent Hospital Pricing Authority |
| IPP | Information Privacy Principle |
| KPI | Key Performance Indicator |
| NGO | Non-government Organisation |
| NHMRC | National Health and Medical Research Council |
| NHRA | National Healthcare Reform Agreement |
| nKPI | National Key Performance Indicators for Aboriginal and Torres Strait Islander primary health care |
| NMDS | National Minimum Data Set |
| NPA | National Partnership Agreement |
| NT | Northern Territory |
| ROGS | Report On Government Services |
| SA | South Australia |
| SDA | Service Delivery Agreement |
| TEHS | Top End Health Service |

Contents

[1 Overview 4](#_Toc527378879)

[2 Purpose 5](#_Toc527378880)

[3 Scope 5](#_Toc527378881)

[3.1 Types of data release 5](#_Toc527378882)

[3.2 Data categories 5](#_Toc527378883)

[3.3 Out of scope 6](#_Toc527378884)

[4 Benefits 6](#_Toc527378885)

[5 General principles 6](#_Toc527378886)

[5.1 Information is a corporate and public good resource 6](#_Toc527378887)

[5.2 Identifiable information 6](#_Toc527378888)

[5.2.1 Privacy of individuals 6](#_Toc527378889)

[5.2.2 Privacy of organisations and service providers 7](#_Toc527378890)

[5.2.3 Privacy of Aboriginal Communities 7](#_Toc527378891)

[5.2.4 Balance between data release and privacy 7](#_Toc527378892)

[5.3 Public information 7](#_Toc527378893)

[5.4 Summary level information 8](#_Toc527378894)

[5.5 Intended use 8](#_Toc527378895)

[5.6 Approval 8](#_Toc527378896)

[5.7 Data linkage 8](#_Toc527378897)

[5.8 File format 8](#_Toc527378898)

[5.9 Work done on behalf of the Department 8](#_Toc527378899)

[5.10 Data refusal 8](#_Toc527378900)

[6 Human Research Ethics Committee approval 8](#_Toc527378901)

[7 Data request for research purposes 9](#_Toc527378902)

[8 Data ownership 9](#_Toc527378903)

[9 Roles and responsibilities 11](#_Toc527378904)

[10 Approval(s) for release 11](#_Toc527378905)

[11 Data release workflow 12](#_Toc527378906)

[12 Data release templates 12](#_Toc527378907)

[12.1 Data release request form 12](#_Toc527378908)

[12.2 Data release review and approval form – Department ONLY (internal) 12](#_Toc527378909)

[12.3 Data release agreements 13](#_Toc527378910)

[13 Appendix A 14](#_Toc527378911)

[13.1 Request for data release – research and service planning or evaluation requests 14](#_Toc527378912)

[Research 14](#_Toc527378913)

[Service planning and evaluation 15](#_Toc527378914)

[Request for data release – other requests 16](#_Toc527378915)

[External data release workflow 17](#_Toc527378916)

[14 Appendix B 18](#_Toc527378917)

[14.1 Glossary of terms 18](#_Toc527378918)

# Overview

NT Health’s data management and reporting functions are vital in ensuring generation of, and access to, the data and information that is needed for effective business management and decision making, and in maintaining compliance with Territory and National reporting obligations. The Department of Health (Department) must deliver a reporting function with the capability to meet reporting needs and obligations relating to:

* The National Health Reform Agreement (NHRA) and other National Partnership Agreements (NPA)
* Compliance with and performance reporting against national key performance indicators (nKPIs), including requirements relating to Activity Based Funding (ABF)
* The Department’s Annual Report and Budget Paper 3 (BP3)
* Generation and integration of reporting functions and requirements for NT Health, the Top End Health Service (TEHS) and the Central Australia Health Service (CAHS) prescribed in the *Health Services Act 2014 (NT)[[1]](#footnote-3)* is enabled through Service Delivery Agreements (SDAs)[[2]](#footnote-4) with the Department
* Service planning and evaluation
* Continuous Quality Improvement
* Clinical, epidemiological, and social health research.

