NATIONAL BLOOD AUTHORITY
AUSTRALIA

NATIONAL BLOOD AUTHORITY DATA AND INFORMATION GOVERNANCE FRAMEWORK

VERSION 5.0

MARCH 2015

REVIEW

This document is endorsed by the Jurisdictional Blood Committee (JBC) as at 6 March 2015 as an overarching document, subject to jurisdictional bilateral data sharing agreements being completed. It is an evolving and living document that will be reviewed, as part of the ongoing better practice, every two years, or when there are material changes either to the data governance under the National Blood arrangements or to laws that impact on data governance. Any updated data governance document will also be endorsed by JBC.

The Australian Government may merge the functions of the National Blood Authority (NBA) and the Australian Organ and Tissue Donation and Transplantation Authority (AOTDTA) with a view to establishing a new independent authority by 1 July 2015. This document relates to the activities of the NBA and will survive any merger post 1 July 2015 for those activities in the new independent authority that relate to blood until such time as the JBC endorses any changes as a result of the merger.

Feedback as a result of this document should be emailed to Data@blood.gov.au.

VERSION CONTROL

Number	Date	Description of changes	Changed by
1.1	July 2013	First Draft	S Cochrane
1.2	September 2013	Internal revisions	S Cochrane
2.0	April 2014	JBC Proxy workshop revisions	S Cochrane
3.0	October 2014	JBC Proxy revisions	S Cochrane
4.0	February 2015	JBC Proxy/Members revisions	S Cochrane
5.0	March 2015	JBC Members revisions	S Cochrane
5.0	June 2022	Revision to Appendix 11	S Cochrane

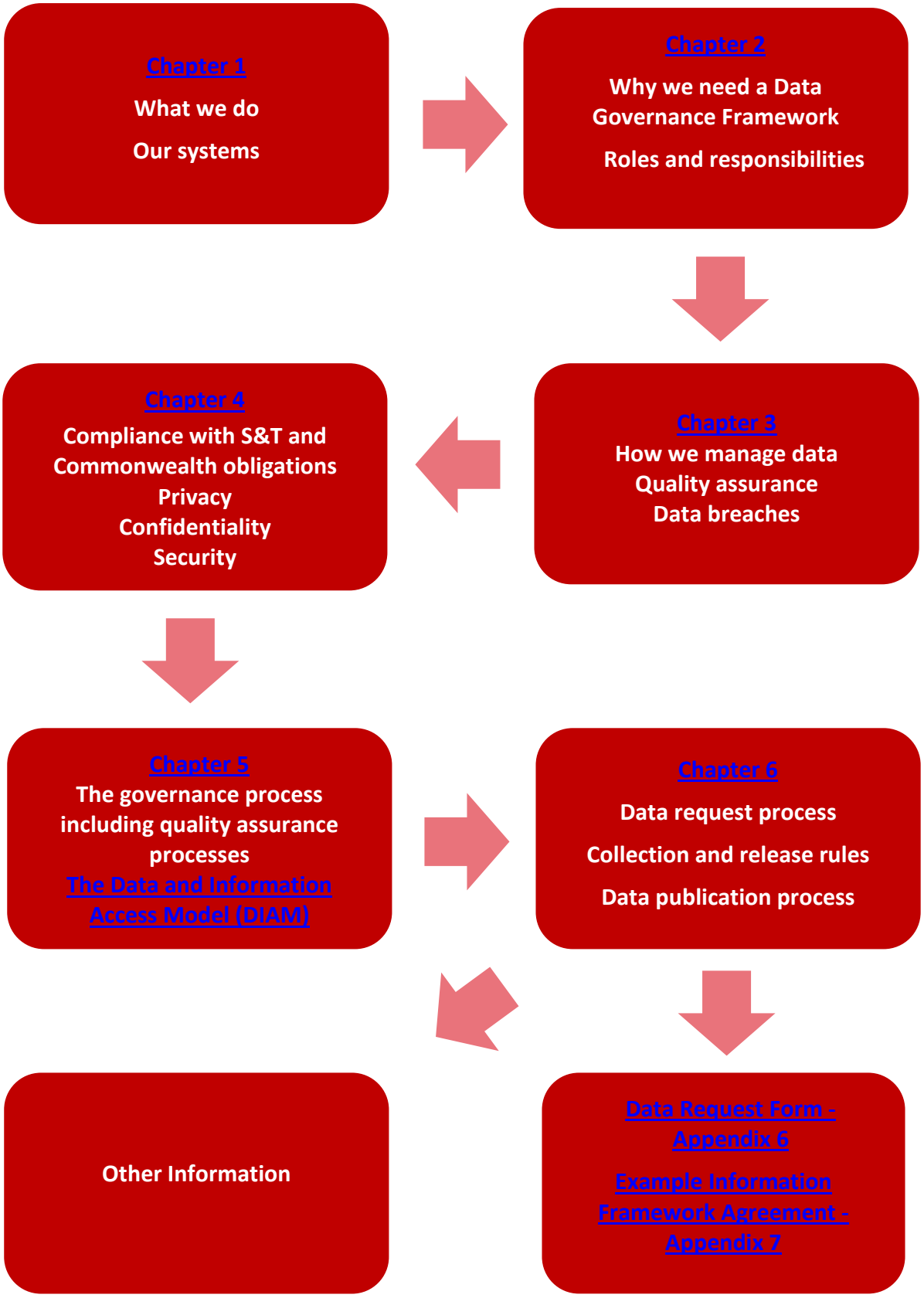
NATIONAL BLOOD AUTHORITY AUSTRALIA

LOCKED BAG 8430
CANBERRA ACT 2601
PHONE: 13 000 BLOOD (13 000 25663)
EMAIL: DATA@BLOOD.GOV.AU

CONTENTS

TABLES AND FIGURES

Structure of the Document



1. Introduction

BACKGROUND

NATIONAL BLOOD ARRANGEMENTS

The primary objectives of Australian Governments under the national blood arrangements established by the National Blood Agreement are:

- to provide an adequate, safe, secure and affordable supply of blood products, blood related products and blood related services in Australia; and
- to promote safe, high quality management and use of blood products, blood related products and blood related services in Australia.

In furtherance of these objectives, the *National Blood Authority Act 2003* provides for the National Blood Authority (NBA) "*to liaise with, and gather information from, governments, suppliers and others about matters relating to blood products and services",* and to provide information, advice and assistance to various stakeholders under the national blood arrangements.

More specifically, the National Blood Agreement provides for the NBA to perform the following activities and to facilitate coordination and information exchange with relevant stakeholders:

- promote optimal safety and quality in the supply, management and use of products, including through uniform national standards
- make best use of available resources, and to give financial and performance accountability for the use of resources by all entities involved in the Australian blood sector
- undertake national information gathering, monitoring of new developments, reporting and research in relation to the Australian blood sector
- undertake or facilitate national information management, benchmarking and cost and performance evaluation for the national blood supply
- facilitate the development of national information systems for safety and quality issues in relation to the Australian blood sector.

JBC STRATEGIC PRIORITIES

Under the national blood arrangements, all Australian governments have approved the *Jurisdictional Blood Committee (JBC) Strategic Plan 2013-15*, including the goal and strategic priorities relating to blood sector data set out in Table 1.

TABLE 1: JBC STRATEGIC PLAN GOAL 2

Goal 2 - Drive performance improvement in the Australian blood sector through a national information management and data analysis capability

Strategic Priority	Description of activities	2012-13	2013-14	2014-15
2.1 Support the development and implementation of national systems for data collection.	Advocate and support provision of data by public and private sectors through BloodNet and other national systems. Consider the need to extend development of data collection capability on non-fresh blood products including Intravenous Immunoglobulin (IVIg). Continue to support exploration of Laboratory Information System (LIS) interfaces to BloodNet.			
2.2 Improve our evidence base to better understand blood and blood product management and use and identify opportunities for improvement.	Support finalisation of a national data strategy for the blood sector as the basis for ongoing data analysis and feedback to JBC. Review the National Information and Data Strategy for approval. Facilitate development of governance arrangements for analysis and publication of data.			

NBA STRATEGIES

In accordance with the JBC Strategic Plan, the NBA has framed the *National Blood Sector Data and Information Strategy and Scorecard 2013-2016* (Sector Data Strategy) which was endorsed by JBC in March 2013. As part of this strategy the development and implementation of the data governance framework is integral to the work of the NBA. The Sector Data Strategy defines the following five Data Strategic Priorities together with relevant desired outcomes and key strategies:

1. Establish an overall architecture for data collection and information flows and relationships
2. Define governance principles for the collection and management of data and information
3. Promote a standardised approach to data sets and system capabilities
4. Prioritise data collection and system development required for the sector
5. Drive sector improvement with data analyses and production

In addition to the Sector Data Strategy, the JBC has endorsed a number of other key strategy documents for blood sector improvement, including:

- National Blood Sector ICT Strategy 2013-2016
- National Patient Blood Management Guidelines Implementation Strategy 2013-2017
- National Blood and Blood Product Wastage Reduction Strategy 2013-17
- National Blood Research and Development Strategic Priorities 2013-16
- National Blood Sector Education and Training Strategy 2013-16

OVERVIEW OF BLOOD SECTOR DATA SYSTEMS AND SOURCES

A significant amount of data exists within the blood sector, however, the extent to which this data is currently available to the stakeholders that need it, the quality of the data, and the capacity of the systems that hold it, varies widely. As is illustrated in Table 2, the majority of data is held either in suppliers systems

or hospital systems. The differences in systems have arisen because they were specifically developed for other purposes then modified for new uses over time.

In general, information within a supplier's systems is (relatively) easily accessible – the systems are typically electronic and core to the supplier's business. Information from hospital systems is much less accessible and in some cases, is not in an electronic form (eg some patient notes) and is therefore extremely difficult to access. In addition, there is limited standardisation of what information is captured, how it is defined, stored and accessed, and limited standardisation of the hospital systems themselves. Jurisdictional arrangements also vary significantly, although some jurisdictions are moving towards standardised state wide systems.

In addition to the existing systems within the sector, there are a number of national systems rolled out to health providers (BloodNet and ABDR) which are likely to positively impact data availability. Their use and the data they capture are also shown in Table 2.

TABLE 2: SECTOR SYSTEMS AND SOURCES

Blood product supply chain activities	Fresh Blood Products	Clotting Factor Products	Immunoglobulin	Other Products
Donor management	eProgesa (Supplier system)			
Quality and manufacturing	eProgesa (Supplier system)	Supplier systems	Supplier systems	Supplier systems
Supplier inventory	eProgesa (Supplier system)	Supplier systems	Supplier systems	Supplier systems
Supplier wastage	eProgesa (Supplier system)	Supplier systems	Supplier systems	Supplier systems
Order by health provider	BloodNet or Hospital/ laboratory systems	Australian Bleeding Disorders Registry (ABDR)	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems
Authorisation details	STARS (Supplier system)	ABDR	STARS (Supplier system)	Supplier systems
Issued to health provider	BloodNet or Hospital/ laboratory systems	BloodNet/ABDR or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems
Receipted by health provider	BloodNet or Hospital/ laboratory systems	BloodNet/ABDR or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems
Inventory by health provider	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems
Wastage (fate of product)	BloodNet or Hospital/ laboratory systems	ABDR/ Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems	BloodNet or Hospital/ laboratory systems
Issued to patient	Hospital systems (patient records and notes and laboratory systems)	ABDR/ Hospital/ laboratory systems	Hospital systems (patient records and notes)	Hospital systems (patient records and notes)

Blood product supply chain activities	Fresh Blood Products	Clotting Factor Products	Immunoglobulin	Other Products
Prescription/ Informed Consent	Hospital systems (patient records and notes and laboratory systems)	ABDR/ Hospital/ laboratory systems	Hospital systems (patient records and notes)	Hospital systems (patient records and notes)
Reason for use	Hospital systems (patient records and notes and laboratory systems), general practitioner/ specialist systems	ABDR/ Hospital/ laboratory systems	Hospital systems (patient records and notes), general practitioner/ specialist systems	Hospital systems (patient records and notes), general practitioner/ specialist systems
Outcome of treatment	Hospital systems (patient records, notes, laboratory systems, adverse events and mortality data), general practitioner/ specialist systems	ABDR/ Hospital/ laboratory systems	Hospital systems (patient records, notes, adverse events and mortality data), general practitioner/ specialist systems	Hospital systems (patient records, notes, adverse events and mortality data), general practitioner/ specialist systems
Reporting (operational and performance)	NBA internal system – BigRed	NBA internal system – BigRed	NBA internal system – BigRed	NBA internal system – BigRed
Audit/Quality improvement	Ad hoc	Ad hoc	Ad hoc	Ad hoc
Payments and contract performance	NBA internal system - IDMS	NBA internal system - IDMS	NBA internal system - IDMS	NBA internal system - IDMS
Supply plan performance	NBA internal system - IDMS	NBA internal system - IDMS	NBA internal system - IDMS	NBA internal system - IDMS

2. Purpose and Scope

PURPOSE

The purpose of this document is to define the NBA's governance principles and arrangements for the NBA's own management of data and information, and for the NBA's dealings with data stakeholders in the blood sector.

In general these governance arrangements are relevant to blood sector data and information that is, or may usefully be, collected, analysed, reported, published and managed systematically and held by the NBA in some form of database, data linkage collection or other structured data sets. It does not preclude governance policies within jurisdictions or organisations for data that is not managed or held by the NBA.

SCOPE

The Sector Data Strategy defines the following scope for the development of data and information governance principles:

Data governance refers to the overall management of the availability, usability, integrity, and security of data. A sound data governance arrangement must be comprehensive and include a governing body, a defined set of procedures, and a plan to execute those procedures. Governance arrangements should exist at all levels within the sector and organisations will be able to demonstrate their compliance against all required standards, regulations and community expectations.

The governance framework for data collection and management at the national level needs to be able to guarantee and demonstrate:

- data is collected and used to meet business, operational or legislative requirements or there is a strategic need for the data
- data will be shared and managed as an asset under documented governance processes (including ethics approval processes)
- data and information will be released under written agreements to ensure compliance with privacy and other regulations
- data and information will be delivered to allow access, release and control
- the data collection is used for reporting at a state level, national level or external to the health service where the data collection resides
- data and information management will be auditable and ensure accountability
- data and information roles and responsibilities will be defined and published
- data will be supported by data dictionaries and metadata and will ensure a high quality data standard with a master data set
- obligations and expectations for data reporting to external stakeholders are managed
- processes are in place to identify and manage breaches of data privacy and confidentiality.

DATA PURPOSE AND USE

Data will be collected and used by the NBA for the following purposes:

- supply and demand planning, supply and contract management, funding and expenditure of the supply of blood and blood products under the national blood arrangements
- requests for access to blood products, where specific eligibility criteria apply, such as Immunoglobulin (IVIg, SCIg, NHIg)

- fate, including use, transfer and discard of blood products
- order, delivery and receipt fulfilment
- clinical use of blood products, transfusions, outcomes and adverse events
- quality or performance improvement processes
- research and development.

Within this scope, some data may be of a business or administrative nature collected for day to day operational purposes with no detail relating to individual patients or clinicians, while other data may contain sensitive personal details relating to clinical management of patients, or be collected with a high degree of accuracy to support robust data analysis. The appropriate level and approach for data governance and management will depend on the nature, context and purpose of the data (refer to the Data and Information Access Model (DIAM)).

DATA ROLES AND RESPONSIBILITIES IN THE NBA

Within the NBA there are a number of roles that have responsibility for the data published and collected and these are described in Table 3.

TABLE 3: DATA ROLES AND RESPONSIBILITIES

Data Role	Data responsibilities
Data Executive – The General Manager	The position which has management of and ultimate responsibility for the data held by the NBA, including the authority to grant access to data and the business rules in accordance with the DIAM. Also has responsibility for setting the overall strategic direction of the specific data collection to ensure the collection is developed, maintained and utilised in accordance with the strategic goals of the NBA.
System Owner – The Chief Information Officer (CIO)	Responsible for the safe custody, transport and storage of data, the content, context and system rules. This usually includes the daily and routine care-taking of all aspects of data systems.
Data Steward – Various (CIO, the Blood Information Governance Group (BIGG), Australian Bleeding Disorders Registry (ABDR) Steering Committee, Executive Director – Fresh, Data and Clinical Development)	Responsible for implementing the agreed strategic direction of the specific data collections as defined by the Data Executive, to ensure the collection is developed, maintained and utilised in accordance with the strategic goals of the NBA. Also responsible for: • The development and implementation of the business rules and adherence to this document. • Maintaining the access, use and disclosure of data from the data collection for clearly defined purposes that comply with obligations in accordance with the DIAM.
Data Custodian – Various (CIO, Executive Director – Fresh, Data and Clinical Development)	Primarily responsible for: • Identifying and acquiring new data collections • Creating and maintaining consistent reference data and master data definitions • Publishing relevant data to appropriate users in accordance with the DIAM • Creating and managing business metadata for published data sources • Resolving data integrity issues across stakeholders • Analysing data for quality and reconciling data issues.

NBA DATA SYSTEMS AND COLLECTIONS

The NBA operates a range of Information and Communications Technology (ICT) systems and collections. The systems described in Table 4 enable the NBA to provide a safe secure and affordable blood supply for all Australians. The custodian and steward for each system are noted.

TABLE 4: NBA DATA SYSTEMS AND COLLECTIONS

System or Collection	Description	Data Steward	Data Custodian
BloodNet	BloodNet	Chief Information Officer	BIGG
BloodPortal	BloodPortal	Chief Information Officer	BIGG
BloodChat	BloodChat	Chief Information Officer	BIGG
BloodDocs	BloodDocs	General Manager	Chief Information Officer
Jurisdictional Reports	Jurisdictional Reporting	Chief Information Officer	BIGG
Australian Bleeding Disorders Registry	Australian Bleeding Disorders Registry	Chief Information Officer	ABDR Steering Committee with the assistance of BIGG
MyABDR	MyABDR	Chief Information Officer	ABDR Steering Committee with the assistance of BIGG
Integrated Data Management System (IDMS)	Used by the NBA to manage the budgeting and forecasting of supply and demand for blood and blood products, inventory management and contract administration.	Chief Information Officer	BIGG
BigRed (Reporting)	BigRed	Chief Information Officer	BIGG
National Haemovigilance Data Collections	Haemovigilance Reporting	General Manager	Executive Director – Fresh, Data and Clinical Development
IVIg STARS Extract	Information is also sourced from the Australian Red Cross Blood Service (Blood Service) STARS database which is maintained by the Blood Service on behalf of all Australian governments in its role as contracted gatekeeper and distributer of IVIg products.	Executive Director – Fresh, Data and Clinical Development	BIGG

The terms and conditions for use of NBA systems will provide relevant privacy and confidentiality provisions, how consent works with the data we collect and how the NBA will use data collected at an aggregate level. By agreeing to the terms and conditions, users are not agreeing to the disclosure of information entered into the system at health provider level. For further information on the requirements refer to the DIAM. Each user of NBA systems will be required to agree with the terms and conditions prior to receiving access and may from time to time be requested to agree with updated/revised terms and conditions of use.

DATA STAKEHOLDER ROLES

The stakeholders that may be relevant within these governance arrangements and their associated roles are outlined in Table 5.

TABLE 5: STAKEHOLDER ROLES

Stakeholders	Data roles
NBA	• Implements and maintains governance framework • Coordinates capture and sharing of data sets in accordance with the DIAM • Custodian of data and information collected directly • Custodian of composite data and information provided by jurisdictions, but held by the NBA • Requests data from various sources • Provides data to various parties • Receives data from various sources • Approves data requests and collections in accordance with the DIAM • Ensures quality assurance processes over data held are undertaken • Ensures compliance requirements are met
State and territory health departments	• Request data from the NBA • Provide data to the NBA • Receive data provided by the NBA in accordance with the DIAM • Approve data requests in accordance with the DIAM • Provide input into governance structures • Data custodians of information provided by jurisdictions to the NBA
Department of Health	• Requests data from the NBA • Provides data to the NBA • Receives data provided by the NBA in accordance with the DIAM • Provides input into governance structures
Health providers (eg hospitals, pathology labs, pharmacies)	• Provide data to the NBA (data input) • Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM
Suppliers/contractors (Blood Service, other suppliers)	• Provide data to the NBA (data input) • Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM
Researchers	• Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM • Provide data to the NBA (data collections)
Clinicians	• Provide data to the NBA (data input) • Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM
ABDR Steering Committee	• Approves data requests in accordance with the DIAM • Provides input into governance structures
Blood Information Governance Group (NBA Committee)	• Reviews data requests (collection and release) • Approves data requests (collection and release) as per the DIAM
JBC and other internal committees	• Receive data for decision making in accordance with the DIAM • Approve governance structures • May approve data requests in accordance with the DIAM • Provide input into governance structures

Stakeholders	Data roles
Colleges and societies	• Provide data to the NBA • Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM
Minister and ministerial councils (COAG Health Council, AHMAC, HPC)	• Receive data for decision making in accordance with the DIAM • Request data from the NBA
Ethics Committees	• Review data collections and use for research and record data • Provide approval for research and record collections and use
National Health Bodies such as AIHW, NEHTA	• Provide data to the NBA • Request data from the NBA • Receive data provided by the NBA in accordance with the DIAM
Other (includes patient organisations and individuals)	• Benefit from the availability and use of well governed, accurate and timely data • Request data from the NBA • Provide data to the NBA within the applicable consent regime • Receive data provided by the NBA

3. Effective Governance

HOW WE MANAGE DATA

The NBA manages data and information it collects and/or distributes to other stakeholders by:

- establishing robust governance arrangements around the collection, storage and management of data from suppliers and other stakeholders and release of information for regular and ad-hoc reporting
- setting criteria for the distribution of standardised data sets (including metadata and definitions) that are published on the NBA website for access by all stakeholders
- setting criteria for distribution of regular and ad-hoc data in response to requests from stakeholders.

