Northern Territory Government

DEPARTMENT OF
HEALTH AND FAMILIES

Data Access Protocol

For Secondary Use of Data Warehouse Derived Data Collections

February 2009

Table of Contents

Background

The Data Access Protocol (DAP) has been developed in response to legislative requirements under the Northern Territory Information Act; a recommendation from the Information Technology (IT Controls Review) Audit by the Auditor-General for the Northern Territory, and a requirement under the framework for Building Healthier Communities.

The DAP recognises that, as set out in the Information Act, 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. Care must be taken in providing access to information held by the Department of Health and Families (DHF) to minimise the risk of disclosing information about people, communities or organisations.

Purpose

The DAP will be used in managing access to and use of data and information that is held in the DHF Corporate Data Warehouse (the Data Warehouse). The DAP aims to provide the rules and processes that are to be used to manage data security and any risk associated with access to data held within the Data Warehouse, while maximising the potential for improved clinical practice, business processes and public good.

The DAP recognises that information is a corporate resource to be utilised wherever possible to enhance strategic and operational decision-making. In general, the data in the Data Warehouse is used to generate management information.

Through the DAP, Data Custodians facilitate:

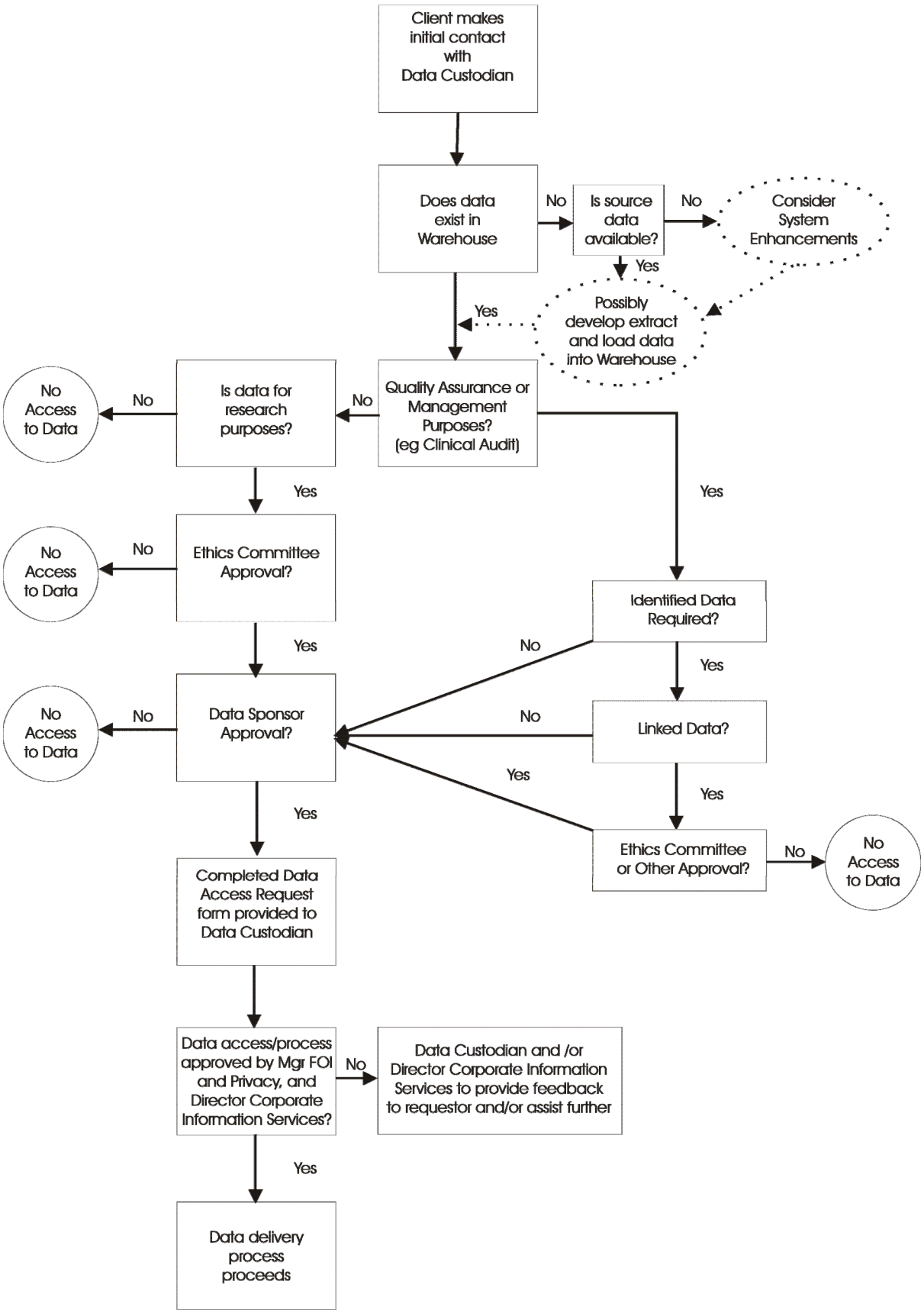
- a service to assess the availability of data in the Data Warehouse, including implementation of datamart development;
- a streamlined and consistent process for the delivery of requested data. This includes managing requests for identifiable data and linked data, and requests for data for quality assurance or research purposes;
- access for approved registered BusinessObjects users to requested data held in the Data Warehouse; and
- timely delivery of data reports or provision of data access.