The Data Release Guideline covers all data collections that are held by the Department including that stored in the data warehouse and its associated datamarts as well as data that currently sits outside the data warehouse (eg. information held by the Innovation and Research Branch).

The Data Release Guideline recognises the *Information Act* (NT), Information Privacy Principles (IPP)[[3]](#footnote-5), and the Department’s Privacy Policy[[4]](#footnote-6).

The Data Release Guideline provides operational information to support the Data Governance NT Health Framework[[5]](#footnote-7) and sits alongside other specific agreements created in relation to more specific data and/or data sources (eg. data registries).

The Department is committed to ensuring that information is available in a timely manner to authorised users and is of high quality to meet the requirements of its intended use. To protect information, authorised users (both internal and external to the department) must be well informed of their obligations to maintain confidentiality and security of the data.

The Department’s Data Management & System Reporting Branch is responsible for maintaining and publishing this guideline.

# Purpose

The Data Release Guideline outlines best practice for managing the release of information from data collections held by NT Health. The purpose of the guideline is to ensure data is released in a responsible and accountable manner that supports the efficient, effective and appropriate use of information. This is achieved through providing a clear understanding of:

* The types of data release requests received
* The evaluation and approval workflow associated with each type of request
* The delegations and approvals relating to each workflow.

The Data Release Guideline provides guidelines for the data steward, data owners, data custodians, system owners, and internal and external clients, to manage access to, and use of, data and information held by the Department. In addition, the Data Release Guideline is an instrument which governs data security and potential risk associated with access to information held by the Department.

The Data Release Guideline is applicable to the Department of Health and the Health Services.

# Scope

This guideline covers the range of data release requests received by NT Health across the broadly defined data categories held by the Department, as follows.

## Types of data release

The guideline applies to the following types of data release:

Provision of information to requestors external to the Department, such as:

* Researchers (including those requiring clearance to release through the AIHW)
* Other NT Government agencies

NT Health client data linked by SA NT DataLink

Data for use by Department of Health staff, such as:

* data/results used in the public domain (eg. Annual Report)
* patient/client level information required for analysis
* epidemiology and research (including for Health Analysis Branch)

Provision of NT Health data to an Australian Government Department via:

* National Minimum Data Sets (NMDS)
* Other specific national agreements (eg. nKPIs)

Clearance of NT Health data held by an Australian Government Department, such as for:

AIHW publications

National Agreements (eg. NPA, nKPIs)

Report On Government Services (ROGS).

## Data categories

This guideline includes the following broad categories of data:

* Financial data
* Workforce data
* Activity data (including patient/client level data).

## Out of scope

* Registry data (eg. Cancer, Perinatal)
* Primary use data
* Freedom of Information (FOI)
* Media

# Benefits

The benefits of the Data Release Guideline and its implementation are:

* Transparency and understanding of the NT Health processes for releasing data and information;
* Facilitation of a process for defining data requirements and delivery of appropriate and relevant data;
* Protection of personal and sensitive information as required under the *Information Act*;
* Assurance for data owners of robust management of data and information collected, managed and stored by the Department; and
* An assurance that consistent and standard processes are used for requests to release data held by the Department.

# General principles

The following general principles underpin the guideline.

## Information is a corporate and public good resource

Information collected, managed and stored by the Department is a corporate resource that is utilised wherever possible to support and enhance the Department’s strategic agenda, clinical and operational decision-making to serve the public good.

## Identifiable information

Identifiable information refers to information (record/patient/client level or aggregated) where the identity of an individual, Aboriginal community, health service, clinician or health professional is apparent, or can reasonably be ascertained.

Identifiable information must only be released to authorised users. An authorised user is a person who has obtained the appropriate approvals for the use of information.