In February 2007, the JBC endorsed a set of data principles for sector data development. In 2010 the JBC noted these principles would guide the implementation of The National Blood Sector Data and Information Strategy and Scorecard. The principles are presented at Appendix 1 and have been used in establishing the rules in this document.

Adherence to policies, protocols and procedures for the management of shared national data and information requirements is the responsibility of the NBA General Manager and is overseen by the internal governance group called the Blood Information Governance Group (BIGG). The BIGG guides the development and revisions to NBA's policies, protocols and procedures, in conjunction with other stakeholders, such as JBC, to:

- oversee and contribute to the Governance Framework
- contribute to the strategic priorities from the Sector Data Strategy
- approve data and information for publication
- set and endorse the schedule of data publications
- review and approve data collection activities
- review and approve stakeholder data requests in accordance with the DIAM
- oversee access to relevant expertise and analysis of data and trends
- maintain a register of data and information requests which identifies ad hoc, recurring and research requests.

The role of the BIGG is to define, apply and oversee the specific requirements and processes for governance and management of data in accordance with this Governance Framework. In doing so, the BIGG ensures that appropriate governance and management is applied, given the nature, context and purpose of the relevant data activity. For example, where data is sensitive due to privacy, confidentiality or stakeholder legislation and concerns, or where a high degree of quality assurance is appropriate, the BIGG ensures a high level of control and scrutiny is applied. The same high level of management may not, however, be required for less sensitive administrative data used for day to day business purposes, and this may be managed directly by other NBA business teams. The BIGG terms of reference are at Appendix 2.

In considering data requests and publication the BIGG will take into account jurisdictional requirements and obligations either through consulting with jurisdictions or through consideration of the restrictions in the information framework agreements or other relevant agreements.

Underpinning these specific functions are a number of internal policies which the NBA also adheres to. These include:

ICT Conditions of Use Policy	Internal document
ICT Change Management Policy	Internal document
Records Management Policy	Internal document
Protective Security Policy	Internal document
Privacy policy	Privacy Link
Information Publication Scheme Agency Plan	IPS Link
Intellectual Property policy	Internal document
Copyright Policy	Internal document
FOI process	FOI Link
Conflict of Interest	Internal document and Employment Link
Public Interest Disclosure Scheme	Public Interest Disclosure Scheme Link

QUALITY ASSURANCE

Effective quality assurance arrangements are a key element in data governance arrangements. The delivery of data and information for blood sector stakeholders will be based on the nature, context and purpose of the data and assessed as part of the overall prioritisation and decision making ensuring they are reliable in both findings and analysis practices. These practices are based on the most appropriate validated base information and data. The management of data and information will seek to adhere to two key quality assurance management principles:

- the data and information should be suitable for the intended purpose
- the data and information provided should be right the first time within agreed quality criteria.

All data requests will be assessed to ensure they meet the quality assurance principles for those that are collected and released. The data request form will be used for both stakeholders requesting data from the NBA and for the NBA requesting data from stakeholders. A quality assurance statement will be endorsed by the NBA and stakeholders prior to the data being released or through the information framework agreements or other relevant agreements.

Refer to the Quality Assurance Process and the Data Request Process for how each data request will be assessed and how data quality monitoring is conducted.

IDENTIFICATION RISKS IN AGGREGATE DATA

In order to maintain the anonymity of individual patients and health providers, small cell data published or released, showing less than five (5) may be suppressed or aggregated unless exceptions are agreed between national and state/territory data custodians.[1]

RISK MANAGEMENT

The NBA will manage risk by ensuring decisions:

- accord with statutory requirements and are consistent with Australian Public Service Values and Code of Conduct
- are in accordance with the *National Blood Authority Act 2003* and the National Blood Agreement
- are in accordance with directions provided by the JBC
- are in accordance with the objectives and policies of the NBA

[1] National Statistical Service, Statistical Data Integration – Primary and Subsequent Suppression

- take account of the constraints imposed and the external environment, and
- are accountable and withstand external scrutiny.

It is the responsibility of the all NBA staff to ensure the principles of risk management are applied in accordance with the NBA Risk Management Key Business Process. The NBA framework is based on the *Australian/New Zealand Standard AS/NZS ISO 31000:2009 – Risk management – Principles and guidelines.* Risk relating to the capture, storage and disposal of information will be documented by the Data Steward and approved by the Data Executive and retained in accordance with the NBA Records Management Policy. A review of all risks is conducted every year to ensure currency and relevance. It is the responsibility of the Data Steward to manage risk relating to the capture, storage and disposal of information.

All NBA external data collection requests, data publications and data requests will be assessed under the NBA Risk Framework and provided for each event as part of the documentation materials for quality assurance.

ETHICS

When considering the ethical acceptability of activities involving information which could identify a person or cause harm to individuals ('identifiable data') the NBA will seek ethics reviews for:

- new data collections of record[2] data or to change the scope of content of existing collections
- new linked datasets
- linked datasets for the purposes of analysis
- access to identifiable or re-identifiable data held by the NBA which external researchers wish to link with research data.

The NBA must be satisfied that the public interest in the research activity outweighs to a substantial degree the public interest in privacy. To ensure this, the NBA will seek ethics considerations in accordance with *The National Statement on Ethical Conduct in Human Research (2007)* which sets out values and principles that apply to all human research and to the definitions of research and consent needed.

If the NBA considers the data request requires ethics committee expertise (in accordance with the DIAM) then the matter will be referred to a National Health and Medical Research Council (NHMRC) compliant ethics committee in each jurisdiction to give the approval as defined in the DIAM.

The NBA will also consider jurisdictional requirements through jurisdictional involvement in decisions or include an assessment of the information framework agreements or obligations in other relevant agreements. Any new linkage of datasets involving jurisdictional data requires approval from the jurisdiction depending on the linkage and data collection and may be conditional upon ethical approvals.

PROBITY AND CONFLICTS OF INTEREST

Probity is the evidence of ethical behaviour in a particular process. Probity is defined as complete and confirmed integrity, uprightness and honesty. Probity should be integrated into all ethical considerations, and should not be a separate consideration. This data governance framework sets out the expectations of the NBA with regard to probity in dealing with data.

Ethics must be conducted with probity in mind to enable researchers and users to deal with each other on the basis of mutual trust and respect. Adopting an ethical, transparent approach enables business to be conducted fairly, reasonably and with integrity.

The probity process should seek to ensure the integrity of the data collection and release is safeguarded through a series of activities designed to progressively and thoroughly assess the level of exposure of the NBA to challenge or process compromise.

[2] Refer to Glossary of Terms for definition

The typical approach should ensure that:

- all persons are given equal access to information and responses, and that procedures are correctly followed
- the procedures are conducted in a fair and unbiased manner, with no party unfairly discriminated against or given advantage over another
- staff provide a recommendation consistent with the evaluation process
- the approval is consistent with the process and with probity principles
- the data and information team provides a regular report to the NBA Executive confirming the extent of compliance with these probity requirements.

Current NBA policy on probity matters is that:

- probity is a core competency for NBA staff
- probity is the collective responsibility of the data and information team and the executive
- generally NBA will not use external consultants or audits for probity assurance.

NBA staff should also note the other legislative requirements in relation to probity and ethics, for example the requirements of the APS Values and Code of Conduct.

Conflicts of interest may arise in the course of business operations. Possible conflicts are varied but include pecuniary interests, legal interests, associations with external organisations and non-direct personal interests. In carrying out one's duties, officials must not allow themselves to be improperly influenced by family, personal or business relationships. NBA staff are required to declare and manage potential conflicts of interest. This extends to any potential conflict of interest in relation to dealing with specific data sets.

NBA policy is that all NBA staff should be asked to complete an annual standard conflict of interest disclosure.

DATA BREACH AND RESPONSE

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse
- malicious actions, such as theft or 'hacking'
- internal errors or failure to follow information handling policies that cause accidental loss or disclosure
- not adhering to the laws of the states and territories or the Commonwealth of Australia.

Reporting of all data breaches will be in accordance with the Commonwealth Protective Security Policy Framework (PSPF), the Australian Government information security management protocol and the NBA Protective Security Policy in relation to the requirements for reporting data breaches. Breaches that present a greater risk (such as a risk posed where personal information of a larger number of people is involved, where the event was systemic or intentional) will be additionally reported to the Australian Privacy Commissioner and the affected individual(s) in accordance with the *Freedom of Information Act 1982* and amendments.

Where stakeholders have been provided with data from the NBA they are required to sign the conditions of data release section of the data request form, and in so doing commit to storing and using the data in accordance with the obligations outlined. If it becomes known to the NBA that these conditions have been breached then the NBA will follow the process below.

HOW TO NOTIFY A DATA OR INFORMATION BREACH

The NBA will follow the process set out below and in Figure 1 if there is a data breach relating to personal information[3] for patients, clinicians, health providers or jurisdictions.

DATA BREACH CHECKLIST

1. Where NBA staff become aware that there has been a data breach, they will notify their manager who will assess the risk, document the event and report in the first instance to the BIGG Chair.
   Where an external party becomes aware of a data breach, they shall notify the NBA by email at support@blood.gov.au or call 13 000 BLOOD (13 000 25663) or for international calls: +61 2 6151 5000. The BIGG Chair will be advisedof the incident for action and rectification.
2. The NBA will maintain a register that will contain:
   - a brief description of the nature of the breach, how it occurred, the date of the breach, the date of discovery and the date of notification to the NBA (for an external breach)
   - a description of the types of unsecured protected health information that were involved
   - information about remediation steps undertaken and any improvement processes to be implemented
   - actions to rectify the data breach, if possible.
3. The NBA will notify the jurisdiction/stakeholder which supplied the data, if the data is identifiable at a health provider or lower level. Each state and territory will have its own process that must be adhered to and the NBA will provide assistance and support in completing these processes.
4. The BIGG Chair will carry out the following process[4]:

   Step 1: Contain the breach and make a preliminary assessment
   - Convene a meeting of the BIGG.
   - Immediately contain breach:
     - IT to implement response process if necessary.
     - building security to be alerted if necessary.
   - Inform the NBA Executive, and the Australian Privacy Commissioner if necessary; provide ongoing updates on key developments.
   - Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the NBA to take appropriate corrective action.
   - Consider developing a communications or media strategy to manage public expectations and media interest.

   Step 2: Evaluate the risks associated with the breach
   - Conduct initial investigation, and collect information about the breach promptly, including:
     - the date, time, duration, and location of the breach
     - the type of personal information involved in the breach
     - how the breach was discovered and by whom
     - the cause and extent of the breach
     - a list of the affected individuals, or possible affected individuals
     - the risk of serious harm to the affected individuals
     - the risk of other harms.
   - Determine whether the context of the information is important.
   - Establish the cause and extent of the breach.
   - Assess priorities and risks based on what is known.
   - Keep appropriate records of the suspected breach and actions of the BIGG, including the steps taken to rectify the situation and the decisions made.

[3] Refer to Glossary of Terms for definition
[4] From OAIC process

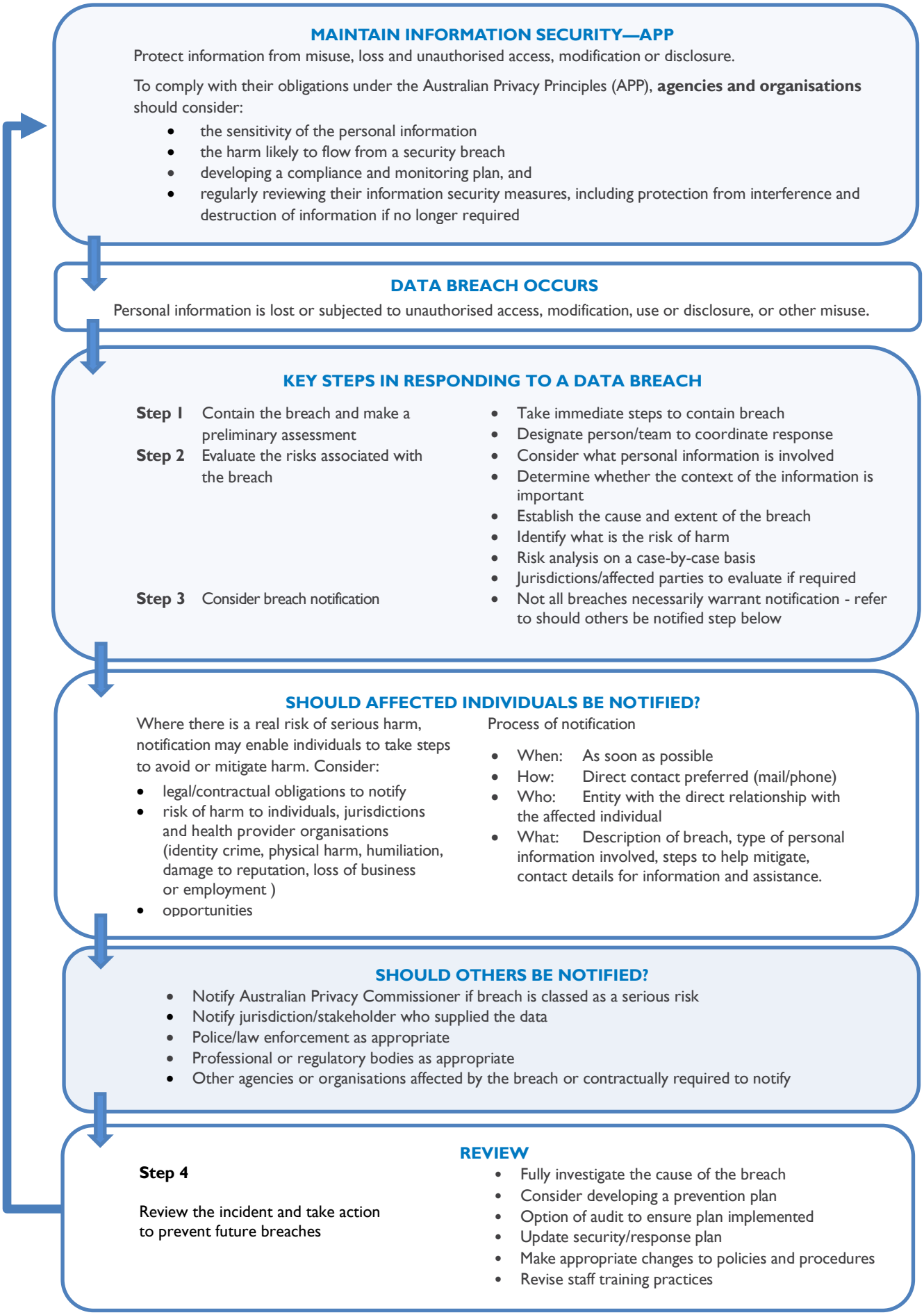
Step 3: Consider breach notification

- Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
- Determine whether to notify affected individuals — is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately (eg where there is a high level of risk of serious harm to affected individuals).
- Consider whether others should be notified, including police/law enforcement, other agencies or organisations affected by the breach, or where the NBA is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

Step 4: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Report to NBA Executive on outcomes and recommendations:
    - Update security plan if necessary
    - Make appropriate changes to policies and procedures if necessary
    - Revise staff training practices if necessary
    - Consider the option of an audit to ensure necessary outcomes are effected.

FIGURE 1: DATA BREACH RESPONSE PROCESS



4. Privacy, Security and Compliance

COMMONWEALTH COMPLIANCE REQUIREMENTS

The NBA operates within a governance and accountability framework established under legislation which requires it to:

- meet the specific accountability and other requirements of the *National Blood Authority Act 2003* (Cth) and the Australian Government Financial Management Framework including the *Public Governance, Performance and Accountability (PGPA) Act 2013* (Cth), PGPA Rule 2014, Commonwealth Procurement Rules and other Australian Government policies;
- ensure openness and transparency through public reporting processes
- allow for external scrutiny, for example by the Auditor-General (*Auditor-General Act 1997* (Cth)) and the Ombudsman (*Ombudsman Act 1976* (Cth))
- collect, store, protect, use and disclose personal information (including sensitive information) in line with the *Privacy Act 1988* (Cth)
- comply with known duties of confidentiality that apply to stakeholders that provide the NBA with personal information about themselves or about a third party (e.g. doctor-patient confidentiality)
- comply with Australian Government Protective Security Policy Framework, the Australian Government information security management protocol
- create, capture, secure, manage, transfer and destroy Commonwealth records in accordance with the *Archives Act 1983* (Cth)
- provide information on behalf of Ministers to the Parliament of Australia, acting through its various committees.

The NBA is also required to promote disclosure of government held information as a national resource in line with the *Freedom of Information Act 1982* (Cth). The FOI Act provides a legally enforceable right of access to a document of an agency. Unless a document is subject to an exemption in the FOI Act the NBA is obliged to disclose it to a requesting party. Refer to the FOI page on the NBA website for how the NBA deals with FOI requests.

Separate contractual arrangements for data and information have been set up with suppliers and vendors and these will be managed by the NBA in accordance with the Commonwealth policies. Third parties requesting and receiving data and information from the NBA will be required to comply with state and territory and Commonwealth obligations and will be addressed on a case by case basis depending on the data requested and the different obligations.

COOPERATION WITH STATE AND TERRITORY STAKEHOLDERS

In general, the NBA, on behalf of all Governments and in accordance with the objectives of the National Blood Agreement is the steward, custodian and manager of data once it is entered into NBA systems (e.g. BloodNet). It is important to note, however, that the NBA has a legal obligation (over and above general privacy requirements) to comply with confidentiality obligations of stakeholders who enter data into NBA systems. At a minimum, governance arrangements for NBA systems must take account of those legal obligations. Data that is supplied from stakeholders to the NBA (or vice versa) outside of these standing systems (e.g. data linkage data sets) is normally controlled and managed by the entity/jurisdiction that supplied the data. Where necessary, the NBA will negotiate appropriate management and licensing arrangements with individual stakeholders in order to satisfy policy, legal and business requirements for each party. For example, for state and territory Governments this will include the formulation of

information framework agreements or other relevant agreements that will set minimum requirements around data exchange and provide for the ability to impose higher standards for specific data sets when necessary. An example of one type of information framework agreement is at Appendix 7.

Governance requirements are likely to vary depending on the entity concerned, the type of data sought and the jurisdiction. Appendix 4 sets out some indicative issues and queries that the NBA will consider when making a request for data. These issues will be added to over time to develop jurisdiction specific arrangements. The jurisdiction will only provide data to the NBA where authorised or permitted by law and for clearly defined NBA purposes. In the event that the NBA wants to transfer or use that data for a purpose that has not been agreed then it will seek prior written consent of the data contributors to do so. If the NBA is legally compelled at law or contractually to provide data to a jurisdiction, it will comply.

As indicated above, the NBA is under a legal obligation to protect known obligations of confidence. This requirement is set out in Part VIII of the *Privacy Act 1988* (Cth). Part VIII extends an obligation of confidence with respect to personal information beyond the initial confidant to the NBA. This requirement will arise where the NBA knows or ought reasonably to know about that confidentiality obligation. The NBA operates on the basis that a duty of confidence exists where personal information of individuals (patients) collected by a doctor (or other confidant) is entered into an NBA system (e.g. ABDR). Hence if the NBA acts in a way that breaches the confidentiality obligation that a doctor has to his/her patient with respect to that information then the patient and the doctor may have a right to seek relief for that breach directly from the NBA.