Benefits

In summary, the benefits the DAP provide are:

- facilitation of a dialogue for defining data requirements and timely delivery of appropriate and relevant data;
- protection of personal and sensitive information as required under the Information Act;
- reassurance for Data Sponsors of robust management of data stored in the Data Warehouse; and
- an assurance that consistent and standard processes are used for requests to access data held in the Data Warehouse.

Data Delivery Flow Chart



Overview

Subsets of the data stored in most DHF operational information systems such as CareSys, PCIS, CCIS, GAS, PIPS and Labtrak are periodically extracted and stored in the Data Warehouse.

This is done to facilitate a number of processes, including:

- strategic and operational management reporting;
- decision support;
- clinical, epidemiological and social health research;
- service level agreements (developing and reporting); and
- Australian Government reporting requirements.

The DAP aims to provide guidelines, for both internal and external clients, that are to be used in managing access to and use of information for secondary purposes through the Data Warehouse: refer the Information Act, Information Privacy Principles (IPP 2), and DHF Privacy Policy. The DAP exists beside other DHF protocols and agreements which relate to more specific data and/or data sources (eg Aboriginal Health Forum KPI data).

The DHF Corporate Information Services Branch provides information and advice on departmental information management policies and practices, as well as details of new and developing information and records management legislation. Corporate Information Services Branch is responsible for maintaining and publishing the DAP, including on the DHF intranet site.

The Appendices to the DAP contain supplementary information on data definitions, data security and a schedule of Data Sponsors and Data Custodians.

Scope

This DAP relates only to data that has been extracted from operational systems and is held in the Data Warehouse and its associated datamarts, data sets (including data set representations such as BusinessObjects Universes) and reports.

Access, security and confidentiality of the information stored in DHF operational systems is outside the scope of this DAP.

General Principles

Information is a Corporate and Public Good Resource

The Data Warehouse was established as a means of facilitating access to quality data to assist evidence-based decision-making within the Agency and by relevant non-government organisations (NGOs) on matters relating to service delivery. Reasonable access to data at this level is considered essential to furthering this objective.

Unless specifically collected on behalf of, or provided by, another organisation (for example, NGOs), information captured by DHF employees and others acting on behalf of DHF remains a departmental corporate resource that will be utilised wherever possible to enhance strategic, clinical and operational decision-making and as a means of serving the public good.

Management Information

In general, the data in the Data Warehouse is used to generate management information.

Wherever possible, operational information will be provided by the relevant operational system. The Data Warehouse will only be used for unit record level reporting when the required information cannot be generated from an operational system in a timely, economical or appropriate manner.

The Data Warehouse is used to generate data that is specified for provision in an Australian Government agreement, where that data exists in the Data Warehouse.

Privacy of Individuals

Access to identified information relating to individual clients will only be provided if all necessary approvals as required under the DAP have been obtained, and in accordance with the Information Privacy Principles.

Privacy of Groups and/or Organisations

Access to information by which individual communities and/or organisations can be identified will only be provided with approval of the appropriate Data Sponsor(s), and endorsement by the community and/or organisation may be required.

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 clients, communities or organisations cannot be reasonably obtained from the data set alone or by combination with other readily available data sets. Summary level data sets will be widely available.

De-identification of Unit Record Data

In general, data sets containing unit record data will be de-identified. That is, the Data Warehouse will randomly allocate an identifier that can be used to link various services provided to the client but cannot be used to obtain any information about the client from the operational systems.

Balance between Data Access and Privacy

In assessing all requests for access to 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.

Protocol for Data Access and Reports

Direct access to data stored in the Data Warehouse will only be provided to DHF staff who are registered BusinessObjects users.

A management reporting service is also available to deliver specific data sets to Agency staff and external clients as ad hoc requests, or routinely under national agreements with, for example, the Productivity Commission, AIHW, Health Boards and Menzies School of Health Research.

Generally, data derived from the Data Warehouse is delivered to external clients as reports in statistical and aggregated form. Reports can also be delivered which include identifiable information for the purposes permitted under Information Privacy Principle 2.1.

Requests for de-identified and/or unlinked data can be delivered more quickly. Refer below for an outline of issues related to identified data and linked data requests.

Management of Requests for Access to Data

All requests, from both internal and external clients, for data access or data delivery by way of report, must be lodged with the appropriate Data Custodian (refer Appendix 3 for details). There are Data Custodians for each major Agency function within Acute Services, Health Services, Health Protection, NT Families & Children, and Performance & Resources.