### Privacy of individuals

The *Information Act* states that a public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Disclosure of, or access to, personal information about an individual for a purpose other than the primary purpose for which the information was collected (ie. to treat or manage the individual’s health condition) must comply with Information Privacy Principle 2. Subject to compliance with this privacy principle, release of personal information will be contingent on a signed deed of confidentiality and compliance. A copy of the deed of confidentiality and compliance can be obtained upon request to Data Management & System Reporting, Data Quality and Governance Unit by email at [DataReleaseRequests.DoH@nt.gov.au](mailto:DataReleaseRequests.DoH@nt.gov.au).

Disclosure and/or access to personal information relating to individual patients/clients will only occur if all necessary approvals - including the approval requirements set out in this Data Release Guideline - have been obtained.

Requests for identifiable information require reasonable justification why non-identifiable information is not sufficient for the purpose of the data request.

Personal information is data that discloses a person’s identity or from which a person’s identity is reasonably ascertainable. Information is considered identifiable where:

* It includes specific identifying information (eg. name, address, date of birth, medical record number); or
* Specific data elements are requested in combination (ie. date of birth, sex, postcode); or
* The data is to be combined with other information the requestor already holds or with other datasets that are being requested; or
* The data is aggregated and there are few individuals in a particular category.

Patient/client names and addresses are not stored within the Department’s data collections and are only available for the purpose of enabling data linkage. The patient/client’s medical record number (HRN) will only be provided external to NT Health where there is no alternative to its provision. In most instances a ‘Patient ID’ (encrypted HRN) will be provided.

### Privacy of organisations and service providers

As a general rule, the provision of data will occur in a manner such that the identity of organisations, or individual service providers within organisations, providing health services cannot be ascertained, either directly or indirectly. Health provider local identifiers will not be provided outside NT Health. The use of data identifying an organisation requires the approval of the local data owner, and if obtained, will be contingent on a signed deed of confidentiality and compliance.

### Privacy of Aboriginal Communities

The collection, use and disclosure of information from which Aboriginal communities might be identified is a sensitive issue in the NT. There is a non-legal concept of ‘community privacy’ which has existed and been respected in the collection and publication of health and other sensitive information about Aboriginal communities in the NT. As a matter of policy, the Department has undertaken to ensure that individual communities are not identified without their consent in Agency publications. This will be taken into consideration in the assessment of relevant requests for data.

It is possible to identify an Aboriginal community when specific data elements are provided, or from particular data elements in combination (eg. postcode, remoteness category). The use of data which would identify an Aboriginal community, either directly or indirectly, requires the permission of the Aboriginal community, and once obtained will be included in the deed of confidentiality and compliance.

### Balance between data release and privacy

In assessing all requests to release information, due care must be taken to minimise the risk of disclosing information about individuals, communities, or organisations, while maximising the potential for improved clinical practice, business processes and public good.

## Public information

Information and data sets that have been formally released to the public will be freely available.

## Summary level information

Summary level data sets will be provided with a level of aggregation such that the identity of individual patients/clients, communities or organisations cannot be reasonably obtained from the data set alone or by combination with other readily available data sets.

## Intended use

Data released can only be used for the purpose for which access or disclosure was sought and approved. Any additional use, or modification of intended use, requires further approval from the Department.

## Approval

Data will be approved by all relevant data owners prior to release.

## Data linkage

Data linkage requires specific skills and knowledge and, as per NHMRC National Statement[[6]](#footnote-8), is to be performed separately to any research project. Data linkage will be performed by staff employed by the Department or by agreed, appropriately qualified data linkage specialists or organisations. Certain requirements relating to data linkage are outlined within the data release request form and further specific conditions may be included by the Department within the applicable deed of confidentiality and compliance. Details of the documents comprising the data release request form are described within section 12 of this guideline.

## File format

Data will be provided in an agreed format, generally as a delimited or fixed width text file or in MS Excel, depending on file size. All files transmitted externally to the NTG network or email will be encrypted and password protected, with the password provided separately to the file.