State and territory hospitals and pathology laboratories (whether public or private) may provide data to the NBA from time to time, either directly or via state and territory governments or suppliers. This includes blood and blood products order, receipt, and use data. Ethics approval is required to obtain patient related data and for research. Ethics approval is in addition to and also complements the legal requirements that may apply including any obligation to seek consent of patients either as a result of general privacy laws or because of an existing obligation of confidence. Where record level data is sought it will be de-identified prior to receipt in accordance with jurisdictional requirements as set out in the information framework agreements or other relevant agreements. De-identification means that the data will no longer contain any personal information of individuals. Access to such data will be strictly controlled via log-in to a secure system on a strictly 'need to know' basis in accordance with the DIAM.

State and territory entities can also make requests to the NBA for data. It is expected that such requests would generally be made through the relevant government entity. However, requests may also be made by private entities or public hospitals directly. Where this occurs the NBA will contact the state or territory government to inform them of the request if the data requested is at record level or in accordance with the DIAM. The main obligations that govern the collection, storage, use and disclosure of information or material for the Commonwealth are detailed at Appendix 5. This is not intended to be an exhaustive list, but merely a guide to the types of issues that may arise for the Commonwealth when dealing with data received or created within the Agency.

COOPERATION WITH OTHER KEY STAKEHOLDERS

The NBA has certain responsibilities when collecting, storing, using or disclosing information or material provided by other key stakeholders such as the patient level data held in the Australian Bleeding Disorders Registry (ABDR) (entered directly at the treatment centre or doctor level). The NBA has, in cooperation with these stakeholders, put in place specific governance arrangements that incorporate the roles and responsibilities managed by the ABDR Steering Committee. The ABDR Steering Committee manages security and access to the ABDR so that only authorised users have access to that system. This committee is made up of representatives of the Australian Haemophilia Centre Directors' Organisation (AHCDO), the NBA, a State or Territory Government representative and the Haemophilia Foundation Australia (HFA). The Steering Committee grants access to authorised staff of the NBA, AHCDO and HFA. The governance arrangements include detail about the authorisation process, the approach to addressing privacy and confidentiality issues as well as issues around data integrity, use and disclosure of data in that system. A link to the ABDR Governance Framework is at Appendix 3.

The NBA co-ordinates requests for data, access to ICT systems and publication requirements on behalf of all Governments to meet the objectives of the National Blood Agreement whilst ensuring that the legal, policy and management requirements of the Commonwealth, state and territory Governments and other relevant stakeholders are satisfied. It is therefore essential that there is governance around data requests which takes into consideration the separate requirements, obligations and objectives of all relevant stakeholders.

PRIVACY

The NBA is required to meet the Australian Privacy Principles (APPs) in Schedule 1 of the *Privacy Act 1988* (Cth) with respect to the collection, storage, security, access, use and disclosure of personal information. Where possible, data items that could identify personal information will also be de-identified or aggregated to a level that cannot allow re-identification. For the purpose of de-identification to meet legal requirements, the NBA will aggregate data on the demographic characteristics of personal identification and service contacts provided. Where identifiable health information is collected in NBA systems this will only occur where it is reasonably necessary to or directly related to a function or activity of the agency and where express consent of the patient has been obtained. The NBA will also take into account any state or territory privacy or other requirements that apply to such data.

The ABDR is a computer database of healthcare information about people with bleeding disorders. The MyABDR app and website link directly to the ABDR and are used by patients to record home treatments and bleeds and manage treatment product stock. After receiving appropriate notification and guidance patients must expressly consent to having their health information included in the ABDR and MyABDR before they will be added to the Registry. They can withdraw that consent at any time. The ABDR Steering Committee limits access to the ABDR to make sure the data is reliable, that the ABDR is used correctly, and/or to provide reports for quality assurance and for research. The following authorised users have access to data for the purposes specified:

- Authorised NBA staff to provide technical and user support for the ABDR and MyABDR, assist in managing the integrity of the data entered into the ABDR, and extract information for approved reports and research;
- Authorised AHCDO staff to help co-ordinate data entry at HTCs, and support good healthcare practice to improve the health and wellbeing of patients;
- Authorised HFA staff to prepare reports on clotting factor product use and access in Australia and adverse event rates for international organisations such as the World Federation of Hemophilia.

Refer to http://www.blood.gov.au/abdr and http://www.blood.gov.au/myabdr for further information.

CONFIDENTIALITY

The basis for handling confidential data is that the NBA limits access to data, in accordance with the confidentiality obligations which underpin that data. Where appropriate (in line with the obligation) this includes limiting access to those who need it. Therefore staff within the NBA will only access data sets that they require in order to do their work. Permission for access to a particular system dataset is coordinated by the Chief Information Officer, delegate or if required the ABDR Steering Committee according to the DIAM. Staff who access data as part of their job function are required to have the appropriate security clearances on recruitment to the NBA and must understand any confidentiality obligations that apply to specified data sets. The NBA has obligations both in contract, equity and (where personal information is concerned) via Part VIII of the *Privacy Act 1988* (Cth) to ensure that its contractors and employees comply with these obligations. Where an obligation of confidence exists the NBA will ensure that the requirements of that obligation are considered as a minimum standard which will apply to that specific data set. This will ensure that confidentiality requirements are considered in addition (and over and above) any general privacy obligations that may ordinarily apply to the NBA.

For example, within the ABDR there are a number of governance processes that have been implemented to ensure privacy and confidentiality obligations are met, including appropriate notification and obtaining express consent of patients for the collection of their health information. The NBA will never rely on an exemption under Commonwealth privacy laws to go outside the parameters set by this closely managed collection process without assessing how this impacts on responsibilities set by confidentiality obligations and state or territory privacy requirements. This would include significant consultation with stakeholders and carefully considered legal advice.

SECURITY ARRANGEMENTS

The protective, information, personnel and physical security of all stored, transmitted or reported data, both internal and externally sourced will adhere to the requirements of the Australian Government Protective Security Policy Framework (PSPF), Australian Government information security management protocol, *Public Service Act 1999* (PS Act), *Privacy Act 1988* (Privacy Act), *Archives Act 1983* (Archives Act), *Freedom of Information Act 1982* (FOI Act), *Criminal Code Act 1995* (Criminal Code Act) and *Crimes Act 1914* (Crimes Act) and the NBA Protective Security Policy.

For all data collected through ICT systems or from other stakeholders the NBA will ensure that all data is stored on secure servers in Australia that are managed appropriately under the applicable Australian Government standards and guidelines as at Appendices 10 and 11.

The NBA requires that all data and information provided to external stakeholders will be stored and secured in accordance with the information framework agreement or any other contractual arrangement where the data was provided under such an agreement. The minimum standards that apply under the information framework agreements or other relevant agreements for storage and security of data provided by the NBA are at Appendices 10 and 11.

5. Data Management

Good data management practices ensure that the NBA is able to make data available while meeting its obligations to all governments. The NBA will carry out data management through the stages of planning, collection, analysis, publication, storage and later re-use.

A data and information plan of activities will be prepared by the NBA and endorsed by the BIGG which will inform the data management activities for the NBA each year for all data requests and data publications. This will ensure timely and coordinated reviews for data requests. The Data and Information Team will process these requests for review within three weeks of the request.

ACCESS TO NBA SYSTEMS AND SYSTEM REPORTS

The NBA's guiding principle for information technology security is the Australian Government Information Security Manual and its associated documentation.

The NBA has a number of ICT systems that support the operational requirements of the Blood Sector and these can be accessed by key stakeholders as outlined in Table 6. The rules for approving access to these systems are governed by the DIAM.

TABLE 6: ACCESS AND APPROVAL FOR NBA SYSTEMS

NBA Systems	Access	Implementing DIAM Approvals	Data Dictionary
BloodNet	• Health Providers using an electronic access approval form to enter and display own data and run their own site reports. Some reports have aggregated peer group, state and national comparator data	NBA CIO	To be made available
	• NBA staff and IT staff developing, administering or supporting the system	BIGG and NBA CIO	
	• NBA Data and Information Team to run reports for analysis, release and publication in line with the DIAM. All personal information is de-identified	BIGG and NBA CIO	
	• Blood Service receives order information to meet supply of products	BIGG and NBA CIO	
	• Jurisdiction reports for own state data and some reports have aggregated peer group, state and national data for comparator purposes. This information is posted to Jurisdictional Reports or provided via report extracts	BIGG and NBA CIO	

NBA Systems	Access	Implementing DIAM Approvals	Data Dictionary
BloodChat	Interested parties can get access to some forums, others are restricted to segments of users by an electronic access approval form	NBA CIO	Not relevant
BloodPortal	Provides a central user management and authentication system, enabling users of National Blood Authority (NBA) systems across the blood sector to have one single username and password, one place where they can update their contact details with the NBA and subscribe to mailing lists relating to transfusion in Australia	Not relevant	Not relevant
BloodDocs	For NBA committee members to access the papers for committee meetings securely and quickly on their iPads	NBA CIO	Not relevant
Jurisdictional reports	For JBC members or their nominees – own state and territory data or aggregated state and territory data with comparator at peer group, state and national level	BIGG and NBA CIO	Not relevant
ABDR As defined by the Permissions matrix agreed by the ABDR Steering Committee. The process for this is shown in Appendices 8 and 9	• Haemophilia Treatment Centre (HTC) employees for data entry of own HTC or shared patient HTC information. • HTC employees can run reports for own site information	BIGG and ABDR Steering Committee	On request of the ABDR Steering Committee
	• NBA staff and IT staff developing, administering or supporting the system	BIGG and ABDR Steering Committee	
	• NBA Data and Information Team to run reports for analysis, release and publication in line with the DIAM. All personal information is de-identified and test system for verifying has scrambled data for de-identification purposes	BIGG and ABDR Steering Committee	
	• HTC Directors receive reports of aggregated data at HTC level for comparator purposes and analysis. No patient level information is supplied only aggregate level	BIGG and ABDR Steering Committee	
MyABDR	A secure app for smartphones (Android and iOS) and a web site for people with bleeding disorders or parents/caregivers to record home treatments and bleeds. Information from this system is updated into ABDR and then the ABDR access permissions are used	Haemophilia Centre	Not relevant
Ig System	TBC	TBC	TBC

NBA Systems	Access	Implementing DIAM Approvals	Data Dictionary
Internal System - Big Red	Internal to the NBA and access is provided to NBA staff on a need to know basis with a business need	Business owner and BIGG	Available to internal NBA users
Internal System - IDMS	Internal to the NBA and access is provided to NBA staff on a need to know basis with a business need	Business owner and BIGG	Available to internal NBA users

ACCESS TO NBA DATA COLLECTIONS

The NBA has a number of data collections that support the operational requirements of the NBA and these can be accessed by key stakeholders as outlined in Table 7. The NBA collects and uses data in accordance with its objectives, Commonwealth policies and jurisdictional requirements. The rules for approving access to these systems are governed by the DIAM.

TABLE 7: ACCESS AND APPROVAL FOR NBA DATA COLLECTIONS

NBA Data Collections	Access	Provided By	Use
National Haemovigilance Data Set	NBA Data and Information Team	Jurisdictions	For the National Haemovigilance Report
Red Cell Data Linkage Set	NBA Data and Information Team	Jurisdictions	For analysis
IVIg STARS Extract	NBA Data and Information Team NBA Business Owners	Contract with Blood Service	For National IVIg Report and supply planning

WHO PROVIDES ACCESS TO THE DATA AT THE NBA

When considering a data request the NBA will always assess the purpose of that collection against its obligations and stated functions under the National Blood Agreement and *National Blood Authority Act 2003.* In particular, this includes ensuring the safe and secure supply of blood and blood products in Australia. Any request for data will be accompanied with information setting out why the data is being sought, how that request links with current government strategic goals and any further detail that may be required for that request, including a notice under Australian Privacy Principle 5 of the *Privacy Act 1988* (Cth) where there is a collection of personal information. The Data and Information Team will review all data requests and system report requirements and when the requirements are confirmed will provide the request to the approvers as per the DIAM for approval to fulfil the data request. The request may then pass to the IT Team for development of a new report including the functional specification.

QUALITY ASSURANCE PROCESS

To ensure that all controls are maintained and steps are adhered to, the NBA will provide a document with each publication or release, detailing supporting quality assurance processes, including:

- data sources, collection methods, and distribution requirements
- validation methods and controls throughout the lifecycle from input to publication or archiving
- data manipulation steps
- relevant quality assurance and approval processes
- quality control for reports including reconciliation and testing
- analysis and investigation of data outliers, in particular those that are consistent
- relevant standards used.

Data releases in response to data requests will be provided with guidance on the data sources, collection methods, distribution requirements and quality assurance and approval process.

INTERNAL REVIEW

Internal reviews of publications and data requests will be undertaken by the Data and Information Team in accordance with the set of criteria set out in the data request and data publication checklists (Checklists). Reviews will be carried out as soon as practicable and validated against the Checklist which determines collation and release. Data requests can be approved for release by the Executive Director if all the criteria in the Checklist have been met in accordance with the DIAM.

BLOOD INFORMATION GOVERNANCE GROUP (BIGG) REVIEW

The BIGG is responsible for ensuring compliance with quality assurance processes. Following internal review, data and information documents may go through a final review by the BIGG in accordance with the DIAM (including Legal, ICT and Communications review) and be signed off by the Executive Director and the General Manager according to the type of publication or data release. A copy of the terms of reference for the BIGG is at Appendix 2.

This part of the review will have three stages:

1. Review and comment on draft data and information materials
2. Review of the revised draft that describes how comments have been addressed
3. Review of the final draft in accordance with the following criteria:
    - Relevance - The degree to which information meets the needs of users. How well the data meets the agreed purpose of the data collection in terms of concepts measured and the population represented.
    - Accuracy - The degree to which the data correctly describes the events they were designed to measure. The implications for how useful and meaningful the data will be for interpretation or further analysis. The types of errors that will be considered and how these relate to the caveats provided when data is released are:
        - coverage error: this occurs when a unit in the data is incorrectly excluded or included, or is duplicated in the data
        - response error: this refers to a type of error caused by records being intentionally or accidentally inaccurate or incomplete. This occurs not only in statistical surveys, but also in administrative data collection where forms, or concepts on forms, are not well understood by respondents
        - non-response error: this refers to incomplete information for a record (e.g. when some data is missing). The use of any imputation strategies should be noted
        - sample error: where sampling is used, the impact of sample error can be assessed using information about the sample design, the total sample size and the size of the sample in key output levels. For sample surveys, response rates should be provided
        - other sources of errors: Any other serious accuracy problems with the statistics should be considered. These may include errors caused by incorrect processing of data (e.g. erroneous data entry or recognition), rounding errors involved during collection, processing or dissemination, and other quality assurance processes
        - revisions to data: the extent to which the data are subject to revision or correction, in light of new information or following rectification of errors in processing or estimation, and the time frame in which revisions are produced

EXTERNAL REVIEWS

Following an internal review, certain data requests and documents may be subject to external reviews by experts, a separate governance group (eg ABDR Steering Committee) or for ethics referral in accordance with the DIAM.

- *Expert Review* – seeks the review and comment of qualified experts in the specific subject matter to verify whether the work satisfies the specifications for review. Reviews may identify deviations

from standards, and suggest improvements. Reviewers will be selected based upon criteria of expertise, balance, independence and the absence of any conflict of interest

- *Separate Governance Groups* - seeks the review and approval of an separate governance group to:
  - verify whether the data publication or data request satisfies the separate governance criteria
  - confirm the specifications for release
  - identify deviations from standards and suggest improvements
- *Ethics Referral* - Where the use of data is for a research project, or where it requires the release of potentially sensitive data such as data on individuals, the NBA will seek documentation that the data proposal has been reviewed and approved by a Human Research Ethics Committee registered with the NHMRC.

EXTERNAL SCRUTINY OF PROCESS

The NBA will provide an annual report to the JBC on the activities and processes conducted by the NBA under this framework.

ACKNOWLEDGEMENT AND AUTHORSHIP

The requestor agrees to acknowledge the data provided by the NBA in publications, promotional material, and activities relating to the data and information provided. The minimum requirement for the acknowledgement is as below and if there are further acknowledgments to be made this will be done on a case by case basis depending on the level of advice or analysis provided by the NBA.

NATIONAL BLOOD AUTHORITY AUSTRALIA

The National Blood Authority on behalf of all Australian governments has provided the data and information in this report.

The criteria for authorship as defined in Section 5 of the Australian Code for the Responsible Conduct of Research 2007, NHMRC should not be offered to those who do not meet the requirements set out. For example, providing data that has already been published or materials obtained from third parties, but with no other intellectual input, does not justify including the provider as an author.

Where the NBA collects data from other stakeholders the NBA will acknowledge these sources when providing data or in publications as agreed with the relevant stakeholder.

RETENTION AND DISPOSAL OF DATA

Unless otherwise raised by stakeholders when requesting data collections, all records retained or disposed within the NBA must be undertaken in accordance with the NBA's Records Disposal Authority, and the relevant General Disposal Authorities issued by the National Archives of Australia.

The NBA's Records Management Policy is consistent with the *Public Service Act 1999* (PS Act), *Archives Act 1983* (Archives Act), *Freedom of Information Act 1982* (FOI Act), *Privacy Act 1988* (Privacy Act), *Evidence Act 1995* (Evidence Act), *Electronic Transactions Act 1999* (ETA 1999), the Administrative Functions Disposal Authority (2010) and the Digital Transition Policy (2012).

DATA AND INFORMATION ACCESS MODEL

An NBA DIAM has been developed to ensure the right level of information is available to appropriate users of ICT systems, data collections and for data requests. The DIAM outlines the level of access for each type of user, both internal and external to the Agency based on the type of data required and the intended audience. The process of developing the access model for a data collection is based on analysis of how information in a system is required to be accessed taking into account the objectives of the National Blood

Agreement as well as any security, confidentiality privacy (legal), policy, ethical or management requirements. Table 8 and Table 9 outline the minimum approval levels for the release of data from the NBA.

Where the NBA has collected jurisdictional data the NBA will restrict the ability to provide or use data based on the rules outlined in the information framework agreements or other relevant agreements with jurisdictions (or other contracts with relevant stakeholders) and in accordance with the DIAM.

The DIAM has been split into two levels for data access/requests, one for record level data requests and one for aggregated level data requests. Under each table there is a level for how the information is identifiable eg Level 1 under Record Level will not identify the jurisdiction, the health provider group/peer group, the health provider or the patient/clinician, while Level 6 identifies all this information.

Under each of these levels is the type of entity requesting data or access to IT systems and the different roles that can approve the request. A description of these approvers as follows:

Approver	**Description**
Release	NBA releases data as requires no approval
ABDR Steering Committee	Australian Bleeding Disorders Registry Steering Committee
The BIGG	The Blood Information Governance Group
Ethics	Relevant Ethics committee(s)
JBC member	JBC member refers to JBC member for jurisdiction data relates to and includes JBC proxies/nominees JBC member may see fit to obtain further approvals from Health Providers or Ethics
Data Custodian	NBA Data Custodian

If the request meets more than one data request level approval should be obtained from all approvers listed under the levels in the DIAM.