In order to access data held in the Data Warehouse, the processes set out below should be followed:

Requests from Parties External to DHF

- The DHF representative who receives the request should contact the relevant Data Custodian to verify that the data to be requested is held in the Data Warehouse, and discuss possible options if the data does not exist in the Data Warehouse. The Data Custodian will provide advice to the requester on data quality, date range availability, possible timeline for data access or report delivery etc.
- If the data does exist in the Data Warehouse, the Data Access Request Form (refer Appendix 2) must be completed, ensuring all necessary approvals have been obtained, including from any relevant Data Sponsor/s and, if required, Ethics Committee.
- The requester should lodge the completed Data Access Request Form with the appropriate Data Custodian, including an undertaking to store and dispose of the data appropriately and in accordance with the Information Act and other relevant legislation.
- Once the Data Custodian is satisfied that the Data Access Request Form has been accurately completed and the necessary approvals obtained from the Data Sponsor(s) and Ethics Committee (if required), the request for access will be processed. The Data Access Request Form will be sent to Corporate Information Services for final endorsement prior to the request being actioned, unless the request is in accordance with existing approved processes. Corporate Information Services will routinely seek endorsement from the DHF Manager FOI & Privacy for all requests.

- Once final approval has been obtained, all necessary feedback will be provided to the client on data quality, date range availability, possible timeline for data access or report delivery etc. The Data Custodian or appropriate DHF representative will be the point of contact for the client for any necessary liaison, information update etc.

Requests from Parties Internal to DHF

- The requester should contact the relevant Data Custodian to verify that the data to be requested is held in the Data Warehouse, and discuss possible options if the data does not exist in the Data Warehouse.
- If the data does exist in the Data Warehouse, a Data Access Request Form must be completed, ensuring all necessary approvals have been obtained, including from any relevant Data Sponsor/s and, if required, Ethics Committee.
- A standard email pro forma can be used as the internal Data Access Request Form for routine data access requests. Information to be provided includes:
  - a description of data required (relevant data collection/BusinessObjects Universe);
  - what the data will be used for;
  - whether the data requested is identified or de-identified;
  - the time period for which access to the data is required; and
  - an undertaking to store and dispose of the data appropriately and in accordance with the Information Act and DHF Privacy Policy.
- The requester should lodge the completed Data Access Request Form with the appropriate Data Custodian.
- Once the Data Custodian is satisfied that the Data Access Request Form has been accurately completed and all necessary approvals obtained, the request for access will be processed. The Data Access Request Form will be sent to Corporate Information Services for final endorsement prior to the request being actioned, unless the request is in accordance with existing approved processes. Corporate Information Services will routinely seek endorsement from the DHF Manager FOI & Privacy for all requests.
- Once final approval has been obtained, all necessary feedback will be provided to the client on data quality, date range availability, possible timeline for data access or report delivery etc. The Data Custodian will be the point of contact for the client for any necessary liaison, information update etc.

Approval Processes for Access to Hospital Activity Data

Requests for access to hospital activity data by staff employed at another hospital are to be approved by the relevant hospital General Manager (or delegate).

Access to cross-hospital activity data (including requests from individuals not employed at the hospital/s) are to be approved by the relevant Data Sponsor/s, and the Director, Acute Care Systems and Performance.

Identified Data

Under the Information Act, DHF staff may use identified data for a range of secondary purposes directly related to the primary purpose for which the information was collected without the consent of the individual(s) to whom the data refers. Where the use of de-identified data will not suffice, and provided it is within the reasonable expectations of the individual(s), identified data may be used without obtaining the prior consent of the individual(s) for such

purposes as planning, evaluation and accreditation activities, quality assurance or clinical audit activities, funding and service monitoring. These purposes do not include use of identified data for teaching or research purposes.

Before identifiable data is sought for these purposes, the data requester should consider:

- whether or not the use of de-identified data will suffice;
- the way DHF clients may want to access our services; and
- any reasonable expectations clients may have about the use of their personal information.

Use of identified data for quality assurance activities is generally considered an approved use under the Information Act and related Information Privacy Principles, but any such use must be closely monitored by the relevant Data Sponsor. Advice should be sought from Corporate Information Services on requests for other purposes, and further advice would normally be sought from the DHF FOI & Privacy Unit and/or Legal Services Branch.

Although the actual names of DHF clients may not necessarily be included as part of a request for data, other data elements and their combinations may be able to produce identifiable data sets. In processing any request for data that has been collected from individuals who have received a service from DHF and are identifiable or capable of being re-identified, DHF has legal and ethical obligations to ensure that data that is being requested is for an approved purpose and in these instances the advice of Corporate Information Services must be sought, who will seek further advice from the FOI & Privacy Unit and /or Legal Services Branch.

Datamart Development

Where new permanent data elements are required to be added to existing datamarts or the development of a new datamart is required to satisfy a client's requirements, the Data Custodian will liaise with the appropriate Data Warehouse staff in regard to any such requirements, including the identification of appropriate Data Sponsor/s. No Universe/Datamart will be placed in a production environment without identification of an appropriate Data Sponsor.

Data Access Request for Research Purposes

All requests for the use of data for the purpose of research must have the approval of a Human Research Ethics Committee. The Data Access Request Form must include:

- a copy of the relevant, current approval from a properly constituted and approved Human Research Ethics Committee; and
- copies of the research protocol or project proposal, any consent forms, questionnaires and other associated documentation.