## Work done on behalf of the Department

On occasion external parties are contracted to perform work on behalf of the Department and require NT Health data. In instances where the head agreement does not include provisions for data security, privacy and confidentiality, an additional deed will be required. The governing law in the Northern Territory in relation to information privacy is the *Information Act* (NT) or law with like obligations in another jurisdiction. Any contractual disputes will be dealt with in the jurisdiction of the Northern Territory.

## Data refusal

If a data release request is refused, the Department will provide the reason for refusal.

# Human Research Ethics Committee approval

Requests for information may require approval from one or both of the following NT Human Research Ethics Committees (HREC):

* Central Australian Human Research Ethics Committee
* Human Research Ethics Committee for the Northern Territory Department of Health and Menzies School of Health Research.

HREC provides an independent, competent and timely review of projects involving the use and disclosure of NT Health information with respect to their ethical acceptability, including the risks versus benefits of the proposed research. In undertaking ethical assessment of research proposals the HREC uses the *National Statement on Ethical Conduct in Human Research (2007)[[7]](#footnote-9),* which consists of a series of guidelines made in accordance with the *National Health and Medical Research Council Act 1992[[8]](#footnote-10)* (NHMRC).

Applications for ethics approval and relevant supporting documents will need to be submitted to the appropriate HREC. Relevant information is available via links at the Department’s website[[9]](#footnote-11).

All requests involving data linkage must have HREC approval.

# Data request for research purposes

All requests for the use of the Department’s data for the purpose of research must have the approval of one or both NT Human Research Ethics Committees, depending on the research and the population to be covered by the research. This includes research projects using NT data held by Australian Government agencies or SA NT DataLink.

For data to be released, the data Release request form must be updated to include:

* A copy of the relevant, current approval from the HREC; and
* Copies of the research protocol, project proposal, or HREC submission, any consent forms, questionnaires and associated documentation.

Patient/client level information will only be disclosed for research purposes if all the requirements of Information Privacy Principle 2.1(ca)(iv)[[10]](#footnote-12) have been complied with. Due to the level of granularity, the additional approval of the Department’s Chief Health Officer will be obtained.

# Data ownership

The Northern Territory of Australia (Territory) is the legal owner of all data collected by, within and for NT Health. The Chief Executive of the Department has primary responsibility (on behalf of the Territory) for the security, management, use and disclosure of the data. For the purpose of this guideline, data also includes personal information. ‘Ownership’ in relation to personal information means personal information is ‘in the custody of’ the Chief Executive of the Department.

To successfully and efficiently apply the principles and processes within this guideline, ownership of the various categories of data (i.e. financial, workforce, activity and patient/client level information) across NT Health has been delegated. It is necessary to gain approval from the data owner(s) prior to the use/release of data.

Data that is Territory-wide requires approval from the Territory-wide Data Owner relevant to the Data Category. Local Data Owner approval is required where the requested data is for a specific Health Service, hospital or clinic.

The following table provides a summary of the delegated Territory-wide, System Manager and Health Service owners of NT Health data:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Category** | **Data Owners** | | | |
| **Territory-wide Owners\*** | **Local Owners** | | |
| **TEHS** | **CAHS** | **System**  **Manager** |
| **Finance Data** | DoH Chief Finance Officer | TEHS Chief Finance Officer | CAHS Chief Finance Officer | DOH Chief Finance Officer |
| **Activity Data** | DoH Senior Director System Performance and Grants | TEHS Chief Operating Officer | CAHS Chief Operating Officer | DOH Deputy Chief Executive Governance & Business Services |
| **Workforce Data** | DoH Executive Director People & Organisational Capability | TEHS Director Workforce | CAHS Director Workforce | DoH Executive Director People & Organisational Capability |
| **Patient/Client Level Data** | DoH Senior Director System Performance and Grants and DoH Chief Health Officer | TEHS Executive Director Medical Services | CAHS Executive Director Medical Services | DOH Deputy Chief Executive Governance & Business Services |
| **Registry Data**  (and other legislated data) | DoH Chief Health Officer | Not Applicable | Not Applicable | Not Applicable |