TABLE 8: DATA AND INFORMATION ACCESS MODEL – RECORD LEVEL DATA

Data Request Level		**Level 6**	**Level 5**	**Level 4**	**Level 3**	**Level 2**	**Level 1**	**Level ABDR Data**
Information Level		**Record**	**Record**	**Record**	**Record**	**Record**	**Record**	**Record**
Information identifiable by								
Jurisdiction		**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**No**	**Yes or No**
Health Provider Group/Peer Group		**Yes**	**Yes**	**Yes**	**Yes**	**No**	**No**	**Yes or No**
Health Provider		**Yes**	**No**	**Yes**	**No**	**No**	**No**	**Yes or No**
Patient/clinician		**Yes**	**Yes**	**No**	**No**	**No**	**No**	**Yes or No**
Item	**Disclose to Requestor**	**Approvers**						
A.	Health Provider or Health Provider organisation requesting own data	BIGG JBC member	n/a	Data Custodian	n/a	n/a	n/a	BIGG ABDR Steering Committee
B.	Health Provider or Health Provider organisation requesting others' data	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee
C.	NBA Data and Information Team	Data Custodian JBC member	Data Custodian JBC member	Data Custodian	Data Custodian	Data Custodian	Data Custodian	BIGG ABDR Steering Committee
D.	NBA staff other than Data and Information Team	Data Custodian JBC member	Data Custodian JBC member	Data Custodian	Data Custodian	Data Custodian	Data Custodian	BIGG ABDR Steering Committee
E.	ABDR Steering Committee	BIGG JBC member	BIGG JBC member	BIGG JBC member	BIGG JBC member	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee
F.	JBC member requesting own jurisdiction's data	Data Custodian BIGG	Data Custodian BIGG	Data Custodian	Data Custodian	Release	Release	BIGG ABDR Steering Committee
G.	JBC member requesting other jurisdiction's data	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee
H.	Researcher or other stakeholder conducting research	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee
I.	Publication	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee
J.	Supplier	No	No	No	No	No	No	BIGG ABDR Steering Committee
K.	Other including individuals	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	BIGG JBC member Ethics	Data Custodian JBC member	Data Custodian JBC member	BIGG ABDR Steering Committee

TABLE 9: DATA AND INFORMATION ACCESS MODEL – AGGREGATE LEVEL DATA

Data Request Level		**Level 4**	**Level 3**	**Level 2**	**Level 1**	**Level ABDR**
Information Level		**Aggregate**	**Aggregate**	**Aggregate**	**Aggregate**	**Aggregate**
Information Level Identifiable by						
Jurisdiction		**Yes**	**Yes**	**Yes**	**No**	**Yes or No**
Health Provider/Peer Group		**Yes**	**Yes**	**No**	**No**	**Yes or No**
Health Provider		**Yes**	**No**	**No**	**No**	**Yes or No**
Item	**Disclose to Requestor**	**Approver**				
A.	Health Provider or Health Provider organisation requesting own data	Data Custodian	Data Custodian	n/a	n/a	BIGG ABDR Steering Committee
B.	Health Provider or Health Provider organisation requesting others data	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
C.	NBA Data and Information Team	Release (no approval required)	Release (no approval required)	JBC proxy*	Release	BIGG ABDR Steering Committee
D.	NBA staff other than Data and Information Team	Data Custodian	Data Custodian	JBC proxy*	Release	BIGG ABDR Steering Committee
E.	ABDR Steering Committee	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
F.	JBC member requesting own jurisdiction's data	Data Custodian	Data Custodian	JBC proxy*	Release	BIGG ABDR Steering Committee
G.	JBC member requesting other jurisdiction's data	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
H.	Researcher or other stakeholder doing research	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
I.	Publication	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
J.	Supplier	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee
K.	Other including individuals	Data Custodian JBC member	Data Custodian JBC member	JBC proxy*	Release	BIGG ABDR Steering Committee

*Release if already publically available but seek JBC proxy agreement if it has not been made public

6. Best Use of Available Data

DATA REQUESTS

DATA COLLECTION AND RELEASE RULES

The data collection and release rules for the NBA are outlined at Table 10 and Table 11.

TABLE 10: DATA COLLECTION RULES

No	Rules
1.	Data is only collected for business purposes that are aligned to NBA objectives and fit for purpose
2.	Any separate governance considerations to be developed for new systems, must be considered for all privacy and compliance aspects
3.	All data collected through and entered directly into national data systems belongs to the NBA on behalf of all Australian governments and should be consistent with agreed minimum data sets and definitions
4.	The requirements and solution design for any new system or collection capabilities developed by the NBA (e.g. the Ig Database) will be aligned to the data governance framework to ensure that the solution will be built and maintained in such in a way that supports the Information Security Manual
5.	Ad-hoc reporting is subject to data availability, resources and rationale for data collection.
6.	New data collections must have appropriate governance protocols established for development, processing, access, use, storage and approvals process
7.	Development of data sets will be consistent with all legal obligations, specifically privacy principles being cognisant of disclosure, collection and use, management and communication of reporting. Where data does not comply with these principles it will not be published or released
8.	Data collected from third parties, including state and territory governments' and other Commonwealth agencies will be subject to the requirements in information framework agreements or other relevant agreements on a case by case basis. This will include compliance with state and territory obligations for storage, security, privacy, confidentiality, intellectual property and records retention policies

TABLE 11: DATA RELEASE RULES

No	Rules
1.	All NBA data activity will be consistent with the agreed sector data principles including release and clearance
2.	All data should be available in accordance with the DIAM or the information framework agreement or other relevant agreement, other than where: • Data sets contain patient identifiable data (all data releases must be de-identified unless approved by each individual) • It is subject to separate governance constraints for example: ABDR reports have process for approval with the ABDR Steering Committee • It could adversely impact security of supply • It could distort market forces
3.	All research should demonstrate ethical consideration. Where a determination by a recognised Human Research Ethics Committee (HREC) is required, the NBA GM will be responsible for sign off of the data release after approval is provided as per the DIAM
4.	Aggregated data at a state and territory or national level will be made available on request in accordance with the DIAM
5.	Where data is patient or clinician identifiable it will be only accessible to defined personnel with responsibility to aggregate or de-identify to a non-identifiable level
6.	Where data is health provider identifiable, approval for publication or release must be obtained from the state or territory

No	Rules
7.	Standard national data reports will be published on a regular basis, based on consultation with internal and external stakeholders to identify priority information needs
8.	Standard release and clearance protocols and publishing rules will be adhered to by the NBA
9.	ABDR and MyABDR data will not be released unless approved by the ABDR Steering Committee
10.	Where data is proposed to be released to third parties, the NBA will adhere to state and territory governments' and other Commonwealth agencies requirements in the information framework agreements or other relevant agreements on a case by case basis or in accordance with the DIAM. Also refer to Appendices 4 and 5
11.	Consider the jurisdictional data collections issues and Commonwealth data governance framework at Appendices 4 and 5
12.	Accuracy of data provided by the NBA is the responsibility of NBA to ensure validity. In releasing any data, the NBA will alert data users to caveats and note differences in data sets between jurisdictions
13.	Research and Development data requests are subject to Section 95A of the *Privacy Act 1988* for private organisations in circumstances where, for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety, an organisation must collect, use or disclose health information. It must be impracticable to seek consent from the individual(s) involved and it also must be that de-identified information will not achieve the purpose of the research or compilation or analysis of statistical activity
14.	Research and Development data requests will require state and territory approval (if the data relates to a specific state or territory) together with Ethics approval if required. If the research proposal has been through formal peer review eg NHMRC application submission, this will provide sufficient assurance as to data management and validity of methodology. The audience and purpose for the research must be stated and approved. If the purpose or audience changes from the initial request then an extension/revision must be sought from the NBA

REQUESTING DATA FROM THE NBA

The NBA will manage data requests using a structured process. Figure 2 and Figure 3 provide an overview of the data request and publication oversight process.

A data request form is to be completed (refer to Data Request Form) and submitted to the Data and Information Team. An initial request can be made verbally, however it must be followed up in writing prior to formal consideration. The request is entered into a register of data requests and identified to the BIGG chair for review against the criteria. The BIGG will provide coordination and oversight on all data access. Table 12 provides further details on the process and responsibilities of each party.

FIGURE 2: DATA REQUEST AND PUBLICATION OVERSIGHT PROCESS

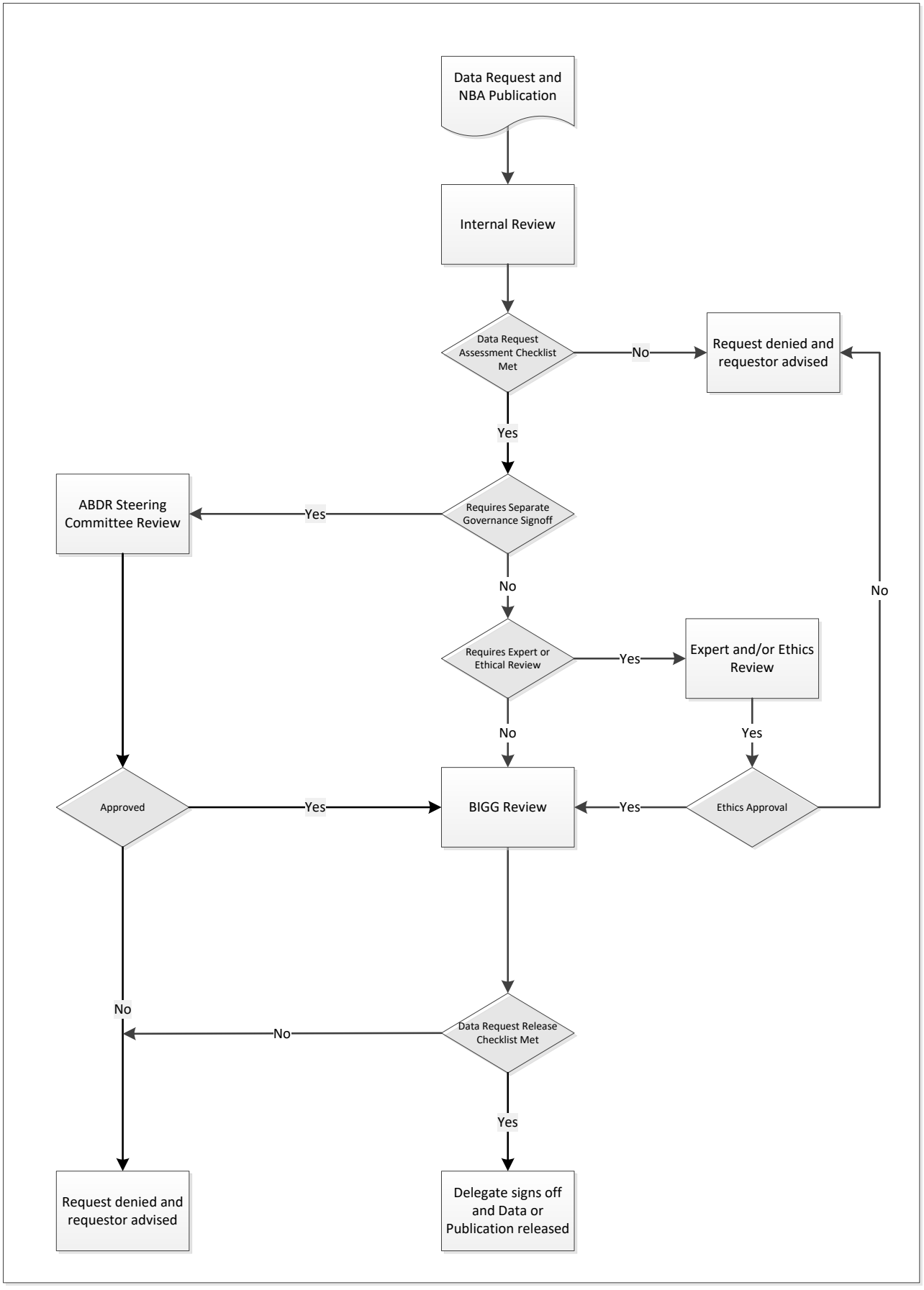


TABLE 12: PROCESS FOR DATA REQUEST FROM THE NBA

Process	Responsibility
Stakeholder requests data from NBA	• Provides written request for data including purpose, use and any proposed disclosures using the data request form • Understands state and territory and Commonwealth data governance obligations • Considers any notified NBA data governance obligations • Understands and communicates any obligations it has to NBA via any information framework agreements or other relevant agreements
NBA considers request for data	• Adds request to register of data requests • Considers data requests in a timely manner against Data Request Checklist 1 and 2 • Notifies separate governance group of request (eg ABDR Steering Committee) and seeks signoff • Notifies entity of specific data governance requirements for request • Understands state and territory and Commonwealth data governance obligations • Understands NBA data governance issues • Identifies sensitivities with specific data requests • Consults with relevant stakeholders • Considers options to address sensitivities including anonymising or aggregating data or dealing with request via licensing or contractual arrangement • Consider jurisdictional information framework agreement obligations or jurisdictions requirements • The NBA will consider the request and provide notice to the requestor of acceptance of the request within 10 business days of receipt
Stakeholder addresses sensitivity issues	• Applies security framework for classification, handling, storage, use and disclosure of confidential, sensitive, or personal information • Considers options to address sensitivity including whether aggregated or anonymous data can achieve objectives or whether consent required • Ensures entity, employees and contractors only access, use or disclose data in accordance with specified limitations
NBA finalises data request	• Approval process from various groups sought within one month of the notice of acceptance provided to the requestor • Data released to entity including any restrictions on use or disclosure, storage and or security requirements • Undertaking or agreement established if required for provision of particular data prior to release • Data is not released to the entity and reasons for that decision are given in writing providing visibility over the application and decision making process and NBA will set out the factors it has considered in making the decision • The NBA will consider appeals and complaint regime which is visible to users/requesters of information
Stakeholder receives data	• When information is released the receiver of the data must comply the specific conditions on which it is provided and also what research results/outcomes should be shared and with which jurisdictions • Uses, discloses and stores data in line with agreed limitations and security requirements • Returns confidential information to NBA if no longer required (subject to legislative, administrative or other limitations)

The assessment and release of data and information will be made against a set of criteria in checklist format as outlined at Table 13 and Table 14. All relevant criteria must be satisfied prior to seeking approval to release. Authority to release the data and information is delegated from the General Manager to the BIGG chair or the BIGG. However, if the risk associated with the data request is assessed as 'high risk' then the General Manager will approve data release.

In instances where approval requires additional information from the requestor or the data is not deemed suitable for release or is not held, then the requestor will be advised within one month of the notice of acceptance.

The data is checked to ensure it can be validated, replicated and/or reconciled and has currency. Where possible it is compared to similar data. Only de-identified, anonymised data compliant with the *Privacy Act 1988* will be released. The data will undergo rigorous quality assurance checks.

Where a data request relates to a pre-existing document (in hard copy or electronic form) the Data and Information Team will liaise with the NBA FOI Coordinator.

DATA REQUEST CHECKLISTS

The criteria to assess data requests and provide release are set out in Table 13 and Table 14 below:

TABLE 13: DATA REQUEST ASSESSMENT CHECKLIST

Criteria	Checklist	Comment
Has the request form been completed and signed?	☐ Yes ☐ No	
Is the use and rationale for the data request within the rules and principles of data collection and release?	☐ Yes ☐ No	
Are there any confidentiality requirements?	☐ Yes ☐ No	
Is the data consistent with similar data released?	☐ Yes ☐ No	
Can the NBA produce the data?	☐ Yes ☐ No	
Does the requester agree to the conditions of the data release?	☐ Yes ☐ No	
Is the data at aggregate or record level for health provider, patient, clinician, jurisdiction or organisation level?	☐ Aggregate ☐ Record	
Have privacy issues been addressed?	☐ Yes ☐ No	
Can the data contribute to possible perverse use? Consider user, patient, clinical, commercial or market drivers.	☐ Yes ☐ No	
Is the release of the data in the public Interest?	☐ Yes ☐ No	
Does the request comply with the Data Collection and Release rules?	☐ Yes ☐ No	

TABLE 14: DATA REQUESTS RELEASE CHECKLIST

Release of Data	Checklist	Comment
Is the data fit for purpose?	☐ Yes ☐ No	To be signed off at all levels of the approval process
Does the data release require legal input?	☐ Yes ☐ No	
Has the data been validated and checked?	☐ Yes ☐ No	
Are there any identified gaps in the data and caveats (e.g. missing data)?	☐ Yes ☐ No	
Is the data population correct at time of extract (e.g. check load dates)?	☐ Yes ☐ No	

Release of Data	Checklist	Comment
Have IP, copyright and creative commons been addressed if required?	☐ Yes ☐ No	
Can the data be replicated?	☐ Yes ☐ No	
Have all quality assurance checks been undertaken?	☐ Yes ☐ No	
Have the NBA style and format guides been adhered to?	☐ Yes ☐ No	
Has the statistical methodology been documented if required?	☐ Yes ☐ No	
Were inputs from 'experts' gathered?	☐ Yes ☐ No	
Does the request comply with the Data Collection and Release rules?	☐ Yes ☐ No	
Has the data release received ethics approval if required from all appropriate bodies?	☐ Yes ☐ No	
Has the JBC member/proxy signed off if required?	☐ Yes ☐ No	
Has the ABDR Steering Committee signed off if required?	☐ Yes ☐ No	
Has the BIGG or other delegate approved release as per the DIAM?	☐ Yes ☐ No	

MECHANISM FOR RELEASE OF DATA

Aggregate level data will be released to approved data requestors via email, NBA reporting portals or secure storage devices as determined by the level in the DIAM and the size of the data file or report to be provided.

Record level data will be released to approved data requestors, NBA reporting portals or secure encrypted storage devices as determined by the level in the DIAM and the size of the data file or report to be provided.

REGISTER FOR DATA PUBLICATION AND REQUESTS

The NBA maintains a register of all data published or released in response to data requests from both internal and external stakeholders. The register is updated and reviewed by the BIGG to ensure it remains current. The NBA register includes:

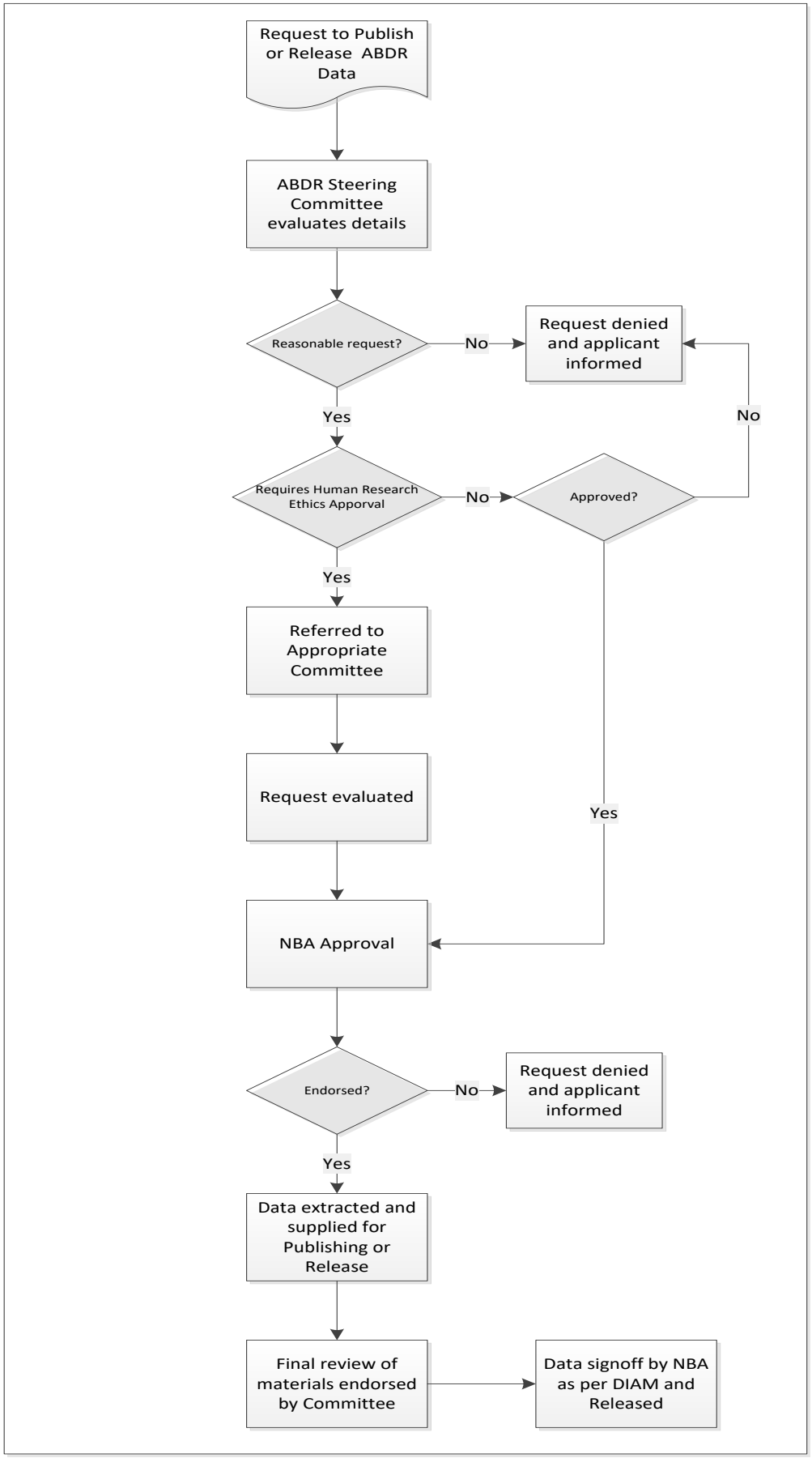
- description of data request
- request number (sequential ie 2013-xx)
- person requesting
- date request received
- current status
- description of data provided
- where data is to be published
- caveats
- audience
- system data was extracted from
- entities informed of the data provision
- date provided data or advised request not met
- approved by and date

ABDR ARRANGEMENTS GOVERNING THE RELEASE OF DATA TO THIRD PARTIES OR PUBLICATION OF DATA

The ABDR Steering Committee has responsibility for oversight of arrangements governing the release of data from ABDR to third parties or publication of data. No data from ABDR is to be released to a third party or be published without AHCDO Executive and ABDR Steering Committee approval and ratified by the NBA in accordance with the processes described in the ABDR data governance framework. Internal data requests must be approved by the ABDR Steering Committee and ratified by the NBA. All requests should be sent to the NBA Data and Information Team who will forward to the relevant party for approval, as outlined at Figure 3.