Community Privacy

The collection, use and disclosure of information from which Indigenous communities may be identified is a sensitive issue in the Northern Territory. 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 Indigenous communities in the Territory. As a matter of policy, DHF 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 and, as an example, where cell counts less than five occur for any data delivered with demographic components, the data must not be released or published.

Requests for Linked Data

Corporate Information Services is responsible for ensuring that any request for a linked data set is managed appropriately. Data linkage raises a number of ethical and privacy considerations, particularly where this may involve the linkage of data that has been collected for different and separate purposes. The Data Warehouse offers a secure process by which data linkage can be facilitated that does not involve the disclosure of identifiable data. However, if there is a request to link data and provide an identifiable data set, then the provisions set out under Identifiable Data above will apply, including advice from the DHF FOI & Privacy Unit and/or Legal Services.

In all cases, approval of the relevant Data Sponsor, or authorised delegate, is a mandatory requirement for any request for linking of data.

Data Access Approvals

The Data Custodian handling the data access request must ensure that all necessary approvals have been obtained from the relevant Data Sponsor/s, for both ad hoc requests, and for regular management or other reporting requirements that may be in place. If the Data Sponsor imposes additional restrictions on a request for access to a particular data collection this must be recorded on the Data Access Approval Form by the Data Sponsor. If the initial Data Sponsor transfers the approval to a more appropriate Data Sponsor, this must be recorded on the Data Access Approval Form by the initial Data Sponsor.

Where access to more than one data set is being requested and is to be linked, whether identifiable or not, approval must be obtained from all relevant Data Sponsors.

Any approvals that are required from a Human Research Ethics Committee must be obtained by the individual/organisation requesting the data access prior to their application for access.

Note: 1. Prior to any publication or release of data or information derived from the data, the Data Sponsor will be provided with adequate opportunity to review the way in which the data has been interpreted and endorse any such publication or release.

Note: 2. Any publication of data provided, in whatever format, will correctly attribute the origin of the data.

Data Access Refusal

If a request for access to data is refused, the Data Custodian will document the basis for the refusal and provide a copy to all parties concerned.

Requests for access to identified or identifiable personal information by individuals or organisations external to the Department is limited and will be approved on a case-by-case basis by the relevant Data Sponsor and the Director, Corporate Information Services, who will seek further advice from the FOI & Privacy Unit and/or Legal Services Branch.

Identified or identifiable data will not in most instances be provided for purposes other than clinical use or health research.

Role of Corporate Information Services

The Director, Corporate Information Services (the Director), or delegate, has responsibility for the 'gatekeeper' function of final endorsement prior to data access requests being granted. The Director must be satisfied that all requirements and processes under this Data Access Protocol have been satisfied, particularly in relation to identified or identifiable information.

Data Access/Delivery

Once all approvals have been obtained, the Data Custodian is responsible for managing and scheduling any additional data management work required to achieve data access/delivery, including:

- liaising with the Data Warehouse Manager to ensure any enhancement work required on an existing Universe is satisfactorily undertaken; and
- coordinating all work required for any new datamart development in order to deliver the requested data.

If necessary, the Data Warehouse Manager may approve the creation of a temporary datamart or data set containing identified personal information as a one-off for a specific project, if this has been approved followed the processes described in the DAP. This datamart or data set will be deleted immediately the project has been completed, unless additional approval has been sought.

Glossary

Term	Definition
BusinessObjects Universe	Business representations of the underlying data incorporating business rules. Universes enforce security and enable periodic and ad hoc reporting. This is how most data requests are satisfied.
Data Custodian	There is a Senior Information Analyst for each major departmental function, including Acute Care Services, Health Services, NT Families & Children, and Corporate Services Reporting functions. The Data Custodian responsible within each program/function system is the first point of contact for anyone seeking access to data that is held in the particular data collection.
Data Collection	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 developed 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 code tables, data sets and datamart environments.
Data Element	The components of a record eg surname, first name etc.
Data Set	A collection of records.
Data Source	Data sources are the operational information systems and can also be data sets provided by internal or external agencies eg standard population data sets from the Australian Bureau of Statistics.
Data Sponsor	The person who undertakes the duties of ownership of a data collection under the control of the Agency.
Data Warehouse	A corporate data repository that contains linked datamarts of data derived from corporate information systems.
Datamart	An enhanced subset of the data held in the Data Warehouse for a specific business purpose. Datamarts provide a mechanism for meaningful data analysis for management purposes.
Disclosure	Releasing personal information to organisations or persons outside DHF. This does not include giving an individual information about themselves.
Operational Information Systems	Information systems that capture activity at the point of service delivery eg CareSys.
Personal Information	Any recorded information from which a person's identity is apparent or is reasonably able to be ascertained.