“Territory-wide Owners” cover Department-only data as well as data across Health Services

# Roles and responsibilities

The following table defines the key stakeholders involved with the workflow processes associated with data release requests to the Department. Requests generated within or directed to local Health Services that include a requirement for data outside the Health Service need to be re-directed to the Department.

| Term | Definition |
| --- | --- |
| Data Steward | Data Stewards have delegated responsibility for setting overall strategic direction of data collections to ensure the collections are developed, maintained and utilised in accordance with the strategic goals of NT Health and use consistent and appropriate data standards. Stewardship is performed in collaboration with the Data Owners.  Data Stewards are also responsible for authorising the access, use and disclosure of data from a data collection for specifically defined purposes that comply with NT Health’s statutory obligations.  Chief Data Officer Data Management & System Reporting (DM&SR) Branch and other agreed data stewards |
| Data Owner | Data Owners are responsible for the management, oversight and use of data for their respective discipline/data category, including authorising access and release. Data Owners work in collaboration with the Data Steward in relation to the overall direction of their respective discipline/data category.  For Data Owners, refer to table in previous section |
| Data Custodian | Data Custodians have delegated responsibility for the ongoing development, maintenance and review of data collections. Data Custodians are responsible for the quality and provision of the data, its security, timeliness and adherence to standards. Data Custodians must be nominated and endorsed by the Data Stewards.  DM&SR Reporting Team Managers or other endorsed custodians |
| System Owner | System Owners are those positions directly responsible for the operational applications and source systems that capture and store the data.  Information Services – Application Leads |
| Subject Matter Expert | Subject Matter Experts are staff who possess expertise and knowledge in relation to specific data sets by discipline/data subject area. |
| Health Service Data Analyst | Data managers, analysts and reporters working directly for a Health Service to provide data and information specific to the Health Service. |
| Data User | End users and recipients of data. Can be both internal to NT Health and external (i.e. other government agencies, universities, researchers etc). |

# Approval(s) for release

For release approval to be completed, data owners are required to authorise release of data for their data subject area. The exception is where there is a separate agreed process in place, such as for the routine submission of data. These separate agreed processes are approved by the relevant data owner and are listed in a separate document for reference. The list may change from time to time.

# Data release workflow

The tables and figure in Appendix A outline the processes required when releasing information from data collections held by NT Health.

# Data release templates

The following forms are used in processing data release requests:

* Data Release Request form

For use by all Applicants (including applicant’s external to NT Health)

* Appendix A. Data Specification
* Appendix B. Deed of Confidentiality and Compliance
* Appendix C. Conditions of Publication

A copy of the data release request form can be obtained upon request to Data Management & System Reporting, Data Quality and Governance Unit by email at [DataReleaseRequests.DoH@nt.gov.au](mailto:DataReleaseRequests.DoH@nt.gov.au).

* Data Release Review and Approval form

Department ONLY (internal document)

* Data Release – Letter of Support

To be issued by Department to a successful applicant (including applicants external to NT Health) confirming support of application subject to completion of final requirements (e.g. completion, execution and return of deed(s) of confidentiality and compliance and conditions of publication form(s) etc.).

## Data release request form

Applicants must consult with the relevant data custodian of the data collection before applying for HREC approval (where such is required).

After initial contact with the data custodian, the applicant completes the data release request form. This form provides the Department with information about the applicant and the nature of their request. The data release request form will provide the scope of the requirements and ensure the request is clearly documented to enable the data custodian(s) and the data owner(s) to assess the request. It also describes the usage of the data, security, storage and disposal requirements, as well as restrictions on further dissemination of the data to third parties.

Where the data is required on a regular basis, completion of a new data release request form may not be required each time.