Privacy and security arrangements will be reviewed at least annually to ensure they are complied with and are effective, and to maintain currency with changes in legislation or government policy.

FIGURE 3: ABDR DATA REQUEST AND PUBLICATION OVERSIGHT PROCESS



NBA REQUESTS STAKEHOLDER DATA

The NBA also requires data from jurisdictions and stakeholders in order to fulfil its duties and these can be at record level or aggregated. Where they are at record level there may be a need to implement a data linkage project and these will be done in accordance with the data linkage process. Table 15 sets out the process for the NBA to request data from stakeholders.

TABLE 15: PROCESS FOR THE NBA TO REQUEST STAKEHOLDER DATA

Process	Responsibility
NBA requests data from stakeholder	• Establishes centralised NBA quality assurance process for data requests • Considers Commonwealth legislation, policy and contractual requirements when making requests • Considers and addresses known state and territory data governance issues when making data requests • Provides written request for data including purpose, use and any proposed disclosures using NBA Data Request Form or stakeholder form • Identifies data sensitivities • Adds request to register of data requests • Informs state or territory government of requests to jurisdictional entity
Stakeholder considers request for data	• Considers data requests in a timely manner • Notifies NBA of specific data governance requirements for request • Liaises with data sources/owners for record level data requests • Understands and communicate state and territory or Commonwealth data governance obligations • Identifies sensitivities with specific data requests • Consults with relevant stakeholders • Considers options to address sensitivities including anonymising or aggregating data • Considers cost of data extraction
NBA addresses sensitivity issues	• NBA assists entity including drafting required confidentiality agreement or licencing arrangement where warranted, anonymising or aggregating data and/or consent
Stakeholder finalises data response	• Data released to NBA including any restrictions on use or disclosure, security requirements, or • Data not released to NBA and reasons for that decision are given in writing
NBA receives data	• Gives due consideration to submissions received on consultation • Consults in writing with relevant stakeholders prior to release or publication • Uses, discloses and stores licensed data in line with agreed limitations and security requirements • Reports to JBC on data requests and data governance issues • Reviews data governance arrangements and conducts regular audits of process

DATA LINKAGE

The NBA, with states and territories will implement data linkage projects and these will be undertaken on a case by case basis under the information framework agreements or other relevant agreements to be established with each jurisdiction. They will set out the roles and responsibilities of all parties as an

overarching document and will include separate schedules for each specific data linkage collection/provision. The schedule for each data linkage project will include:

- toolkits on how the data will be collected, retained, secured, archived, accessed and published
- principles and policies which guide the way that the linkage is done
- procedures for how the linkage will be implemented, including minimum data sets

The schedule to be completed for each data linkage project is at Appendix 7.

DATA PUBLICATION BY THE NBA

The 2010 amendments to the FOI Act require documents owned by the NBA to be released under an open licence unless there is a reason not to do so. For further details on the NBA FOI process refer to the FOI page on the NBA's website. The Australian Privacy Commissioner has established a guide to assist agencies to comply with these obligations. Part 13 of the guide details the Information Publication Scheme (IPS) which outlines requirements for agencies, some of which are presented below:

> 13.83 An agency's operational information must be published as part of an agency's IPS entry (s 8(2)(j)). 'Operational information' is defined in s 8A(1) as:
>
> … information held by the agency to assist the agency to perform or exercise the agency's functions or powers in making decisions or recommendations affecting members of the public (or any particular person or entity, or class of persons or entities).
>
> 13.84 The publication of operational information ensures that members of the public can be adequately informed about the framework of rules, policies, principles and procedures that agencies apply in making decisions or recommendations that affect members of the public.
>
> 13.86 Operational information is all information held by an agency, whether generated by the agency or not, that assists it to perform or exercise its functions or powers in making decisions or recommendations that affect members of the public (or any particular person or entity, or class of persons or entities). The person affected by an agency decision may be an individual, an organisation or a business entity. Section 8A refers to the following as examples of operational information: '[t]he agency's rules, guidelines, practices and precedents relating to … decisions and recommendations' affecting members of the public.

The NBA agency plan describes how the NBA proposes to do this, as required by s 8(1) of the FOI Act.

In order to achieve the agency plan the NBA is reviewing all data held and reported by NBA and will provide a plan for what data will be published and how these will link to the IPS requirements. The process for publication or release of data held by the NBA or provided to stakeholders by the NBA is outlined in Table 16.

TABLE 16: PROCESS FOR PUBLICATION OR RELEASE OF DATA

Process	Responsibility
Stakeholder release or publication of NBA data	• Maintains security framework for classification, handling, storage, use and disclosure of confidential, sensitive, or personal information • Ensures entity, employees and contractors only access, use or disclose data in accordance with specified limitations • Understands state or territory data governance obligations, including the security framework • Evaluates impediments to release or publication in line with legislative, policy, administrative and contractual obligations as well as any identified sensitivities

Process	Responsibility
	• Consults with NBA prior to any proposed disclosure or use outside agreed limitations • Gives due consideration to public consultation submissions received • Publishes and releases data in line with state and territory obligations
NBA release or publication of Stakeholder data	• Applies NBA quality assurance and governance process for data publication • Uses, discloses and stores data in line with agreed limitations and security requirements • Completes the NBA publishing criteria checklist • Consults in writing with relevant stakeholders prior to release or publication • Gives due consideration to submissions received on consultation • Reports to state and territory on data requests and data publication • Evaluates impediments to release in line with legislative, policy, administrative and contractual obligations • Notifies stakeholders where legal requirement to disclose arises • Adds publication to the register of data requests and publications

Data and information publication and release by the NBA will be assessed within the NBA Publishing Criteria Checklist at Table 17 for release on the NBA website. Release will be governed by this plan and agreed by the BIGG in accordance with the IPS and the DIAM.

TABLE 17: NBA PUBLISHING CRITERIA CHECKLIST

CRITERIA	PRIORITY	WHY
Decision to Publish		
Required to meet IPS obligations in conjunction with transparency objectives	1	Comply with IPS
Must balance user data needs against NBA available resources and efficiency	1	Meet user information needs within NBA resource constraints
Meet needs of user and does not impose burden on data collectors and reporters	1	Meet user information needs within external resource constraints
Data provided previously to be used where required	1	Consistent data publication
Align data publication with NBA, governments and Australian blood sector priorities	1	Ensure NBA stays relevant and inform government decision making
Personal data must be de-identified and aggregated	1	Protect privacy of individuals and comply with NBA governance arrangements
Non personal data such as State and territory and health provider may be identified and aggregated in accordance with the DIAM	1	Protect privacy of individuals and comply with NBA governance arrangements
Data must be timely and relevant	1	Improve availability of data
Must ensure quality of data	1	Improve data quality and analyse and investigate consistent data outliers
Data must be approved by the BIGG before publishing in accordance with the DIAM	1	Comply with NBA governance arrangements
Required for internal induction activities, skills transfer and/or knowledge management	1	Meet user information needs within NBA

CRITERIA	PRIORITY	WHY
How and what to Publish		
Data must have a meaningful title	2	Improve usability and interpretability of data
Data must have headers for rows and columns	2	Improve usability and interpretability of data
Data must be unlinked from source data before publishing	2	Improve availability of data
Data must comply with NBA Branding Guidelines or ABDR Branding Guidelines if required and acknowledge source of information as appropriate	2	Standardise data formats
Must provide different but suitable file formats for data, including Excel and CSV	2	Improve data reuse and accessibility
Data (set) must have an unique identifier (e.g. UML)	2	Maintain single source of truth
Web data contents must be tested for accessibility conformance before publishing	2	Improve data access
Data must be indexed and published under relevant themes/categories	2	Enable users to find and use NBA data easily
An NBA copyright/ licence notice (open licence or restricted licence) must be attached to published data	2	Protect NBA copyright and licensing
Should provide data citation information	2	Encourage users to use, reuse and cite NBA data
Should provide (text) summaries for data published by the NBA	2	Improve usability and interpretability of data
Should update online data on a regular basis for ongoing data collections	2	Improve availability of data
Should specify the expansion of abbreviations or acronyms for header labels	2	Improve usability and interpretability of data
Should publish simple formulas (e.g. summation and proportion) for calculations in Excel sheets	2	Improve usability and interpretability of data
Should use NBA data templates or agreed report format to publish data	2	Standardise data
Should not rely on the use of colours to convey information in tables	2	Improve accessibility of data
May use colours to convey information in tables as long as there is a symbol or other code that enables those that can't 'read' colours to still obtain the same data	2	Improve accessibility of data
May add footnotes to tables to explain data source, quality and methodologies	3	Improve usability and interpretability of data
May publish detailed metadata (e.g. content, quality and method) for data	3	Improve usability and interpretability of data
May document/explain the logical links for all tables in a dataset	3	Enable users to find and use NBA data easily
May consider the likelihood of linking data to other relevant resources	3	Improve usability and interpretability of data
May provide other file formats (e.g. html, PDF and XML) for data	3	Improve data reuse and accessibility

The following data is published by the NBA on an annual or biannual basis:

- Annual ABDR Reports
- Annual IVIg Reports
- NBA Annual Reports
- Haemovigilance Reports

DATA USE AND INTERPRETATION

The NBA will provide data for publication according to the following:

- the data and information should be suitable for the intended purpose
- the data and information must only be used for the purpose specified
- the data and information provided should be right the first time with mistakes eliminated
- the delivery of data and information for blood sector stakeholders is at the highest level of controlled reliability in its findings and analysis practices which are based on the best possible validated base information and data
- the data and information must not be used by a person other than the person(s) authorised
- the data and information must not be used to identify or contact any individual unless this is an approved purpose
- the data and information must not be merged with any other information sets held by the user without prior approval from the NBA in accordance with the DIAM
- the data and information must be protected by appropriate and approved security measures
- the data and information must not be kept for longer than approved without prior approval from the NBA
- the data and information must be appropriately disposed of in accordance with the NBA disposal policy.

The NBA will document where appropriate for the readers of all data publications the:

- data sources, collection methods, and distribution requirements
- data analysis and interpretation undertaken
- validation methods and controls throughout the lifecycle from input to publication or archiving
- data manipulation steps
- relevant standards used.

SECTOR SCORECARD REPORTING

The NBA will provide performance reporting through a Blood Sector Performance Scorecard administered by the NBA. The key objective in establishing this scorecard is to ensure integration of blood sector performance measurement with broader government health performance and accountability agendas.

The NBA will provide the performance indicators on the website within three months of the end of the financial year.

DEVELOPMENT IN LINE WITH THE COST BENEFIT FRAMEWORK

System development for data capture and data collection requirements will be supported by a business case and approved by all governments. The business case will provide a suite of roles and responsibilities on how each stakeholder will work with the NBA to support the use of the proposed system, together with the process for how the data will be reported and shared with relevant stakeholders.

Transparency in decision making on data collection including cost of collecting and storing data items will be made available to all governments together with the rationale for the data collection.

7. Sustainable Data and Information

SECTOR DATA

The sector has multiple disparate sets of patient level data which have been collected for specific purposes, such as pathology laboratory data. Suppliers often hold post-market data collections, and have entered the data management field collecting data from patients via electronic devices. Secondary data from the Australian Bureau of Statistics can be incorporated to provide contextual analysis, such as using population collections.

NATIONAL BLOOD SECTOR DATA AND INFORMATION STRATEGY

The National Blood Sector Data and Information Strategy 2013-2016 (Sector Data Strategy) outlines the direction and scope of data and information development for the blood sector over three years to meet the requirements identified under the National Blood Agreement.

Consistent with best practice, the Sector Data Strategy will be a 'living' document with feedback being invited via the NBA website and this will be collated and reviewed for the next version.

The development of the next Sector Data Strategy will be undertaken in consultation with key stakeholders and will be signed off by the JBC. It may be appropriate to provide public consultation with the next development of the Sector Data Strategy as further data requirements are understood and known.

The NBA proposes to provide a gap analysis of the data collections as part of the Sector Data Strategy. This will be done in collaboration with the blood sector. Additionally, there will be 'unknown' sets of data that may be 'discovered' as part of the gap analysis. The intent is to identify where efforts are to be deployed to deliver the most useful data and information for the benefit of the sector. The NBA will act as a 'hub' by collecting, storing, analysing and disseminating blood sector data.

OWNERSHIP AND MANAGEMENT OF AUSTRALIAN BLOOD SECTOR DATA AND INFORMATION

Ownership and management of the multiple blood sector data and information sets rests with many entities/parties/stakeholders. There is no defining list for the Australian blood sector. The NBA proposes to answer this question, in collaboration with the blood sector, by using the gap analysis to identify the following:

- Data custodian and steward details
- Where the data is held/stored/population cycle
- Identification of release officer
- System and format of available data/limitations
- Metadata and other relevant information

One issue relating to ownership and control is currency of data. The NBA will apply best practice in maintaining this blood sector information through consultation on a regular basis.
In carrying out the business of government and providing the Australian blood sector with agreed data and information, the NBA will interact with all stakeholders in the blood sector including other government agencies and industry bodies to monitor what is held, by whom and where it is held.

How data relates within the sector can be answered once the collection of the known blood sector data and information sets are documented by the NBA. The NBA will collaborate with the blood sector to produce this information.

Specifically this task will identify

- Value to the Blood Sector (agreed by the sector)
- Commonality (systems, format etc.)
- Degree of integration possible
- Limitations and barriers to future collection
- Timeliness (historical and comparability)
- Metadata and business rules
- Identification of minimum sets of data for the blood sector.

Best practice principles such as 'transparency of process and ensuring the accuracy of the information collected' will underpin this significant body of work. At the NBA, the BIGG will take oversight of the project plan in collaboration with the sector.

NATIONAL BLOOD SECTOR ICT STRATEGY

This *National Blood Sector ICT Strategy 2013-2016* outlines the context and prioritisation of the national ICT systems that underpin the delivery of data and operational systems to the blood sector. This strategy is intended to direct all ICT development funded under the National Blood Agreement (excluding internal NBA systems), however it is not intended to direct ICT development outside the scope of the national blood arrangements.

WHY WE NEED DATA STANDARDS

Governance arrangements exist at all levels within the sector. The blood sector must be able to demonstrate compliance against all required standards and community expectations. The governance framework for data collection and management at the national level must be able to guarantee and demonstrate:

Data is supported by data dictionaries, metadata and ensures a high quality data standard.

Standards are required for comparative purposes. Integrating data from disparate data collections requires the same meaning and consistency which can only be achieved through standardising how the data is defined.

An agreed set of data principles have been published through the provision of this framework against which data development can be assessed, with a guiding commitment to the development of a standards based approached.

DEVELOPMENT AND IMPLEMENTATION OF DATA STANDARDS

The development and implementation of data standards for the NBA will be in accordance with the data standards used by the Australian Institute of Health and Welfare (AIHW). The AIHW manages Australia's national health, community services and housing metadata items and standards, which provide the national infrastructure for metadata development.

Where a data standard does not exist within the standards published by AIHW, the NBA will ensure that the development and implementation of the data standard is in line with the practices used by AIHW, and only make changes where an Australian blood context is required.

DEVELOPMENT AND IMPLEMENTATION OF NATIONAL MINIMUM DATA SETS AND DATA DICTIONARIES

A minimum data set improves the comparability and consistency of national information. The national blood sector information requirements have been developed for specific data and the data set specifications were developed for the NBA minimum data sets. This includes development of specific data dictionaries, guidelines and other supporting documentation.

As defined by AIHW a national minimum data set (NMDS) is a minimum set of data elements agreed for mandatory collection (under the legal framework) and reporting at a national level. The NBA will establish data and information agreements with all states and territories when setting and agreeing minimum data sets for the blood sector. The data agreements will include the data dictionary and how the data and information will be used and published. Any blood sector minimum data sets will be at best a minimum set of data elements AGREED for collection and reporting at a national level.

The AIHW national health data dictionary is the model that the NBA will adhere to when creating data dictionaries to support data collection and developing data systems. This model will provide guidance for blood related data dictionaries. The AIHW NMDS descriptions can be found at METeOR. This alignment with AIHW dictionaries will avoid duplication and diversity of solutions thus reducing the cost of data development.

CURRENT NATIONAL MINIMUM DATA SETS FOR THE BLOOD SECTOR

The following is a list of agreed blood sector national minimum data sets that have been agreed or are in development in the blood sector:

- National Haemovigilance Data Dictionary
- Red Cell Data Linkage (in development)

As part of the National Blood Sector Data and Information Strategy 2013-2016 the NBA will develop data principles for the sector and identify the gaps by:

- documenting the data sets available for the blood sector and identifying the gaps in data collections and data linkages within the sector
- documenting the blood sector data collection architecture including the information flows and relationships
- prioritising and identifying measures to address the gaps in data collections and data linkages within the sector
- developing and implementing data and information agreements for data sharing and use between blood sector stakeholders
- identifying minimum data set specifications that align with nationally authorised data dictionary definitions
- developing and implementing standards for blood sector data within prescribed national minimum data sets and aligning blood sector data with the data requirements of the National Health Reform to provide consistency of content and definition, to avoid duplication and diversity of solutions, and to reduce the cost of data development.

Also as part of the Patient Blood Management (PBM) Guideline Implementation Strategy 2013-17 there is a requirement for data to support patient blood management practice improvement. The NBA will also update the Blood Measures document to include guidance on, and minimum data sets for transfusions and PBM outcomes.

8. Appendices

APPENDIX 1: DATA PRINCIPLES

COMPATIBILITY OF DATA

The NBA should:

1. Encourage the development of blood sector data collections at a local, regional and/or national level that have the capacity to be benchmarked against similar Australian or international collections through the development and/or promulgation of common or model data definitions, dictionaries, standards and processes
2. Facilitate the promulgation of local, regional, national and international data collections that allow participants in the sector to self-assess their performance against other sector participants
3. Facilitate development of blood sector data collections that maximise compatibility with broader health collections

ACCESS TO DATA

Having regard to privacy legislation and jurisdictional sensitivities, the NBA should support data collections where:

4. The data is directly accessible to those who can derive immediate benefit from access to the data
5. The data will be published and made broadly available to drive sector performance both in Australia and internationally in accordance with the DIAM
6. Data will be stored, used and released in accordance with strict protocols with the intention of maximising the potential usefulness of any data collections to the blood sector without undermining ownership or confidentiality provisions
7. The potential clinical benefits of data promulgation are not delayed by persons or institutions seeking an individual benefit
8. The process of publication will involve relevant stakeholders and publication will NOT occur without the agreement of ALL relevant stakeholders

EFFICIENCY OF DATA COLLECTION EFFORTS

Recognising that the use of blood products is a small part of total activities in most medical facilities, and that jurisdictions and health facilities can have very different data environments and systems, national collections should ideally:

9. Provide a benefit to those who enter the data
10. Not require unnecessary duplicate data entry, and be a by-product of service delivery
11. Not depend on the existence of a particular supplier and/or supply arrangements, unless related to the performance of that supplier/supply arrangement
12. Strive to minimise effort at all levels

DEVELOPMENT OF COLLECTIONS

13. Should be within a cost benefit framework, which considers alternative methods such as audits, sample collections and surveys, before commencing the development of new comprehensive national collections

14. Should seek the minimum data required to make a material difference with minimum collection effort

15. Should not duplicate existing systems which serve an essentially similar purpose

16. Should provide benefits to a number of stakeholders

17. Process development should include key stakeholders through consultation and/or a steering committee

18. Must comply with national and international data standards

USE AND INTERPRETATION OF DATA

19. Must be undertaken with a full understanding of the methods of data collection, including the reliability and validity of the measures

20. Should understand and acknowledge limitations of the data sets

21. Must be sensitive to confidentiality, ethics and privacy issues that may surround the data sets

22. Must ensure that data access would be through an ethically developed governance framework and processes that clearly specify who has regular access to what data and reports and how non-standard requests are handled

THE BLOOD INFORMATION GOVERNANCE GROUP (BIGG)

TERMS OF REFERENCE

Version 3.0

March 2015

PURPOSE

The Blood Information Governance Group (BIGG) will ensure that the National Blood Authority (NBA) data and information is governed through a uniform and coordinated framework. The BIGG will guide the development of shared national data and information requirements for the management, benchmarking, cost and performance evaluation of the Australian blood sector.