Primary purpose for collection and use of data	The primary purpose is the main or dominant reason a health service provider collects information from an individual, that is, for the purpose of providing a health service to the individual from whom the information is collected.
Privacy	Means privacy with respect to personal information, but also with respect to Northern Territory Indigenous communities.
Quality Assurance	A program for the systematic monitoring and evaluation of the data integrity to ensure that standards of quality are being met.
Record	Recorded information in any form (including data in a computer system) that is required to be kept by a public sector organisation as evidence of the activities or operations of the organisation, and includes part of a record and a copy of a record.
Secondary use of data	A public sector organisation must not use or disclose personal information about an individual for a purpose ("the secondary purpose") other than the primary purpose for collecting it unless one or more of the secondary purposes set out in IPP 2.1 can be satisfied.
Summary Data Set	Consists of records containing counts, sums, averages, rates or other summary statistics that are derived by aggregating and/or otherwise manipulating unit record data sets.
System Owner	Manages the operational database system on behalf of the Data Sponsor. Ideally this should be someone with a detailed knowledge of the data collected and manipulated by the system.
Unit Record Data Set	Consists of records containing information referring to a single event associated with an individual or organisation (such as an episode of care or a service event). Unit record data sets may or may not contain information that identifies individuals or organisations.

DATA ACCESS REQUEST FORM

Request for delivery of/access to data held in the DHF Data Warehouse

PART A – Requestor Details

Date of Request _____

Name of Requestor _____

Position Title _____

Section/Branch/Organisation _____

Telephone _____

E-mail _____

Supervisor's Name _____

Supervisor's Position Title _____

Signature of Supervisor
(as endorsement of access request) _____

Applicant's certification about use of information

1. The information to which access is sought will be used solely for the purpose of undertaking this project/activity and all reasonable measures will be taken to ensure that the arrangements for the security, use and disposal of the information accessed are complied with.
2. Any publication, presentation or other uses for which the data requested will be used, will correctly attribute the origin of the data.
3. Where the endorsement of the Data Sponsor is required for any release of data or information derived from the data, adequate opportunity for review and comment will be provide.
4. I understand that data will be transmitted to me in a secure manner (eg electronic data sent via email will be encrypted and password-protected), and that where I have approval to convey information to a third party I will do this in a secure manner.
5. I have read, understand and agree to comply with the DHF Privacy Policy.

Signature of Applicant _____

PART B – Identifiable Data

This section is to be completed where:

- the request is for access to patient/client identifying records; or
- there is intended or requested data linkage with other data; or
- the data will be used for research purposes.

Health Research Ethics Committee approval (if data is for research purposes) Yes ☐ No ☐

Period of Data Retention _____

Details of any intended third party provision _____

(If not known at time of request, a further request is required before data provision or access is provided to any person not named in this application.)

PART C – Data Request Details

General description of data required to be accessed

Name of Data Collection _____

Data Elements Required _____

Data range/s required – eg: service events date range, age range

_____

Period of Approval (ongoing or fixed period – the latter is required for a project) _____

Data Request Category	☐ ad hoc report	☐ periodic report	☐ data audit
Required Delivery Time	☐ this week	☐ this month	☐ next month
	☐ this quarter	☐ next six months	
Level of Request	☐ urgent	☐ important	☐ routine

Reasons for data request: (eg how the data will be used; the aims and objectives of the Project/Activity including, where relevant, details of cooperating agencies, sponsors and other stakeholders; any legislative requirement authorising collection of the data,; funding implications)

Part D – Data Security

Detailed description of data security measures (including how and where data will be stored):

How data will be disposed of:

Name, position, role of all people with access to the data:

PART D – Approval

I have read the material set out in this application and approve access to the information requested for the purpose of this project/activity in accordance with, and subject to, the methodology and measures set out in this application.

Data Sponsor Name _____ Signature _____

Approved by Data Sponsor Yes ☐ No ☐ Date

Signature Manager FOI & Privacy _____

Endorsed by FOI & Privacy Yes ☐ No ☐ Date

Signature Director CIS _____

Endorsed by CIS Branch Yes ☐ No ☐ Date

Data Description	Universe	Data Sponsors/alternative data sponsor	Data Custodian	Source System
Acute Care				
• CIA	CIA	RDH - Clinical Governance Group, ASH – Clinical Governance Committee, KDH – Director of Medical Services (Dr Tony Watson), TCH – Manager TCH (Michael Wright), GDH - Director of Medical Services – (	CIA Officers at each hospital	CareSys
• Clinical Audit	Clinical Audit data mart	Data access is provided to clinicians on patients who have received services from their Division. Clinical Division Heads act in the role of "Data Sponsor" for data access approvals.	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Infection Control				
• Intensive Care (Critical Care)		Director Intensive Care	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Maternal & Child Health (Paediatrics)		Director Maternal & Child Health	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Medicine		Director Medicine	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Surgery/Theatre		Director Surgery & Critical Care	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Emergency Dept	ED data mart	Director Emergency	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Crossborder charging	Crossborder data	Director Acute Care Systems Performance	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Darwin Private Hospital	DPH data	Manager, Darwin Private Hospital	Manager Acute Care Data Unit	DPH database