## Data release review and approval form – Department ONLY (internal)

Prior to releasing data, a data review and approval release form must be completed by Data Quality and Governance team, and the data custodian(s), and signed by the data owner(s). This form documents the assessment of privacy and the appropriateness of the data for review by the data owner(s).

For established routine data release requests, a data review and approval release form only needs to be produced on the initial request for data, unless substantial modifications to the data request have been made.

## Data release agreements

Data custodians need to ensure and be confident that the recipient of the data fully understands the conditions of the data release and their required obligations. The data custodians administer this by signing a data release deed of confidentiality and compliance with the requestor/recipients of the data. This is particularly important when releasing confidential and/or sensitive data.

The data release deed of confidentiality and compliance outlines obligations of privacy and confidentiality with respect to information received from the Department. Signing of the data release deed of confidentiality and compliance confirms and ensures authorised recipients are informed and understand their obligations.

Further to the deed of confidentiality and compliance, if there is a publication component a conditions of publication will be required to be signed by the requestor.

The data release deed of confidentiality and compliance is signed by all applicants who will have access to the data prior to data delivery to the requestor.

# Appendix A

## Request for data release – research and service planning or evaluation requests

### Research

|  |  |  |
| --- | --- | --- |
| Step | Action | Responsibility |
| 1. Initial Contact and Discussion | * Initial contact, discussion and high level scoping with Data Custodian to determine data exists, is appropriate and is available. | Requestor |
| 1. Generation of Request for Data Release | * Completion of *“*Data Release Request” form with submission to DM&SR Data Quality & Governance (DQ&G). | Requestor |
| 1. Review and Assessment | * DM&SR Data Quality & Governance, in conjunction with the relevant Data Custodian(s), assesses the request in terms of privacy, data fitness for purpose and data availability, with findings documented in the “Review and Approval” form. | DM&SR |
| 1. Obtain Approvals | * Obtain necessary approvals from relevant Data Owner(s) in accordance with the owners identified in Section 5. For example, if the data request is for admitted activity information across all NT Health, then approval will need to be obtained on the “Review and Approval” form by the Department of Health Senior Director System Performance Branch. | DM&SR  Data Owners |
| 1. HREC Approval | * The approved “Review and Approval” form is the Department’s documentation of in-principle support, a Letter of Support will be sent to the Requestor to finalise HREC approvals. * Submission to HREC for approval. | DM&SR  Requestor |
| 1. Submit Final Documentation | * Provide finalised documentation including but not limited to the “Data Release Request”, and the HREC submission and HREC approval. | Requestor |
| 1. Deed of Confidentiality and Compliance | * Signing of “Data Release Deed of Confidentiality and Compliance” and relevant documents. | Requestor /DM&SR |
| 1. Delivery of Data | * Extraction and delivery of data. | Requestor/Data Custodian(s) |

### Service planning and evaluation

| Step | Action | Responsibility |
| --- | --- | --- |
| 1. Initial Contact and Discussion | * Initial contact, discussion and high level scoping with Data Custodian to determine data exists, is appropriate and is available. | Requestor |
| 1. Generation of Request for Data Release | * Completion of *“*Data Release Request” with submission to Data Management & System Reporting (DM&SR). | Requestor |
| 1. Review and Assessment | * DM&SR Data Quality & Governance Unit, in conjunction with the relevant Data Custodian(s), assesses the request in terms of privacy, data fitness for purpose and data availability, with findings documented in the “Review and Approval” form. | DM&SR |
| 1. Obtain Approvals | * Obtain necessary approvals from relevant Data Owners in accordance with the owners identified in Section 5. For example, if the data request is for financial information across all NT Health, then approval will need to be obtained on the “Data Release Request Form” by the Department of Health Chief Finance Officer. | DM&SR  Data Owners |
| 1. Deed of Confidentiality and Compliance | * Signing of “Data Release Deed of Confidentiality and Compliance” or relevant documents. | Requestor /DM&SR |
| 1. Delivery of Data | * Extraction and delivery of data. | Requestor/Data Custodian(s) |