The purpose of the BIGG is to:

- approve, oversee and contribute to the National Blood Sector Data and Information Strategy, the Blood Sector Scorecard and the NBA Blood Sector Data and Information Governance Framework
- contribute to the strategic priorities from the National Blood Sector Data and Information Strategy
- set and endorse the schedule of publications and approve the data and information for publication by the NBA
- provide relevant expertise and analysis of data and trends
- consider recommendations from internal and external IT System User Groups
- provide advice and recommendations for consideration by the NBA ICT Steering Committee on data requirements for system development, reporting applications and reporting priorities.

FUNCTIONS

The BIGG is to provide the NBA with consistent, timely and transparent recommendations on data and information:

- development (including metadata, models, data streams, data specifications and gap analyses)
- quality and validation
- access, oversight and control
- audit and compliance
- release and publication, noting the requirements of the Information Publication Scheme (IPS) and the *Privacy Act* (1988), and in accordance with the DIAM and the information framework agreements or other relevant agreements; and
- requirements for the blood sector, to guide and address sector needs, and to drive performance improvements through national reporting and benchmarking.

MEMBERSHIP

The chair and members will be appointed by the NBA General Manager. Appointments will be reviewed annually:

Position title	**Current occupant**
Executive Director – Fresh, Data and Clinical Development (Chair)	Sandra Cochrane
DGM Commercial Contracts and General Counsel	Michael Stone
Executive Director – Health Provider Engagement and CIO	Peter O'Halloran
Chief Finance Officer	Ashley Jackson
Two JBC Proxies	TBA

Other stakeholders and NBA staff will be made aware of meetings of the BIGG and may be invited as observers for meetings relevant to their work or expertise.

DUTIES OF THE CHAIR

The main role of the chair is to provide leadership to the BIGG, and to ensure that the BIGG carries out its functions effectively and efficiently.

The roles and responsibilities of the chair are as follows:

- Agree meeting agendas based on suggestions from the BIGG members and the needs of the NBA
- Direct the BIGG discussions to use time effectively to address critical issues
- Ensure that the BIGG functions within these Terms of Reference
- Obtain approval from the BIGG members for recommendations, noting that;
  - Ordinarily, decisions and recommendations of the BIGG will be achieved by consensus
  - Where consensus is not requested or cannot be achieved, both assenting and dissenting views are to be presented
- Forward recommendations to NBA teams and management as appropriate
- Present a summary of the BIGG's activities to the JBC as part of the General Manager's Update.

DUTIES OF MEMBERS

Members are to actively contribute to setting the Agenda for the BIGG meetings and give input or responses as agreed in meetings. The BIGG members are appointed to provide their expertise, advice and guidance in relation to the Data and Information team activities of the NBA. In undertaking their responsibilities, the BIGG members should:

- Participate in accordance with these Terms of Reference
- Actively contribute to setting the agenda for the BIGG meetings and give input or responses as agreed in meetings
- Contribute to the deliberations of the BIGG and prepare for scheduled meetings
- Respond to meeting action items as required

DUTIES OF INVITED OBSERVERS

Considering the complexity of the National Blood Sector Data and Information Strategy it will require a multidisciplinary approach and extensive consultative processes with a range of internal stakeholders. In light of this complexity, additional experts may be required. These experts may be invited to attend the BIGG meetings for the whole or part of a meeting, and provide their expert advice as required. They will not participate in any decision-making processes.

Requests for any additional experts will be agreed to by members of the BIGG prior to their involvement.

MEETINGS

The BIGG will normally meet quarterly for no more than 60 minutes. Irregular meetings may be convened as required by business needs. Out of Session work on items of a more granular nature may also be scheduled to address specific issues as they arise.

The Data and Information team will be responsible for the preparation of the agenda, collation and circulation of agenda papers and the minutes and action items arising from each meeting (made available on the NBA intranet).

Actions arising and decisions from the meeting will be prepared following each meeting, circulated out of session, and ratified at the next meeting.

DISPUTE RESOLUTION

In the event of a dispute arising between the members of the BIGG, the Chair of the BIGG will seek to resolve the dispute in the first instance. If this is unsuccessful, the issue will be referred to the NBA General Manager advising that agreement has not been reached and seeking advice.

APPENDIX 3: ABDR GOVERNANCE FRAMEWORK

Refer to http://www.blood.gov.au/abdr under 'ABDR/MyABDR Governance Arrangements'

APPENDIX 4: JURISDICTIONAL DATA COLLECTION ISSUES

Subject Matter	Issues
Agreements for the provision and collection of data and data sets	➢ What is the rationale for data collection and provision? ➢ How will data be used and published? ➢ Will the data be provided to third parties and what is the governance process for the third party? ➢ Will the data be linked to other data sets? ➢ What are the storage, archive and security requirements? ➢ What restrictions or obligations are required to be considered under the information framework agreements or other relevant agreement with stakeholders on how the data can be used and provided to third parties?
Freedom of Information	➢ Impediments to release i.e. could release of the data cause damage? ➢ What type of damage would result? ➢ If damage would result would this amount to an exemption under State or Territory FOI legislation? ➢ How does the Commonwealth intend to store, use and disclose this data in line with the sensitivities that may arise with the type of data concerned?
Privacy	➢ Does the data sought contain personal information? ➢ What is the purpose of the collection? ➢ Is the proposed purpose permitted? ➢ Does the data contain sensitive, health information or health records? ➢ If yes to either, has consent been granted for the proposed use or disclosure by the individual concerned? ➢ What kind of consent has been given (implied or express)? Is this sufficient in the jurisdiction concerned and for the type of data concerned? ➢ If no, how does the State and Territory legislation, the common law, guidelines or applicable administrative instruction impact on the ability of the jurisdiction to disclose or use that data in the manner suggested? ➢ What limits are there on the further use and disclosure of that data by the Commonwealth?
Copyright	➢ Is the work original in that it is not a mere copy? ➢ Is the work connected to Australia? ➢ If the answer is yes to all of these questions then copyright may subsist in the work concerned. Note that medical records may attract copyright, e.g. referral letters and consultation notes but not prescriptions and health summaries. ➢ Who owns the copyright in the work? ➢ Does the Commonwealth have permission to publish the data and if so what, if any, restrictions are required to be followed? ➢ Does the Commonwealth need to negotiate a licence (and/or sub-licence) to use, copy, publish, adapt or exploit the work?
Trademarks	➢ Does the data include a registered trademark under the *Trademarks Act 1995* (Cth)? (e.g.: logo, device, label, name etc.) ➢ If it does include a trademark did the owner authorise its use for the good or service concerned?

Subject Matter	Issues
Moral Rights	➢ Does the work have an author? ➢ If this is an authored work, need to consider when using the data how authors should be listed and in what order. ➢ Need to consider what concept of authorship should be used, consent of author to be included and whether a particular framework or policy should apply for determining this, e.g. *Uniform Requirements for Manuscripts Submitted to Biomedical Journals.* ➢ Does the work have a performer or director? ➢ If yes, has consent been granted for the proposed use or publication? (check the terms of any licence to use this material). ➢ Are there any requirements to attribute the performance of a work to the performer? (check the terms of any consent) ➢ If the work will be adapted or varied would this result in a material alteration of the performance that is prejudicial to the performer's reputation? (consent will resolve this issue)
Reputation protection/trade secrets and know how	➢ Was the data originally obtained from a business? ➢ If so is there 'goodwill' that may need to be protected here? ➢ Could the data be considered a trade secret, commercially valuable or know how – i.e. would a trader get an advantage over its competitors by obtaining data that is not generally known? ➢ Is the data essential for the profitability or viability of the business concerned? ➢ Would the proposed publication or use cause real or significant harm to the owner of the secret?
Contractual rights	➢ Did the data come from a party contracted by the jurisdiction? ➢ If so, who owns the data? ➢ If so, is there a contractual right that needs to be protected here? ➢ In particular consider whether there are obligations to maintain confidentiality and the nature of those obligations for specifically identified information and any intellectual or moral rights that may arise.
Confidentiality (contractual, common law or equitable requirements)	➢ Are there formal confidentiality arrangements in place protecting the data concerned? (check any formal agreements in place for the exchange of data including any arrangements made with the Commonwealth) ➢ Is the data in the document confidential? (it must be secret or only known to a limited group) ➢ Was the document provided and received on the basis of a mutual understanding of confidence? (the entity needs to have understood and accepted an obligation of confidence) ➢ Does the State or Territory have possession of the document or is it a third party document? ➢ Does the jurisdiction require an agreement or undertaking to be entered into before data is provided? ➢ Has an agreement been entered into with a third party seeking data to ensure confidentiality arrangements in place are protected? ➢ Taking into account any confidentiality obligations and laws, is the proposed disclosure authorised? ➢ Data should not be collected/provided if patient care and clinical safety of a patient is in any way compromised. ➢ Data collection will have no adverse impact on core clinical care duties, budget and resources of health service providers.

Subject Matter	Issues
Ethical requirements	➢ When the patient/clinical data was collected, was informed consent obtained to share the data for the particular purpose or to share it more broadly? (Note: even personal sensitive data can be shared if consent has been obtained and if suitable procedures, precautions and safeguards are followed) ➢ Does that consent to use or disclose the data include the consent of third parties – such as data from or about other identifiable family members or data that may be culturally significant to a particular section of the community? ➢ What limits on future use or data sharing exists for the data? (Note that any specific agreements made with individuals must be fulfilled) ➢ Would anonymous data be sufficient to meet the required use or disclosure? ➢ If anonymous data would be sufficient how should it be anonymised? (e.g. removing name and address; aggregating data; using pseudonyms; removing rare or small numbers where needed) ➢ If the data is not anonymised who can have access to the data and how should it be stored and protected? (database systems; access controls, particular confidentiality arrangements) ➢ If the data is sensitive, does the jurisdiction require a restrictive licence to be in place for the Commonwealth's proposed use or disclosure? ➢ Is there an ethics committee that must consider the data sharing prior to approval being granted? (particularly the case for micro level data such as patient information). ➢ If there is an ethics committee what is the internal process and/or forms, evidence required for that particular committee? (see for example list of Human Research Ethics Committees (HRECs) at http://www.nhmrc.gov.au/health-ethics/human-research-ethics-committees-hrecs/human-research-ethics-committees-hrecs for human research) ➢ If the data relates to human research does the proposed use or disclosure align with the particular arrangements in place for protecting the privacy of individuals? ➢ Does the jurisdictional entity require an undertaking that the NBA will not attempt to re-identify material or information to protect the privacy or confidentiality of data? ➢ Does the data request relate to a research proposal? If so, has this been communicated to the jurisdiction including any details about the research proposal required under the *National Statement on Ethical Conduct in Human Research (2007)*? ➢ Does the data request include unique patient identifiers?

APPENDIX 5: COMMONWEALTH DATA GOVERNANCE FRAMEWORK

Subject Matter	Governance Framework	Summary of relevant obligations	Interaction with State and Territory obligations
Freedom of Information	*Freedom of Information Act 1982* (Cth)	**Information Publication Scheme** - requires agencies to publish – generally on the agency website – an information publication plan (agency plan), describing what the agency proposes to publish and how the information will be made available. The scheme specifies nine classes of information that must be published and provides for agencies to publish additional information. Exempt material is not required to be published. **Request for access -** Any person has the right to apply for access to a document of an agency or an official document of a minister (subsection 11(1)). A document in the possession of the NBA will be a document of the agency for the purposes of the FOI Act. A person may also make a request to an agency for access to a document held by a contractor or subcontractor relating to the performance of a 'Commonwealth contract'. **Disclosure log -** NBA must publish information that has been released in response to each FOI access request received, subject to certain exceptions, including where the document is exempt under the Act (section 11C). **Amendment -** individuals may seek amendment or annotation of their own personal information in a record held by an Agency (section 48).	Each State and Territory has its own FOI legislation. Although each has a scheme enabling requests for access to documents, exemption provisions are not always consistent with the Commonwealth Act. Commonwealth and jurisdiction legislation include provisions relating to consultation. The NBA will consult with a jurisdictional entity where a request is received under the FOI Act for documents obtained from that entity prior to making any decision on release or publication of material.
Privacy and ethics	*Privacy Act 1988* (Cth) *The National Statement on Ethical Conduct in Human Research* (2007) *Healthcare Identifiers Act 2010* (Cth) (HI Act)	The Commonwealth is required to meet the Australian Privacy Principles (APPs) in section 14 of the *Privacy Act 1988* (Cth) with respect to the collection, storage, use and disclosure of personal information. The NBA will: • have an up to date privacy policy • give individuals the option of not identifying themselves, or of using a pseudonym, when dealing with the agency in relation to a particular matter • meet additional constraints on collection, use and disclosure of sensitive information and proscriptive requirements about the content of collection notices • notify individuals where there will be an overseas disclosure and	The intention of the *Privacy Act 1988* (Cth) is not to override or affect the operation of State or Territory law where it can operate concurrently (see section 3). The principles under Cth law are not identical to the jurisdictions and therefore there are inconsistencies across the jurisdictions.[5] **Public Sector:** Most have enacted legislation to govern the handling of personal information and some such as NSW and VIC have additional or specific legislation that governs the handling of health information. QLD has legislative protections for health information. SA and WA have no legislative privacy regime in place at present rather; privacy is governed via administrative arrangements. In VIC and ACT additional privacy rights

[5] Those inconsistencies are dealt with in ALRC Report 108 *For Your Information: Australian Privacy Law and Practice*, 12 August 2008.

Subject Matter	Governance Framework	Summary of relevant obligations	Interaction with State and Territory obligations
		increased accountability for the NBA with such disclosures. The HI Act imposes security obligations on any entity holding a healthcare identifier to protect it from misuse or loss. Furthermore, there are significant penalties for the unauthorised use or disclosure of a healthcare identifier. Contravention of the HI Act or *the Healthcare Identifiers Regulations 2010* may also be considered a breach of privacy under the *Privacy Act*.	are recognised via broader human rights legislation or charters. Local governments and private universities are also regulated in some jurisdictions but not in others. **Private Sector:** Private sector organisations (including non-profit organisations) with an annual turnover of more than $3M and private health service providers in each of the jurisdictions are governed by the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth). Some businesses under $3M are also obliged to meet the Cth requirements. **Common law:** Queensland is the only jurisdiction in Australia that has unequivocally recognised the existence of a tort of invasion of privacy, albeit only at the level of the District Court, in Grosse v Purvis [2003] QDC 151 (related to allegations of ongoing and significant stalking). The Australian Law Reform Commission (ALRC) in its 2008 report (ALRC 108 – For Your Information: Australian Privacy Law and Practice) recommended the establishment of a statutory cause of action for serious invasions of privacy. In September 2011, the Commonwealth Department of the Prime Minister and Cabinet released an Issues Paper on 'A Statutory Cause of Action for Serious Invasion of Privacy', seeking public submissions. At this point the Commonwealth has not yet announced what action, if any, it intends to take in relation to this. Given the various arrangements that apply it is important to maintain open lines of communications with the jurisdictions to ensure individual State and Territory requirements are met.
Secrecy provisions	Secrecy provisions in Commonwealth legislation are many and varied. ALRC Report 112 *Secrecy Laws and Open Government in Australia* identified 506 secrecy provisions in 176 pieces of primary and subordinate legislation as at 11 November 2009. Eg: *National Health Act 1953*	A secrecy provision is any provision in primary or subordinate legislation which imposes secrecy or confidentiality obligations relating to the handling of Commonwealth information. Generally secrecy provisions provide a relatively prescriptive framework regarding how certain types of information are to be handled. These secrecy provisions often outline the obligations imposed upon an individual officer within an agency regarding their handling of particular information in the course of an agency carrying out its activities and functions. Sanctions, including criminal sanctions, which impose individual responsibility upon an officer are contained in both general secrecy provisions such as the *Crimes Act 1914* (Cth) as well as provisions that protect specific types of Commonwealth information.	Some jurisdictions have secrecy provisions in place which govern the handling of information in certain circumstances. Cth secrecy provisions may also apply to State and Territory employees where information protected by a secrecy provision is acquired as a result of their employment. Given the consequences for individual officers it will be essential to deal with issues relating to secrecy provisions on a case by case basis.

Subject Matter	Governance Framework	Summary of relevant obligations	Interaction with State and Territory obligations
	(Cth); *Social Security (Administration) Act 1999* (Cth), *Health Insurance Act 1973* (Cth)	Can deal with any information or alternatively, confidential, personal, commercial or investigations information often related to matters such as taxation, health and social services, law enforcement and finance.	
Confidentiality considerations		Any publication or release of data must be considered against confidentiality arrangements. Confidential information must be specifically identified prior to communicating any data so that it can be adequately protected.	States and Territory entities are likely to have their own obligations around confidentiality (as indicated above at Appendix 4). Issues of confidentiality should be dealt with on a case by case basis. A party receiving a request for information should consider their own confidentiality obligations (including any obligations at contract) and ensure these are communicated and protected prior to releasing any data.
Court ordered production - subpoena, notice to produce[6], discovery, warrant	The Federal Courts and Tribunal have rules that govern Court ordered production.	Although procedural rules vary depending on the forum concerned general principles apply to court produced documents. Some relevant general principles to take into account when considering obligations to produce include: • relevance of the documents sought to the issue in dispute • whether subpoena is issued in the proper form • whether documents sought are only relevant to the credibility of individuals in circumstances where credibility is not relevant • whether production would be oppressive i.e.: documents are not specified with any reasonably particularity or it calls for production of a large amount of material not relevant to the actual proceedings • would answering the subpoena result in a breach of secrecy provisions in an enactment • do the documents include privileged material (e.g. contained legal advice) • does the subpoena amount to discovery or a mere fishing exercise to see if there is any case at all?	As at the Federal level State and Territory Courts and Tribunals have rules and govern Court ordered production. It will be essential to consider the particular rules of the Court or Tribunal. However, the general principles remain relevant to the jurisdictions.

[6] In some jurisdictions one party to a proceeding can give another a notice to produce which has the same coercive effect as a subpoena.

Subject Matter	Governance Framework	Summary of relevant obligations	Interaction with State and Territory obligations
Government Policy and legislation relating to security of Commonwealth information	Protective Security Policy Framework	Several policies that operate across the Australian Government apply to personnel security, information security and physical security. Of particular relevance are the Protective Security Manual and the Australian Government Information and Communications Technology Security Manual (ACSI 33). Some general principles that should guide the NBA when considering information or data security are: • the availability of information should be limited to those who need to use or access the information to do their work (the 'need to know' principle) • where the compromise of information could cause harm to the nation, the public interest, the government or other entities or individuals, agencies must consider giving the information a security classification • once information has been identified as requiring security classification, a protective marking must be assigned to the information; and • once information has been security classified, agencies must observe the minimum procedural requirements for its use, storage, transmission and disposal of that information. The combined effect of sections 70 and 79 of the *Crimes Act 1914* and section 91.1 of the *Criminal Code Act1995* is that the unauthorised disclosure of information held by the Australian Government is subject to the sanction of criminal law.	The Commonwealth is required to implement the PSPF when sharing information with State and Territory Governments. The Commonwealth expects that State and Territory government agencies that hold or access national security classified information will apply the PSPF. The NBA is responsible for ensuring that these obligations are understood by jurisdictional counterparts. This obligation will be reflected in the Data and Information Agreements in place with States and Territories. In turn, the NBA is required to treat information provided by other governments in accordance with agreements or administrative arrangements in place between the parties concerned. The NBA will enter into MOUs or legal agreements (as required) with other agencies when regularly sharing information.
Intellectual Property and moral rights	*Statement of IP Principles for Australian Government Agencies* (IP Principles) *Copyright Act 1968* *Trade Marks Act 1995* *Designs Act 2003* *Patents Act 1990*	IP rights exist in many forms and in some cases do not need to be registered in order to be protected (eg copyright). Moral rights (in addition to IP) also exist which are personal rights protecting the integrity and right of attribution of the creator granted under the *Copyright Act 1968.* These rights cannot be assigned or licensed, but consent can be given to acts that would otherwise constitute infringement of the rights. The IP Principles require development and implementation of appropriate measures for identifying and recording the IP that Commonwealth agencies create, use or manage. They also require the development and implementation of agency policies to appropriately protect such IP. The NBA is in the process of developing a governance framework, including a comprehensive policy, for managing IP. The NBA is currently assessing its information holdings with a view	See Appendix 4 for specific issues relating to IP for States and Territories. The issues raised for States and Territories also apply to Cth data.

		to applying consistent licensing across its holdings. When considering whether to share Cth IP the NBA is required to consider: • Whether sharing the IP will compromise agency operations (e.g. loss of operational benefits or missed opportunities to commercialise IP) • compromise the protection of IP • inhibit the exploitation of IP (e.g. appropriate commercialisation), or • increase the risk of misuse of IP (e.g. use of IP in a way that is inconsistent with any licence conditions) • any costs or increase in risks to the NBA.	