Data Description	Universe	Data Sponsors/alternative data sponsor	Data Custodian	Source System
			(Gary Inglis)	
• Hospital Activity Reporting (Inpatients)	HAR data mart/ 5YR data mart	Director Acute Care Systems Performance	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Hospital Activity Reporting (Outpatients)	HAR_91 data mart	Director Acute Care Systems Performance	Manager Acute Care Data Unit *(Gary Inglis)*	CareSys
• Pathology	Pathology data mart	Director Pathology (Prof Ken Donald)	Information Analyst for Acute Care *(Gary Inglis)*	Labtrak database
• Patient Travel	PTS data mart	Director Acute Care Systems Performance	Information Analyst for Acute Care *(Gary Inglis)*	Patient Travel System
• Perinatal	Perinatal data mart	Program Director Maternal, Child and Youth Health	Perinatal Data Business Analyst *(Sheryl Mccullough)*	CareSys / DPH database
• Pharmacy	Pharmacy data mart	Chief Pharmacist	Information Analyst for Acute Care *(Gary Inglis)*	Ascribe database
• Radiology	Radiology universe	Director Radiology	Information Analyst for Acute Care *(Gary Inglis)*	
• Renal	Renal universe	Director Medicine	Information Analyst for Acute Care *(Gary Inglis)*	CareSys
• Surgery/Critical Care	Surgical data mart	Director Surgery & Critical Care, *alt* Director Surgery	Information Analyst for Acute Care *(Gary Inglis)*	CareSys
• Waitlist	Waitlist data mart	Director Acute Care Systems Performance	Management Information Officer for Acute Services	CareSys
• Retrieval (NTRSD)	Retrieval Services	Director of Retrieval Services	Director of Retrieval Services	

Data Description	Universe	Data Sponsors/alternative data sponsor	Data Custodian	Source System
Health Protection				
• Alcohol & Other Drugs		Director Alcohol & Other Drugs	Manager CCIRS	
• Domestic Violence	Domestic Violence data mart	Manager Women's Health Strategy Unit	Manager Health Services Data Unit (Richard Inglis)	Domestic Violence website
• Immunisation	Immunisation General	Head of Immunisation), alt Director Disease Control	Manager Health Services Data Unit (Richard Inglis)	CCIS Immunis'n module
• Leprosy	Leprosy	Leprosy Medical Officer	Manager Health Services Data Unit (Richard Inglis)	Leprosy
• Market Basket Survey System	Market Basket	Program Director, Nutrition & Physical Activity	Manager Health Services Data Unit (Richard Inglis)	Market Basket Survey
• Mental Health (Hospital)		Mgr Mental Health Services	Information Analyst for Acute Care (Gary Inglis)	Caresys
• Mental Health (Community)	Mental_Health data mart	Director Mental Health	Manager Community Services Data Unit (Emidio Coccetti)	CCIS
• Notifiable Diseases	Notify data mart	Director Disease Control	Head of Surveillance (Dr Peter Markey)	Notifiable Diseases d'base
• Rheumatic Heart	Rheumatic Heart	Community Paediatrician Disease Control	CNC NT Rheumatic Heart Program (Jeff Tinsley)	Rheumatic Heart Register
• Syphilis Register		Director, Disease Control	Manager Health Services Data Unit (Richard Inglis)	
• Tuberculosis	Tuberculosis	TB Medical Officer Control	Manager Health Services Data Unit (Richard Inglis)	CCIS

Data Description	Universe	Data Sponsors/alternative data sponsor	Data Custodian	Source System
NT Families & Children				
• Family and Children's Services	FYCS data mart	Director Family and Children's Service	Manager Community Services Data Unit (Emidio Coccetti)	CCIS
• Family and Children's Services	CCIS_GENERAL	Director Family and Children's Service	Manager Community Services Data Unit (Emidio Coccetti)	
Health Services				
• Aged Care & Disability (ACAT)	ACAT Datamart	Director Aged & Disability	Manager Community Services Data Unit (Emidio Coccetti)	CCIS
• Aged Care & Disability (CCIS General)	CCIS_GENERAL	Director Aged & Disability	Manager Community Services Data Unit (Emidio Coccetti)	
• Aged Care & Disability (CSTDA)	CSTDA Datamart	Director Aged & Disability	Manager Community Services Data Unit (Emidio Coccetti)	CCIS and NGO database
• Aged Care & Disability (HACC)	HACC Datamart	Director Aged & Disability	Manager Community Services Data Unit (Emidio Coccetti)	CCIS and NGO database
• Community Health	Generic data mart	Director Community Health	Manager Health Services Data Unit (Richard Inglis)	CCIS
• Coordinated Care	CCT	Health Board CEO9s) Clinical Division Heads	Manager Health Services Data Unit (Richard Inglis)	CCT database
• Growth Assessment and Action	GAA data mart GAAWARE	Program Director Maternal, Child and Youth Health	Manager Health Services Data Unit (Richard Inglis)	GAA Survey GAAWARE
• Healthy School Age Kids	Health School Age Kids	Program Director Maternal, Child and Youth Health	Manager Health Services Data Unit (Richard Inglis)	HSAK
• Interim KPI	IDCT	Director Remote Health	Manager Health Services Data Unit (Richard Inglis)	IDCT