### Request for data release – other requests

| Step | Action | Responsibility |
| --- | --- | --- |
| 1. Initial Contact and Discussion | * Initial contact, discussion and high level scoping with Data Custodian to determine data exists, is appropriate and is available. | Requestor |
| 1. Generation of Request for Data Release | * Completion of *“*Data Release Request” with submission to Data Management & System Reporting (DM&SR). | Requestor |
| 1. Review and Assessment | * DM&SR Data Quality & Governance Unit, in conjunction with the relevant Data Custodian(s), assesses the request in terms of privacy, data fitness for purpose and data availability, with findings documented in the “Review and Approval” form. | DM&SR |
| 1. Obtain Approvals | * Obtain necessary approvals from relevant Data Owners in accordance with the owners identified in Section 5. For example, if the data request is for financial information across all NT Health, then approval will need to be obtained on the “Data Release Request Form” by the Department of Health Chief Finance Officer. | DM&SR  Data Owners |
| 1. Deed of Confidentiality and Compliance | * Signing of “Data Release Deed of Confidentiality and Compliance” or relevant documents as required. | Requestor /DM&SR |
| 1. Delivery of Data | * Extraction and delivery of data. | Requestor/Data Custodian(s) |

### External data release workflow



# Appendix B

## Glossary of terms

| Term | Meaning |
| --- | --- |
| Authorised User | An authorised user is a person who has obtained the appropriate approvals for the access and use of information. |
| Data Collection | Refers to a store of data captured in an organised way for a specific, defined purpose, which is not restricted to operational use by the business unit that created it but is available to a wider group of users. This includes paper-based collections as well as electronic collections and may contain information about individuals or business activities. Examples include data sets, datamart environments, and code tables.  A data collection shall have a Data Custodian. |
| Data Custodian | An individual with delegated responsibility for the ongoing development, maintenance and review of a data collection. The Data Custodian is responsible for the quality and provision of the data, its security, timeliness and adherence to standards. Data Custodians must be nominated and endorsed by the Data Stewards. |
| Data Linkage | Is the activity of finding connections between different pieces of information that are thought to belong to the same person, family, place or event. |
| Data Owner | An individual who is responsible for the management, oversight and use of data for their respective discipline/data category, including authorising access and release. The Data Owner also works in collaboration with the Data Steward in relation to the overall direction of their respective discipline/data category. |
| Data Repository | Refers to data that is collected from various sources, including operational data collections for the primary purpose of monitoring, evaluation, reporting and research. Examples of data repositories include data held within the Hospital Morbidity Data Collection, Finance Data Warehouse and the Emergency Department Data Collection. |
| Data Steward | A delegated person responsible for setting the overall strategic direction of a specific data collection. The Data Steward ensures the collection is developed, maintained and utilised in accordance with the strategic goals of NT Health, working in collaboration with the Data Owner(s). The Data Steward is also responsible for authorising access, use and disclosure of data from the data collection for defined purposes that comply with the Department of Health’s statutory obligations. |
| Data User | An end user, or recipient, of data. A Data User may be internal to NT Health or external (eg. other government agencies, researchers etc). |
| Health Information | "Health information" means:  (a) Personal information about:  (i) the physical or mental health of a person; or  (ii) a person's disability; or  (iii) the provision of a health service to a person, including the person's expressed wishes about that provision; or  (b) Personal information connected with the provision of a health service; or  (c) Personal information connected with the donation or intended donation by a person of his or her body parts, organs or bodily substances; or  (d) Personal information that is genetic information about a person in a form that is, or could be, predictive about the person's health at any time. |
| Health Service Data Analyst | A data manager, analyst or reporter who works directly for a health Services to provide data and information specific to the Health Service. |
| Human Research Ethics Committee (HREC) | Specialised committees that protect the welfare and rights of participants involved in research. HREC review research proposals that either involve humans directly or require the use and disclosure of personal health information. HREC is responsible for ensuring that research proposals are ethically acceptable and in accordance with relevant standards and guidelines. |
| Identifiable Information | Information where the identity of an individual, health service, clinician or health professional can be reasonably ascertained by the holder of the information. Examples of identifiers include: name, address, full date of birth, geocodes, hospital names or numbers. An individual will be identifiable if the information contains unique personal identifiers and the holder of the information also has the master list linking the identifiers to individuals. It may be possible to ascertain the identity of individuals from combinations of data elements, or aggregated data where there are very few individuals in a particular category. |
| Information | Refers to data that has been processed in such a way as to be meaningful to the person who receives it. |
| Information Disclosure | In the context of this guideline information ‘release’ and ‘disclosure’ are considered synonymous and involves providing information from the Department of Health’s data collections to authorised users (both internal and external to the Department of Health). Information is generally released in a form of hard copy documents, data extracts or electronic medium. |
| Information Release | Refer to Information Disclosure. |
| Non-Identifiable Information | Non-identifiable information is information that may correspond to a particular person or health provider, but is not sufficient to identify, contact or locate the person to whom such information pertains. Non-identifiable information is generally collected in an aggregated form.  In a health context, requests for non-identifiable information refer to requests for information (record level or aggregated) that have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual or health facility can be identified by the recipient of the information.  This also applies to data that may contain a unique person identifier, but the identifier has no meaning to the recipient of the information when viewed alone or in combination with other data. |
| Operational Data Collection | Includes data that is collected as part of the day-to-day activities of an area for the primary purpose of tracking and managing operational aspects of the area. The operational data collection is typically a transaction- based system which contains detailed data elements to represent the activities of the area. |
| Personal Information | "Personal information" means government information from which a person's identity is apparent or is reasonably able to be ascertained. |
| Potentially Identifiable Personal Health Information | Contains a range of data items that in combination with each other contain sufficient overall detail that it is possible that some individuals could be identified. This may result when combining two or more de-identified data sets. |
| Patient/Client Level Data | Usually data at the level of an individual person. Patient level data need not directly identify the data subject, but is more vulnerable to re-identification than aggregate data. |
| Primary Use Data | The primary purpose for the collection is the reason why the information was collected. |
| System Owner | The position directly responsible for an operational application or system that captures and stores data |
| Subject Matter Expert | An individual who possesses expertise and knowledge in relation to specific data sets by discipline/data subject area |