APPENDIX 6: DATA REQUEST FORM

Data Request Form		
Request Number	(Office Use Only):	
Date Requested	Date:	
Requestor details		
Name of requestor	First name:	Last name:
Email address		
Phone number	( )	
Organisation		
Role of requestor		
Organisation type (please tick)	☐ Australian government	☐ State/territory government
	☐ Commercial sector/private company	☐ Policy advisor
	☐ Health provider	☐ Researcher/academic
	☐ General public	☐ Other *(please specify):*
Postal address (optional)	Street address/PO Box:	
	Suburb:	
	City:	
	State:	
	Post code:	
Data request details		
Describe the specific dataset or information that you are seeking (include data variables/questions of interest) ***If you wish to attach a document with details of your information/data needs, please provide the attachment***		
What is the purpose of your request? (include details of the project you are undertaking and who you are undertaking this for; whether your request is authorised or permitted by or under law and if so which law; any justification for requiring health information or other sensitive information attributable to an individual rather than anonymised or aggregated data)		
Please describe what the data will be used for		
Please describe any likely disclosures of that data including who it will be disclosed to and whether it will be disclosed to any overseas parties (include the likely countries of such disclosure)		
Date data required by	*ddmmyyyy*	

Describe how you would like the data to be provided e.g. tables in an MS Word document, comma delimited (CSV) format, Excel file
Storage and protection of data
Describe how the data will be stored
Platform type (server): **Host:** **What if any contract is in place with that host?** **Is the host required to comply with the following relevant laws or policies (or similar laws or policies that include the same types of requirements around security of information, privacy and ethics)? As relevant here the Protective Security Policy Framework (PSPF)?** **Location of server:** **Is cloud computing used by the Party?** **Does the server concerned provide redundancy (backup), disaster recovery, security and is it Information Security Manual Compliant (ISM)?** **What access controls are in place to ensure the confidentiality and integrity of the server where the data will be stored?**
Will any third parties including contractors or sub-contractors have access to this data set? If yes specify who and confirm that they are required to comply with this agreement.
What steps are taken by your organisation to ensure that the data will be appropriately stored and protected from unauthorised access?

Retention of data		
What is the requirement that applies for retaining the requested data? If this is considered to be a record what is the time period that will apply for retention and how will it be disposed of once that retention period is satisfied?		
Release of data		
Will the data be publically released?	☐ Yes	☐ No
If the data is to be publicly released, why (include for what purpose)?		
Is it possible to release aggregated/anonymised or de-identified data? If no – why?		
Will the data analyses and results be publically released?	☐ Yes	☐ No
Please describe how the data will be released (For example, the format, publication type, intended audience, etc).		
Please describe who will use or have access to this information within your organisation and if it will be used by subcontractors how the data will be governed.		

Conditions of data release	
Please note that data is made available with the following conditions and by signing the contract, the user acknowledges and agrees to the following: • Data is released subject to satisfying confidentiality and quality considerations • NBA must be acknowledged in all published material which uses the data requested • Footnotes and other caveats accompanying data tables must be replicated as provided when data is reproduced, whether in full or in part • The data will not be used for any purpose other than that specified in the approved request • The data released remains the property of the NBA • The data must not be used, published or disseminated in a way that might enable the identity of individual patients or the service profiles of individual doctors or hospitals to be ascertained • Data files are to be maintained and stored in a secure manner in an environment where they cannot be linked (either electronically or by personal inspection) with other records and they must be stored on-shore in the organisation's own ICT controlled infrastructure or in a private cloud • If data files are made available to third parties engaged by the recipient then the consultants must also agree to these conditions • Additional conditions may apply to specific data sets	
I have read and accept these conditions ☐	
Signature:	
Name of Recipient:	Date: *ddmmyyyy*

Internal use only		
Action required		
Canned report	☐ Yes ☐ No	
If no, provide process		
Timeline to provide data		
Approval to provide data		
Priority	(H/M/L):	
Resources allocated		
Report Parameters		
Parameters		
Date range		
Report/extract details (Data releases in response to data requests will be provided with guidance on the data sources, collection methods, distribution requirements and quality assurance and approval process)		
Checklist completed		
Approved by		
Date approved	*ddmmyyyy*	
Date provided	*ddmmyyyy*	

APPENDIX 7: EXAMPLE INFORMATION FRAMEWORK AGREEMENT

When the NBA is providing record data to, or collecting data from stakeholders and third parties, an information framework agreement or other relevant agreement must be developed and implemented. The agreements ensure the confidentiality and security of the data.

These will be established with each state and territory as an overarching document with schedules for each data set provided or collected and will include, core obligations, confidential information, intellectual property rights, personal information obligations, moral rights, personnel, copyright, ownership, and the schedule will include publication obligations, acknowledge obligations, rationale for collection, use, storage and archiving requirements. An example of a generic information framework agreement and Schedule is below. Each state and territory will have their own agreement with the NBA and the NBA will meet the obligations as agreed.

The following elements must be outlined within the schedule to the agreement to ensure the following are in accordance with Commonwealth, NBA and state and territory requirements:

- ownership of data
- storage and security of data
- retention and disposal of data
- audit requirements
- disposal of data after the agreement expires
- access arrangements within the third party
- disclosure arrangements.

EXAMPLE – GENERIC

INFORMATION FRAMEWORK AGREEMENT

between the

COMMONWEALTH OF AUSTRALIA
as represented by the
National Blood Authority

and

[Enter the appropriate party that has authority to enter into this arrangement on behalf of the jurisdiction]

For

Data Exchange and Sharing

INFORMATION FRAMEWORK AGREEMENT

Between the

Commonwealth of Australia ('the Commonwealth'), acting through the **National Blood Authority** ABN 87 361 602 478 ('the NBA');

and

[Enter the appropriate party that has authority to enter into this arrangement on behalf of the jurisdiction in full, including address and ABN]

Purpose

1. The NBA and the Jurisdiction ('the Parties') wish to agree on a framework of standing obligations which are to be applied to information of a confidential, sensitive or personal nature provided between them in the course of carrying out their respective roles as stakeholders under and in connection with the national blood arrangements established in accordance with the National Blood Agreement as defined in section 3 of the *National Blood Authority Act 2003* (Cth).

2. It is intended that this agreement will replace the Information Framework Agreement agreed between the Parties on [If there is a previous agreement in place with the Commonwealth note that here].

Legal Basis

3. In pursuing the primary policy objectives of Governments' under the National Blood Agreement the NBA must have regard to undertaking national information gathering, monitoring of new developments, reporting and research in relation to the Australian blood sector. This objective aligns with the NBA's function under paragraph 8(1)(a) of the *National Blood Authority Act 2003* ('NBA Act') which requires the NBA to liaise with and gather information from governments, suppliers and others about matters relating to blood products and services.

4. The NBA is bound to protect personal information (including health information) in accordance with the *Privacy Act 1988* (Cth) ('Privacy Act'). This includes the need to consider any requests for data for research purposes in line with the National Health and Medical Research Council (NHMRC) Guidelines under section 95 of the Privacy Act for the protection of privacy in the conduct of medical research. The NBA is also required to protect sensitive government information in accordance with the Protective Security Policy Framework (PSPF).

5. In addition to legislated obligations the NBA is also required to comply with a Data Governance Framework agreed by the Jurisdictional Blood Committee which sets out the governance principles and arrangements for the NBA's own management of data and information, and for the NBA's dealings with stakeholders in the blood sector including State and Territory Governments.

6. The Jurisdiction also has obligations in relation to personal information and health information. The Jurisdiction will only disclose data to the NBA in line with its responsibilities. A list of relevant legal and policy obligations to which the Jurisdiction must comply are included at Schedule 2 (Jurisdiction Obligations) to this agreement.

7. The Parties intend to act in accordance with this agreement however; they acknowledge that, this agreement does not create legally enforceable obligations.

8. Additionally, the Parties agree to consult with each other on any, legislative or policy changes that may have implications for the core obligations of each party under this agreement.

Interpretation

9. In this agreement unless the contrary intention appears:

'**confidential information**', being information that is by its nature confidential and either:

a) is specified by a Party as confidential prior to or at the time of disclosure either via Schedule 1 or otherwise (however, if a period of confidentiality is specified, this information is Confidential Information only for that period); or,

b) is agreed by the Parties in writing to be Confidential Information for the purposes of this agreement (however, if a period of confidentiality is specified, this information is Confidential Information only for that period);

but does not include information which:

c) is or becomes public knowledge other than by failing to comply with this agreement, breach of any other confidentiality obligation, or any other unlawful means; or,

d) is in the possession of either Party without restriction in relation to disclosure before the date of receipt from either Party;

'Intellectual Property' includes all copyright (including rights in relation to phonograms and broadcasts), all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trade marks (including service marks), registered and unregistered designs, circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields;

'Material' includes documents, equipment, software (including source code and object code), goods, information and data stored by any means to which this agreement applies;

'**Moral Right**s' means rights of integrity of authorship, rights of attribution of authorship, rights not to have authorship falsely attributed, and rights of a similar nature conferred by statute that exist, or may come to exist, anywhere in the world;

'Sensitive Government Information', including without limitation information which is, or may reasonably be expected to be, sensitive for the government of the Commonwealth of

Australia or any Australian government for policy, security, operational, financial or legal reasons.

Scope of Information

10. This agreement applies to all information provided by the NBA to the Jurisdiction or by the Jurisdiction to the NBA within the following categories:

    a) Confidential Information;

    b) Sensitive Government Information;

    c) personal information, within the meaning of that phrase in the *Privacy Act 1988* (Cth) but which for the purposes of this agreement includes deceased persons where that information is covered by the privacy legislation and/or policies and health record legislation and/or polices which operate in the Jurisdiction;

and includes all information which the disclosing party has identified, or has notified the receiving party as being, Confidential Information, Sensitive Government Information or personal information (including health information) whether set out specifically in Schedule 1 or otherwise.

11. This agreement applies to information defined in clause 10 in any material form including written, oral or electronic.

12. This agreement applies to information defined in clause 10 given by any representative of the disclosing party, including without limitation the General Manager, Chief Executive, a Board or committee member, or any other employee or officer of the Party, or any consultant or agent on behalf of the Party.

13. This agreement applies to information defined in clause 10 given to any representative of the receiving Party, including without limitation the General Manager, Chief Executive, a Board or committee member, or any other employee or officer of the Party, or any consultant or agent on behalf of the Party.

14. The Parties also intend this agreement to apply to information specified by a Party in writing as being governed by this agreement despite it falling outside the categories defined in clause 10.

Core Obligations

[Please note that the clauses in this agreement are designed to be a starting point for further discussion. Although the objective is to deliver consistency nationally, clauses should be updated to ensure that more stringent obligations of the jurisdiction are captured where relevant.

Please note any particular requirements you have in the various sections for Commonwealth consideration.

If you have policy which applies but which is not publicly available we ask that you provide it so that we can work closely with you to draft appropriate clauses to meet your obligations.]

15. Each Party agrees to ensure that information to which this agreement applies is dealt with in accordance with any applicable legal or administrative restrictions, requirements or procedures which apply to that Party from time to time (including within the Australian Commonwealth public sector or Jurisdiction's public sector, as relevant) to Confidential Information, Sensitive Government Information or personal information, including in relation to classification, handling, storage, collection, use, disclosure or disposal of such information. For the avoidance of doubt, this includes the requirements set out in the Commonwealth PSPF.

16. Each Party agrees to comply with any legal or administrative restrictions, requirements or procedures (in addition to restrictions, requirements or procedures referred to in clause 15 which apply to the disclosing party in relation to information to which this agreement applies, where the disclosing Party has identified in writing that such restrictions, requirements or procedures apply to the information at the time the information is given to the receiving Party.

17. Each Party agrees to consult with the other Party in the event that a document to which this agreement applies is sought prior to any decision being made for access in accordance with relevant Freedom of Information legislation applying to that Party.

Confidential Information

18. Each Party agrees not to disclose to any person, other than the other Party, any Confidential Information without prior written consent from the other Party (which consent will not be unreasonably withheld or delayed).

19. In giving consent under clause 18 a Party may impose any reasonable conditions or restrictions it considers appropriate, and the other Party agrees to comply with such conditions or restrictions.

20. Notwithstanding clause 18 a Party may disclose Confidential Information if the Confidential Information is:

    a) disclosed to its advisers or personnel solely in order to comply with this agreement;

    b) disclosed to internal management personnel, solely to enable effective management or auditing of activities related to this agreement;

    c) disclosed by a Party to its responsible Minister or to Cabinet;

    d) disclosed by a Party in response to a request by a House or a Committee of the Parliament of the Commonwealth of Australia or the Government of [Insert jurisdiction]; or,

    e) authorised or required by or under an Australian law.

21. Where a Party discloses Confidential Information under clause 20 the Party must inform the recipient of the other Party's claim that the information disclosed is confidential.

22. Nothing in this section derogates from any obligation which either Party may have either under relevant privacy legislation or policy as amended from time to time, or under this agreement, in relation to the protection of Personal Information.

Personal Information

23. With respect to personal information the Parties agree in particular to:

a) take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and protected from misuse, interference, loss, unauthorised access, modification or disclosure;

b) only collect, use and disclose personal information to which this agreement applies in accordance with the primary purpose that it was disclosed unless the disclosing party is notified and:

(i) consent (whether express or implied) of the relevant individual is obtained;

(ii) the individual would reasonably expect the Party to use or disclose the information for the secondary purpose and the secondary purpose is:

- if the information is sensitive information as defined by the Privacy Act —directly related to the primary purpose; or
- if the information is not sensitive information—related to the primary purpose; or

(iii) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;

(iv) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure and the Party reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;

(v) the Party has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and the party reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter;

(vi) the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim;

(vii) the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

c) take steps (if any) that are reasonable in the circumstances to ensure that personal information that the entity collects and discloses is accurate, up to date and complete.

Intellectual Property Rights

[Please note that the IP clauses reflect a general approach which can be varied on a case by case basis depending on the nature of the data being provided. See Part B of Schedule 1.]

24. Subject to clauses 25, 26 and 27, nothing in this agreement affects ownership of:

a) any Intellectual Property rights in information to which this agreement applies; or

b) any Intellectual Property rights in a Party's pre-existing Material.

25. A disclosing Party must only provide information to the other Party under this agreement where:

a) the Party owns the Intellectual Property rights in the Material; or

b) the owner of the Intellectual Property rights in the Material has consented to the disclosure.

26. Unless otherwise agreed between the Parties, including via Part B of Schedule 1, the Jurisdiction grants to the NBA a perpetual, licence-fee free, non-exclusive licence to use, reproduce, adapt, distribute, publish, exploit and communicate Material provided under this agreement for non-commercial Commonwealth purposes.

27. Unless otherwise agreed between the Parties, including via Part B of Schedule 1, the NBA grants the Jurisdiction a perpetual, licence-fee free, non-exclusive licence to use, reproduce, adapt, distribute, publish, exploit and communicate Material provided by the NBA under this agreement for non-commercial Government of [Insert jurisdiction] purposes.

Moral Rights

28. For the purposes of this clause, 'Specified Acts', in relation to particular Material, means the following classes or types of acts or omissions performed by or on behalf of a Party to this agreement:

a) those which would, but for this clause, infringe an author's right of attribution of authorship or the author's right of integrity of authorship,

but does not include:

b) those which would infringe the author's right not to have authorship falsely attributed.

29. The disclosing Party agrees to ensure that:

a) the author of any Material, has given or will give a written consent to the Specified Acts (whether occurring before or after the consent is given) which is given expressly for the benefit of the recipient Party; or,

b) any requirement to maintain an author's right of attribution of authorship or an author's right of integrity of authorship is notified to the recipient Party including the requirements around that attribution.

Personnel

30. Each Party agrees to ensure that officers, employees, consultants, contractors, sub-contractors or agents are only able to access, use or deal with information to which this agreement applies where the officers, employees, consultants, contractors or agents perform a function in that Party which is relevant to the performance of the disclosing Party's role as referred to in clause 1 of this agreement, or where the officers, employees, consultants, contractors or agents perform a function which is relevant to the administration of the restrictions, requirements or procedures referred to in clauses 15 and 16.

31. Each Party agrees to establish and maintain reasonable legal or administrative policies and procedures to ensure that officers, employees, consultants, contractors, subcontractors or agents of that party having access to information to which this agreement applies, are aware of and comply with the restrictions, requirements or procedures referred to in clauses 15 and 16.

Requests for information

32. Each Party agrees to provide the other Party with information or copies of documents in relation to any restrictions, requirements or procedures referred to in clauses 15 and 16 as the other Party may reasonably request from time to time.

33. The Parties agree that any request for information under this agreement will be accompanied by Part A of the Data Request Form in Schedule 1 to this agreement.

34. For the avoidance of doubt, the Parties acknowledge that Part B to the Data Request Form at Schedule 1 to this agreement may include additional obligations required by a disclosing Party for a specified data set including with respect to any particular conditions, restrictions, requirements or procedures referred to in clauses 15 and 16.

35. For the avoidance of doubt, Part B to the Data Request Form at Schedule 1 to this agreement may also vary the terms of the Intellectual Property licence described in clauses 25 to27 of this agreement for the particular data set concerned.

Apparent legal requirement to disclose

36. If a Party becomes aware of any apparent legal requirement on it to disclose information to which this agreement applies, it agrees, to the extent that it is properly able to do so, to:

a) notify the other Party of the apparent legal requirement as soon as possible; and,

b) take into account the views of the other Party in relation to any action in response to the apparent legal requirement.

Return of information

37. Subject to any applicable legal or administrative restrictions or requirements of the Parties, as relevant, if information to which this agreement applies is no longer required by a Party, the Party undertakes to return any Material containing that information to the other Party, or to dispose of that Material in a manner acceptable to the other Party.

Term of Agreement

38. The Parties agree that:

a) this agreement commences upon the date of the last party to sign; and

b) continues until it is terminated by any Party giving notice to that effect in writing to the other Party.

Effect of termination

39. The Parties agree that a notice provided under clause 38(b) may include conditions, including the return or disposal of information to which this agreement applies and any particular process around that return or disposal.

40. A Party issuing a notice under clause 38(b), agrees to consult about any conditions that may be applicable prior to issuing the notice.

41. Notwithstanding termination, the Parties agree that the obligations set out in this agreement continue to apply to information provided by a Party under this agreement for as long as that information falls within one of the categories listed in clause 10.

SIGNED for and on behalf of [Enter the appropriate party that has authority to enter into this arrangement on behalf of the jurisdiction])

by)

……..)

who is duly authorised in that regard in the presence of:)

……..
Signature of Witness

……

Name of Witness

……..
Date

……..
Signature of Authorised Officer

SIGNED on behalf of the Commonwealth)

acting through)

NATIONAL BLOOD AUTHORITY)

ABN 87 361 602 478 on:)

)

_____ __)

Date)

by:)

)

_____) _____

Name of signatory) *Signature*

)

_____)

Position of signatory)

Schedule 1 (Data Request Form)

PART A – DATA REQUEST

Recipient/Requestor details		
Name of representative of requesting Party	First name:	Last name:
Email address		
Phone number		
Organisation		
Role of representative of requesting Party		
Postal address	Street address/PO Box:	
	Suburb:	
	City:	
	State:	
	Post code:	
Data request details		
Describe the specific dataset or information that you are seeking (include data variables/questions of interest) ***If you wish to attach a document with details of your information/data needs, please provide the attachment***		
What is the purpose of your request? (include details of the project you are undertaking and who you are undertaking this for; whether your request is authorised or permitted by or under law and if so which law; any justification for requiring health information or other sensitive information attributable to an individual rather than anonymised or aggregated data)		
Please describe what the data will be used for		
Please describe any likely disclosures of that data including who it will be disclosed to and whether it will be disclosed to any overseas parties (include the likely countries of such disclosure)		

Date data required by	

Describe how you would like the data to be provided e.g. tables in an MS Word document, comma delimited (CSV) format, Excel file

Storage and protection of data

Describe how the data will be stored

Platform type (server):

Host:

What if any contract is in place with that host?

Is the host required to comply with the following relevant laws or policies (or similar laws or policies that include the same types of requirements around security of information, privacy and ethics)? As relevant here the Protective Security Policy Framework (PSPF)?

Location of server:

Is cloud computing used by the Party?

Does the server concerned provide redundancy (backup), disaster recovery, security and is it Information Security Manual Compliant (ISM)?

What access controls are in place to ensure the confidentiality and integrity of the server where the data will be stored?