Data Description	Universe	Data Sponsors/alternative data sponsor	Data Custodian	Source System
• Nutrition	Generic CCIS	Program Director, Nutrition & Physical Activity	Manager Health Services Data Unit (Richard Inglis)	CCIS
• Palliative Care	Generic CCIS	Director Community Health	Manager Health Services Data Unit (Richard Inglis)	CCIS
• Primary Care	PCIS	Director Remote Health	Manager Health Services Data Unit (Richard Inglis)	PCIS database
Corporate Services				
• Client Master Index	Client Master Index	Chief Information Officer	Information Analyst for CMI	Client Master Index
• Finance	GAS data mart	Chief Finance Officer	Manager Corporate Systems Data Unit *(Richard Smith)*	GAS mainframe
• Payroll	PIPS data mart	Chief Finance Officer	Manager Corporate Systems Data Unit (Richard Smith)	PIPS
Strategic Quality				
• Complaints	Complaints	Senior Director, Office of the CE	Complaints & Sentinel Events Coordinator *(Suzanne Cameron)*	
Systems Performance				
• Aboriginal Language Survey (ALS)	ALS	Ass Sec Systems Performance & Aboriginal Policy	Principal Policy Officer, Aboriginal Health	
• Initiatives Activity	Policy data mart	IASS Administrator	Manager Corporate Systems Data Unit (Richard Smith)	IASS

Privacy Policy

Appendix 3

Introduction

The Northern Territory Government has established a privacy regime for the Northern Territory public sector under the *Information Act.* The Act establishes ten Information Privacy Principles (IPPs) that impose specific obligations on all NT Government agencies concerning the collection, use, storage and other handling of personal information.

Personal information includes personal details of an individual and any other information that directly or indirectly identifies a person who is alive or who has been alive within the last five years. All personal information collected in the provision of a health service is considered to be 'health information' or 'sensitive information' under the IPPs.

Policy Statement

1. The Department of Health and Families (DHF) is committed to safeguarding the privacy of the personal information that it collects and handles and has implemented measures to comply with its obligations under the IPPs.
2. DHF collects and handles a range of personal information about clients and staff for the purposes of providing services or carrying out its functions. DHF also uses some of this information for planning, funding, monitoring, and evaluating its services and functions. Where practicable, when using information for these purposes, identifying details such as name and address are removed. Personal information is not included in reports or publications that are released to the public, except with the consent of the person concerned or where this is authorised by law.
3. In accordance with its responsibilities, the services and functions DHF provide relate primarily to the areas of health, community support, and the protection of public health and safety. The main services provided include aged and disability, alcohol and other drugs, child protection, environmental health, family and children's, mental health, primary and community health, public health and public hospital services.
4. DHF recognises that the nature of these services means that much of the information handled is particularly sensitive and acknowledges the right of individuals to have their information handled in ways that they would reasonably expect and that respect their privacy.
5. DHF recognises that it provides services to a culturally diverse community and makes every effort to ensure that information is handled in culturally sensitive and appropriate ways.
6. Subject to the exceptions expressly stated in the IPPs, DHF will:
    - collect only that information which is needed for a particular purpose ('the primary purpose');
    - collect sensitive information (which includes health information) directly from the person concerned, wherever possible, and with their consent;
    - take reasonable steps to let the person concerned know why information about them was collected and how DHF will handle it;
    - use and disclose sensitive information only for the primary purpose, or for another purpose ('a secondary purpose') which is directly related to the primary purpose and one which the person would reasonably expect;
    - otherwise use and disclose sensitive information with the person's consent (except where it is an emergency and the information is needed to lessen or prevent serious harm, or its use or disclosure is authorised by law);
    - take all reasonable steps to ensure the information it collects is stored securely, protecting it from unauthorised access;
    - take reasonable measures to ensure the information it collects is accurate, complete and up-to-date;
    - provide the person concerned with access to information held about them, and to seek its correction where the person considers the information is inaccurate, incomplete or out-of-date.

Appendix 4

Information Act

Information Privacy Principles

IPP 1 Collection

1.1 A public sector organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 A public sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) a public sector organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it;

(b) the fact that the individual is able to have access to the information;

(c) the purpose for which the information is collected;

(d) the persons or bodies, or classes of persons or bodies, to which the organisation usually discloses information of the same kind;

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, a public sector organisation must collect personal information about an individual only from the individual.

1.5 If a public sector organisation collects personal information about an individual from another person, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of the individual or another individual.

IPP 2 Use and disclosure

2.1 A public sector organisation must not use or disclose personal information about an individual for a purpose ("the secondary purpose") other than the primary purpose for collecting it unless one or more of the following apply:

(a) if the information is sensitive information –

(i) the secondary purpose is directly related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(b) if the information is not sensitive information –

(i) the secondary purpose is related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(c) the individual consents to the use or disclosure of the information;

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent –

(i) a serious and imminent threat to the individual's or another individual's life, health or safety; or

(ii) a serious threat to public health or public safety;

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(f) the use or disclosure is required or authorised by law;

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;

(ii) enforcing a law relating to the confiscation of proceeds of crime;

(iii) protecting public revenue;

(iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;

(v) preparing for or conducting proceedings before a court or tribunal or implementing the orders of a court or tribunal;

(h) the Australian Security Intelligence Organisation ("ASIO") has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIO authorised by the Director-General of ASIO to receive the information and an officer or employee of ASIO authorised by the Director-General of ASIO to do so has certified in writing that the information is required in connection with the performance of the functions of ASIO;

(i) the Australian Secret Intelligence Service ("ASIS") has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIS authorised by the Director-General of ASIS to receive the information and an officer or employee of ASIS authorised by the Director-General of ASIS to do so has certified in writing that the information is required in connection with the performance of the functions of ASIS.