1. <https://legislation.nt.gov.au/en/Legislation/HEALTH-SERVICES-ACT> [↑](#footnote-ref-3)
2. <https://health.nt.gov.au/health-governance/service-delivery-agreements-sda> [↑](#footnote-ref-4)
3. <https://infocomm.nt.gov.au/privacy/information-privacy-principles> [↑](#footnote-ref-5)
4. <http://hdl.handle.net/10137/726>, NT Health Privacy Policy [↑](#footnote-ref-6)
5. <http://internal.health.nt.gov.au/pgc/dm/_layouts/WordViewer.aspx?id=/pgc/dm/Documents/CSB/Data%20Management/Data%20Governance%20NT%20Health%20Framework.docx&DefaultItemOpen=1> [↑](#footnote-ref-7)
6. <https://www.nhmrc.gov.au/book/chapter-3-2-databanks> [↑](#footnote-ref-8)
7. <https://www.nhmrc.gov.au/book/national-statement-user-guide-0> [↑](#footnote-ref-9)
8. <https://www.legislation.gov.au/Details/C2014C00364> [↑](#footnote-ref-10)
9. <http://www.health.nt.gov.au/Agency/Advisory_Groups_and_Taskforces/Human_Research_Ethics_Committee/index.aspx> [↑](#footnote-ref-11)
10. A copy of the guidelines issued by the NT Information Commissioner for IPP2.1(ca)(iv) (Use and disclosure of health information for research and statistical purposes) can be accessed from: <https://infocomm.nt.gov.au/resources/guidelines> [↑](#footnote-ref-12)