Will any third parties including contractors or sub-contractors have access to this data set? If yes specify who and confirm that they are required to comply with this agreement.

What steps are taken by your organisation to ensure that the data will be appropriately stored and protected from unauthorised access?

Retention of data
What is the requirement that applies for retaining the requested data? If this is considered to be a record what is the time period that will apply for retention and how will it be disposed of once that retention period is satisfied?
Release of data

Will the data be publically released?	☐ Yes	☐ No
Will the data analysis and results be publically released?	☐ Yes	☐ No

Please describe how the data or analysis/results will be released (For example, the format, publication type, intended audience, etc.).
If the data is to be publicly released, why (include for what purpose)?
Is it possible to release aggregated/anonymised or de-identified data? If no – why?

PART B - Conditions of data release – Disclosing Party Requirements

The release of the data in this request is subject to the requirements set out in the *Information Framework agreement* between the Commonwealth of Australia as represented by the National Blood Authority and the [Enter the appropriate party that has authority to enter into this arrangement on behalf of the jurisdiction] dated [Enter Date] and the following restrictions/requirements:

- Intellectual Property:

Note any variation to clauses 26-27 which apply to the specified data set concerned.

- Moral Rights:

Note any particular requirements around attribution that must be followed by the recipient.

- Confidential Information:

Specify whether the particular data set is or parts of the data set sought are Confidential Information for the purposes of this agreement. Include any particular requirements around storage, mechanics of disclosure to the recipient Party.

- Personal Information:

Specify whether the data set is considered to be personal information and whether any particular additional requirements apply to that data particularly if it is health or sensitive information. For example, the data must not be used, published or disseminated in a way that might enable the identity of individual patients or the service profiles of individual doctors or hospitals to be ascertained OR that any publications must not identify individual persons or hospitals where express consent for release by those persons/hospitals has not been given.

- Miscellaneous:

Specify any additional restrictions or conditions that apply to the specified data set in accordance with clause 16 of the agreement.[see below for examples]

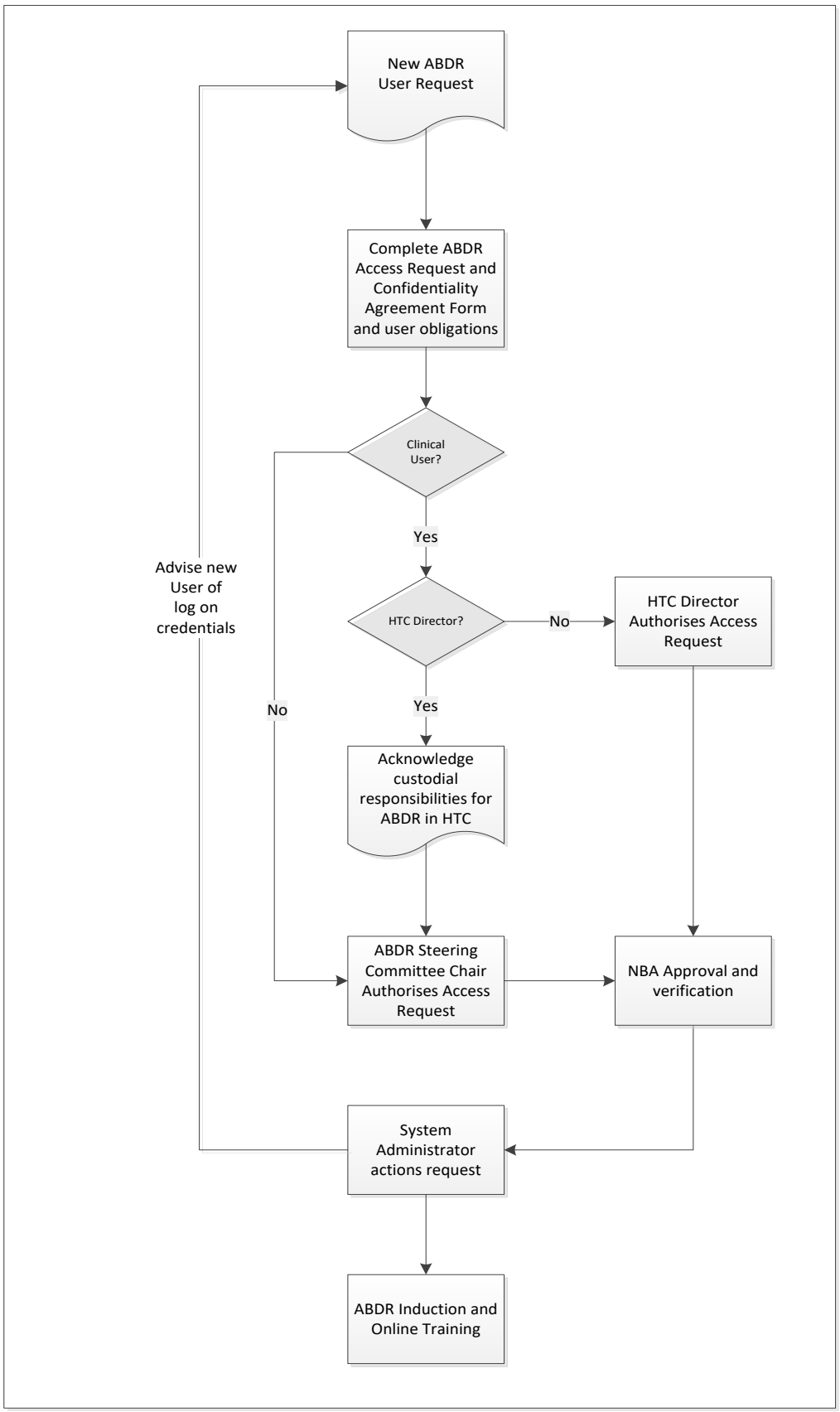
- The disclosing Party must be acknowledged in all published Material which use the specified data requested.
- Footnotes and other caveats accompanying this data set must be replicated as provided when the data set is reproduced, whether in full or in part.
- The data set must not be used for any purpose other than that specified in the approved request or as authorised by this agreement.
- The data released remains the property of the disclosing Party
- The specified data set and any associated Material derived from that data set must be maintained and stored in the following manner: [e.g. a secure manner in an environment where they cannot be linked (either electronically or by personal inspection) with other records].
- The data set must be stored on-shore in Australia in the recipient Party's own security protected ICT controlled infrastructure.
- In addition to the documents listed at Schedule 2 to the agreement the following additional legal or policy obligations apply to this data set: [ ]

I have read and accept these conditions as an authorised officer on behalf of [ ] ☐	
Signature:	
Name and role of Authorised person on behalf of recipient Party:	Date: *ddmmyyyy*

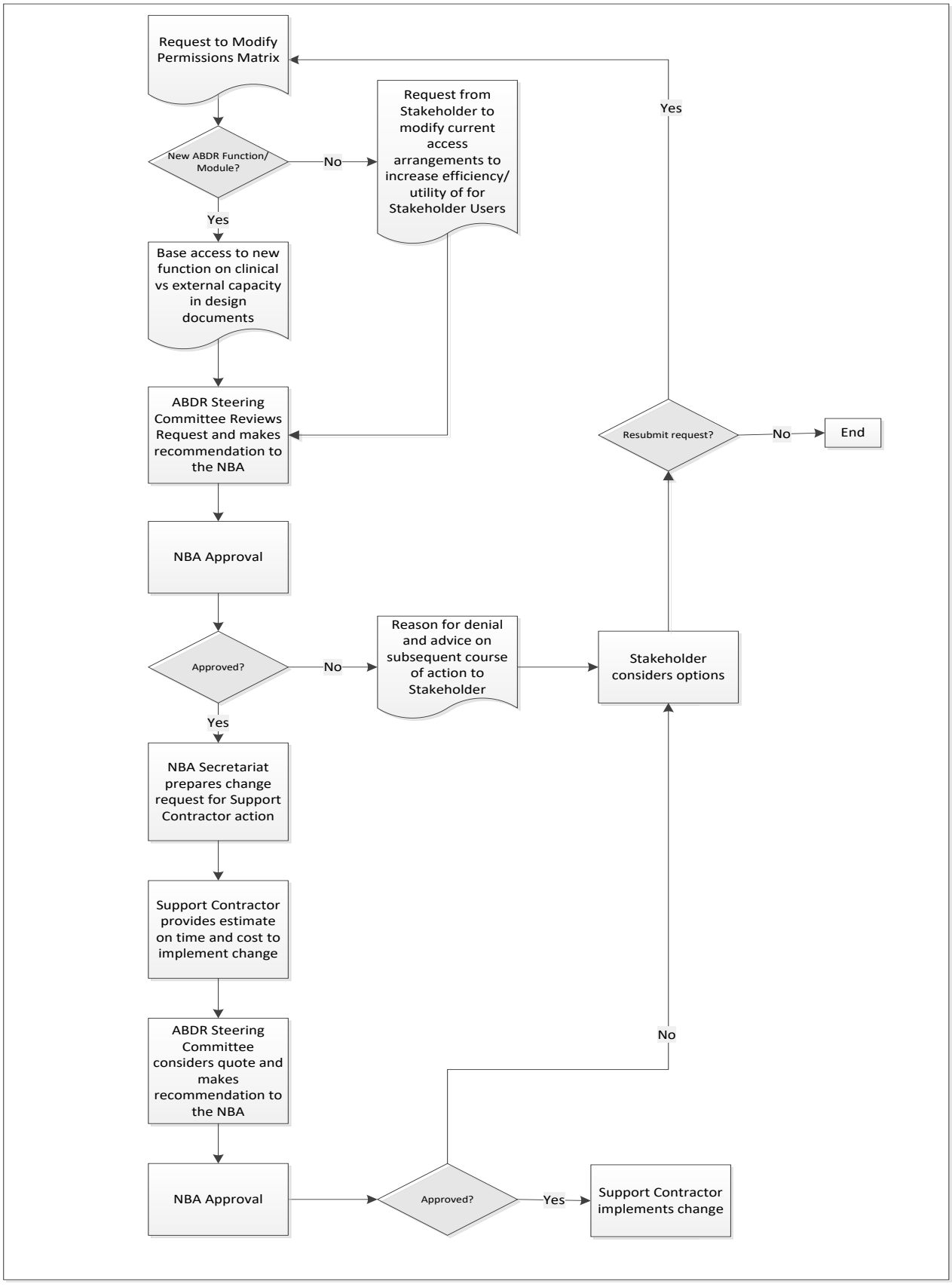
Schedule 2 (Jurisdiction Obligations)

For the purposes of Clause 6 of the agreement the relevant legal and policy obligations to which the Jurisdiction must comply are: [Examples- Health Care Acts, Public Sector Acts, Privacy Acts, Records and Information Acts, Security Acts, Secrecy provisions, internal policy obligations]

APPENDIX 8: ABDR ACCESS PROCESS



APPENDIX 9: ABDR ACCESS VARIATION PROCESS



APPENDIX 10: APPLICABLE STANDARDS AND GUIDELINES FOR PROTECTIVE SECURITY

Once the data is collected and created, it must be stored in a manner that best supports business processes. To determine the appropriate storage media and format, factors such as retention period, security and classification of the data must be addressed.

Data should be classified in terms of its sensitivity and criticality to the NBA. The classification assigned determines how the information must be stored.

Security of confidential and protected data must be implemented to ensure data is not lost or accessed by unauthorised personnel. To ensure the appropriate security mechanisms for data, the following standards/guidelines are followed by the NBA.

Standard/Guideline	Publisher	Summary
Australian Government Protective Security Policy Framework (PSPF)	Attorney-General's Department	The PSPF is the Australian Government's top-level framework for protective security. It is the principal means for publishing Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources.
Australian Government Information Security Manual (ISM)	Australian Signals Directorate	Provides policies and guidance to Australian Government agencies on how to protect their ICT systems. It promotes a consistent approach for information that is processed, stored or communicated with corresponding risk treatments to reduce the level of security risk to an acceptable level. As of 2013 the ISM is issued in three distinct publications: Executive Companion, Principles document and Controls Manual.
ISO17799 / ISO27001 / ISO27002/ AS/NZS17799 – Code of Practice for Information Security Management	Standards Australia, International Organisation for Standardisation	This standard is a globally accepted code of practice for information security management. It is controls based for organisations to manage their information security according to eleven (11) domains: - Information security policy - Organising information security - Asset management - Human resources security - Physical and environmental security - Communications and operations management - Access control - Information systems acquisition, development and maintenance - Information security incident management - Business continuity management; and - Compliance.
AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines	Standards Australia / SAI Global	A risk management standard that defines a general framework consisting of five major stages: Stage 1: Establishing the Context Stage 2: Identifying the Risks Stage 3: Analysing the Risks Stage 4: Assessing & Prioritising Risks Stage 5: Determining Appropriate Controls

Standard/Guideline	Publisher	Summary
CobiT – Control Objectives for IT	ISACA	Provides flexible framework for organisations to meet business objectives and quality, financial and security requirements. It defines seven information criteria: - Effectiveness - Efficiency - Confidentiality - Integrity - Availability - Compliance; and - Reliability of information.
AS8015 – Corporate Governance of ICT	Standards Australia	Is an Australian standard for corporate governance of information and communication technology (ICT). It provides six guiding governance principles and a model by which organisations can ensure that IT is aligned with their business objectives. The six principles are: - Establish clearly understood responsibilities for ICT - Plan ICT to best support the organisation - Acquire ICT validly - Ensure ICT performs well, whenever required - Ensure ICT conforms with formal rules; and - Ensure ICT use respects human factors.

APPENDIX 11: STORAGE AND PROTECTION OF DATA

The NBA adheres to the standards and guidelines of the Commonwealth and in so doing requires that all recipients of NBA data adhere to the same requirements. For all data requests stakeholders/recipients must outline how the data and information will be stored and protected. In meeting the requirements of jurisdictions and safeguarding data assets the NBA stores and protects data as follows:

Physical security of ICT infrastructure

1. All data is stored on secure servers in Australia that are managed appropriately under applicable Australian Government legislation, standards, policies and guidelines as updated from time-to-time.
2. All storage of data is restricted to the geographic region of Australia.

Electronic security of ICT infrastructure

1. Data is encrypted both in transit and at rest and is always encrypted at 256 bits AES when physically copied from the NBA's environment.
2. Any media (such as faulty hard drives) removed from the NBA's infrastructure is physically destroyed when it is no longer needed.
3. CD/DVD burning and USB memory stick access is restricted to less than five NBA officers, with electronic transmissions (such as email and web-browsing) heavily restricted with active filtering and monitoring in place.
4. A triple-level of firewalls are in place, with the outer layer owned and operated by ASD (monitored 24/7 by their Cyber Security Operations Centre), the middle layer owned and operated by DHS and the internal layer owned and operated by the NBA directly. Regular penetration testing is undertaken of all relevant systems.
5. Privileged access requires two-factor authentication.
6. All access to NBA systems are monitored through event logs and audit trails and the process is monitored by the information technology security advisor in accordance with all protective security requirements.

Personnel security matters relating to ICT infrastructure

1. Privileged access is restricted to core NBA officers and a limited number of contracted ICT service providers who only have access under the direct supervision of NBA infrastructure engineers.
2. All users with privileged access hold security clearances at or above the level of Negative Vetting, Level 1 issued by the Australian Government Security Vetting Agency.
3. All users of NBA ICT equipment without privileged access hold security clearances at or above the level of Baseline issued by the Australian Government Security Vetting Agency.
4. Access to all systems is reviewed on an annual basis.
5. All access to systems is reviewed and revoked where appropriate when NBA officers or contracted ICT service providers change roles or leave the organisation.

9. Acronyms and glossary of terms

ACRONYMS

ABDR	AUSTRALIAN BLEEDING DISORDERS REGISTRY
AHCDO	AUSTRALIAN HAEMOPHILIA CENTRE DIRECTORS' ORGANISATION
AHMAC	AUSTRALIAN HEALTH MINISTERS ADVISORY COUNCIL
AIHW	AUSTRALIAN INSTITUTE OF HEALTH AND WELFARE
ALRC	AUSTRALIAN LAW REFORM COMMISSION
AOTDTA	AUSTRALIAN ORGAN AND TISSUE DONATION AND TRANSPLANTATION AUTHORITY (
APP	AUSTRALIAN PRIVACY PRINCIPLES
ASD	AUSTRALIAN SIGNALS DIRECTORATE
ASIO	AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION
BIGG	THE BLOOD INFORMATION GOVERNANCE GROUP
CC	CREATIVE COMMONS
CIO	CHIEF INFORMATION OFFICER
COAG	COUNCIL OF AUSTRALIAN GOVERNMENTS
CTH	COMMONWEALTH
DHA	AUSTRALIAN GOVERNMENT DEPARTMENT OF HUMAN SERVICES
DIAM	DATA AND INFORMATION ACCESS MODEL
DSD	DEFENCE SIGNALS DIRECTORATE
FOI	FREEDOM OF INFORMATION
HFA	HAEMOPHILIA FOUNDATION AUSTRALIA
HPC	HOSPITALS PRINCIPAL COMMITTEE
HREC	HUMAN RESEARCH ETHICS COMMITTEES
ICT	INFORMATION AND COMMUNICATIONS TECHNOLOGY
IPS	INFORMATION PUBLICATION SCHEME
ISM	INFORMATION SECURITY MANUAL
JBC	JURISDICTIONAL BLOOD COMMITTEE
LIS	LABORATORY INFORMATION SYSTEM
MOU	MEMORANDUM OF UNDERSTANDING
NBA	NATIONAL BLOOD AUTHORITY
NHMRC	NATIONAL HEALTH AND MEDICAL RESEARCH COUNCIL
NMDS	NATIONAL MINIMUM DATA SET
PBM	PATIENT BLOOD MANAGEMENT

PSPF	PROTECTIVE SECURITY POLICY FRAMEWORK
SCEC	SECURITY CONSTRUCTION AND EQUIPMENT COMMITTEE
STARS	SUPPLY TRACKING AND REPORTING SYSTEM

GLOSSARY OF TERMS

AGGREGATED DATA	Data is summarised and/or categorised that is analysed and placed in a format that prevents further analysis to prevent the chance of revealing an individual's identity and individual records cannot be re-identified.
DATA	Facts and statistics collected together for reference or analysis or make decisions.
DATA COLLECTION	Is a systematic gathering of data for a particular purpose from various sources, including manual entry into an information system, questionnaires, interviews, observation, existing records and electronic devices.
DATA RE-IDENTIFICATION	Data re-identification is the process by which personal data is matched with the person it describes.
DE-IDENTIFIED DATA	Personal Information that has been reformatted so that the person cannot be identified and this may be through an identifier other than personal details and where the numbers aggregated cannot be identified
GOVDEX	Online Collaboration Tool - It is a secure, private web-based space that helps government agencies to manage projects, and share documents and information.
IDENTIFIED DATA	Refer to Personal Information and Record Level Data.
INFORMATION	Knowledge derived from study, experience, or instruction, and a collection of facts or data.
IVIG	Intravenous immunoglobulin
METeOR	AIHW's Metadata Online Registry
NHIG	Normal human immunoglobulin
PERSONAL INFORMATION	All information where the identity of a person can reasonably be established from the information itself. Information is also personal information if it is reasonably possible for the person receiving the information to identify the individual by using other information.
PUBLICATION	Release of Data externally in hard or soft copy through any media to parties outside of governments.
RECORD LEVEL DATA	Data at the level of an individual person. Record level data may not directly identify the person, but is more open to re-identification than aggregate data.
SCIG	Subcutaneous immunoglobulin

REFERENCES

Government of Western Australia	Department of Health http://www.health.wa.gov.au
Government of South Australia	SA Health http://www.sahealth.sa.gov.au
Queensland Government	Queensland Health http://www.health.qld.gov.au/
Northern Territory Government	Department of Health http://www.health.nt.gov.au/
NSW Government	NSW Health http://www.health.nsw.gov.au
Victorian Government	Department of Health http://www.health.vic.gov.au/
Tasmanian government	Department of Health and Human Services http://www.dhhs.tas.gov.au/
ACT Government	ACT Health http://www.health.act.gov.au
Australian Government	Office of the Australian Information Commissioner http://www.oaic.gov.au/
Australian Government	Australian Institute of Health and Welfare http://www.aihw.gov.au/
Australian Government	Department of Finance http://www.finance.gov.au/
Australian Government	Department of Health http://www.health.gov.au/
Australian Government	National Statistical Service, Statistical Data Integration http://www.nss.gov.au/nss/home.NSF/pages/Data+Integration+Landing%20Page?OpenDocument
Australian National Data Service	http://www.ands.org.au/datamanagement/