Note 1: It is not intended to deter public sector organisations from lawfully co-operating with law enforcement agencies in the performance of their functions.

Note 2: IPP 2.1 does not override any existing legal obligations not to disclose personal information. IPP 2.1 does not require a public sector organisation to disclose personal information – a public sector organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: A public sector organisation is also liable to the requirements of IPP 9 if it transfers personal information to a person outside the Territory.

2.2 If a public sector organisation uses or discloses personal information under IPP 2.1(g), the organisation must make a written note of the use or disclosure.

IPP 3 Data quality

3.1 A public sector organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

IPP 4 Data security

4.1 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.

4.2 A public sector organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

IPP 5 Openness

5.1 A public sector organisation must make available to the public a document in which it clearly expresses its policies for the management of personal information that it holds.

5.2 On the request of an individual, a public sector organisation must take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.

IPP 6 Access and correction

6.1 If an individual requests a public sector organisation holding personal information about the individual for access to the personal information, the organisation must provide the individual with access to the information except to the extent that –

(a) providing access would pose a serious threat to the life or health of the individual or another individual;

(b) providing access would prejudice measures for the protection of the health or safety of the public;

(c) providing access would unreasonably interfere with the privacy of another individual;

(d) the request for access is frivolous or vexatious;

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery or subpoena in those proceedings;

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way that would prejudice the negotiations;

(g) providing access would be unlawful;

(h) denying access is required or authorised by law;

(i) providing access would be likely to prejudice an investigation of possible unlawful activity;

(j) providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
(ii) enforcing a law relating to the confiscation of proceeds of crime;
(iii) protecting public revenue;
(iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
(v) preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or

(k) providing access would prejudice –
(i) the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or
(ii) the maintenance of law and order in the Territory.

6.2 However, where providing access under IPP 6.1 would reveal evaluative information generated within a public sector organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

6.3 If a public sector organisation holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.4 If –

(a) an individual and a public sector organisation disagree about whether personal information about the individual held by the organisation is accurate, complete or up to date; and

(b) the individual requests the organisation to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date,

the organisation must take reasonable steps to comply with that request.

6.5 A public sector organisation must provide reasons for refusing to provide access to or correct personal information.

6.6 If a public sector organisation charges a fee for providing access to personal information, the fee is not to be excessive.

6.7 If an individual requests a public sector organisation for access to or to correct personal information held by the organisation, the organisation must –

(a) provide access or reasons for refusing access;

(b) make the correction or provide reasons for refusing to make it; or

(c) provide reasons for the delay in responding to the request,

within a reasonable time.

IPP 7 Identifiers

7.1 A public sector organisation must not assign unique identifiers to individuals unless it is necessary to enable the organisation to perform its functions efficiently.

7.2 A public sector organisation must not adopt a unique identifier of an individual that has been assigned by another public sector organisation unless –

(a) it is necessary to enable the organisation to perform its functions efficiently;

(b) it has obtained the consent of the individual to do so; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contract service provider in the performance of its obligations to the outsourcing organisation under a service contract.

7.3 A public sector organisation must not use or disclose a unique identifier assigned to an individual by another public sector organisation unless –

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to that other organisation;

(b) IPP 2.1(d), (e), (f) or (g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 A public sector organisation must not require an individual to provide a unique identifier in order to obtain a service unless its provision –

(a) is required or authorised by law; or

(b) is in connection with the purpose for which the unique identifier was assigned or for a directly related purpose.

IPP 8 Anonymity

8.1 A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.

IPP 9 Transborder data flows

9.1 A public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the Territory unless –

(a) the transfer is required or authorised under a law of the Territory or the Commonwealth;

(b) the organisation reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to these IPPs;

(c) the individual consents to the transfer;

(d) the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request;

(e) the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual;

(f) all of the following apply:

(i) the transfer is for the benefit of the individual;
(ii) it is impracticable to obtain the consent of the individual to the transfer;
(iii) it is likely that the individual would consent to the transfer;

or

(g) the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred in a manner that is inconsistent with these IPPs.

IPP 10 Sensitive information

10.1 A public sector organisation must not collect sensitive information about an individual unless –

(a) the individual consents to the collection;

(b) the organisation is required by law to collect the information;

(c) the individual is –

(i) physically or legally incapable of giving consent to the collection; or
(ii) physically unable to communicate his or her consent to the collection,

and collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or

(d) collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

10.2 Despite IPP 10.1, a public sector organisation may collect sensitive information about an individual if –

(a) the collection –

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
(ii) is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services;

(b) there is no other reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.