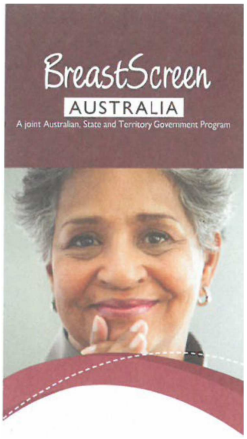


BREASTSCREEN AUSTRALIA NATIONAL QUALITY MANAGEMENT COMMITTEE (NQMC)

Data Governance and Management Assessment Framework

Version 2

March 2017

1 Introduction

1.1 Purpose

This document outlines a framework for the Data Governance and Management Assessments (DGMA) that apply under the BreastScreen Australia Accreditation System.

The purpose of the DGMA Framework is to:

- Summarise the requirement to undergo a DGMA, as outlined in the BSA Accreditation Handbook, and the assessment process that applies;
- Outline the requirements against which Services and SCUs will be assessed; and
- Describe how Services/SCUs and Data Assessors should approach this assessment – that is, the questions that should be asked, and the types of evidence that should be taken into account.

1.2 Review

This document is subject to ongoing review to ensure that the DGMA Framework reflects technological changes and learnings from Data Assessors, SCUs and Services.

Please visit the CancerScreening website to ensure you have the most recent version of the DGMA Framework.

1.3 Context

Purpose of DGMA

DGMAS are undertaken to achieve national consistency within the BSA Program regarding:

- the collection and reporting of data governance and management accreditation information across jurisdictions and BreastScreen Services;
- business processes to ensure data is of a high quality, valid and collected in accordance with the specifications of the BreastScreen Australia Data Dictionary; and
- the interoperability between jurisdictional PACS and individual BreastScreen registries, both within and external to the jurisdiction.

The intent of the DGMA is to assess whether the outcomes of the data governance and management arrangements of a Service or SCU as a whole are robust. Specifically, a DGMA is defined in the Handbook as:

> *An independent assessment of a Service and/or SCUs policies and processes that are in place to ensure effective governance and management of BreastScreen data. These policies and processes must meet those requirements as outlined in the National Accreditation Standards (NAS).*

DGMAs will be undertaken by a qualified Data Assessor, who will form part of the survey team lead by the National Surveyor. The Data Assessor's findings of the DGMA will be recorded in the survey team findings.

Requirement to undergo a DGMA

As outlined in the National Accreditation Handbook, all Services and SCUs are required to undergo a DGMA as part of the Accreditation survey.

In the case of multi-service jurisdictions that have a central PACS/Client Management System, only the SCU will be required to undergo a DGMA.

However, the operational level allocation of responsibility between the Service and SCU for the implementation/maintenance of the Standard 5 Protocols is an important issue for the Data Assessor to understand for the purposes of undertaking a DGMA of an SCU.

Therefore, it is proposed that each multi-service jurisdiction is required to complete a document (a Standard 5 Protocol Responsibility Framework – or PRF5) detailing the allocation of operational level responsibility between the Service and SCU for each area of data governance and management.

This does not alter the fact that, in multi-service jurisdictions which have a central PACS/ Client Management System, the SCU has overall responsibility for ensuring the consistency and quality of information recorded in the BreastScreen Service Client Management System within the jurisdiction.

The PRF5 will need be provided to the Data Assessor prior to the organisation of a DGMA. It will help the Data Assessor to understand the evidence provided by the SCU of the quality and consistency of data that is entered at each service within the jurisdiction.

1.4 DGMA Requirements

The DGMA involves assessing the Service/SCU against defined requirements, outlined in the Handbook (the DGMA Requirements) and NAS Commentary. There are three sources for the DGMA requirements:

- National Program Features for Data Management and information systems;
- Data Discipline Key Areas for each of the four disciplines of Data Governance and Management; and
- 10 Standard 5 Protocols.

The DGMA Requirements are structured according to the 4 data disciplines. A detailed summary of the sources for the DGMA Requirements is contained in Attachment A.

The revised NAS includes a Data Management and Information Systems Standard that comprises one criterion with two measures: NAS Measure 5.1.1 and 5.1.2. These standards are assessed as part of a Service/SCU's Annual Data Report or re-application for accreditation and are not within the scope of this DGMA Framework. However, the Standard 5 Protocols are part of the DGMA Requirements.

1.5 DGMA Assessment Points

The Service/SCU self-assesses against the DGMA Assessment Points by assigning a Risk Rating to each assessment outcome, using a risk rating tool.

2 The DGMA Framework

The DGMA Framework involves, at a high level:

- Four *Assessment Points* built around the 4 data disciplines.
- For each Assessment Point, a number of *DGMA Requirements* are identified. They reflect the expected outcomes that should be achieved by the SCU/Service.
  - For each DGMA Requirement an assessment is made of the achievement rating – that is whether performance is met, unmet, met with exception or unable to be assessed.
  - In the context of the DGMA, met with exception (ME) means that the DGMA Requirement was achieved with the exception of a small number of cases.
  - Unable to be assessed applies if there is insufficient evidence to determine whether a Service or SCU meets the DGMA requirement.
  - Each of the DGMA Requirements has been referenced back to either a program policy feature, a Data Discipline Key Area or a Standard 5 Protocol.

The DGMA results in four risk ratings (one for each Assessment Point) rather than a single DGMA outcome. Risk ratings are determined based on an assessment of the likelihood that the Service/SCU is not meeting the relevant Assessment Point, and the severity of the consequences (using the risk rating tool provided).

Importantly, the DGMA Framework has been designed for use for self-assessment by SCUs/ Services and for independent assessment by Data Assessors. In this respect, the broad process for a DGMA is part of the normal application process, whereby SCUs/Services complete a self-assessment prior to the survey of the SCU/Service by an independent survey team led by the National Surveyor.

DGMA Key Features

Table 1 sets out the key features of the proposed DGMA Framework.

Table 1: Key Features of the proposed Data Governance and Assessment Framework

Assessment Point		DGMA Requirement	Source
1. Data security arrangements are acceptable	1.1	Data is secure from unauthorised access, within systems and during transfers between systems.	*Disciplines Key Area 1.1 & 1.2; Protocol 5.4.*
	1.2	Data identity is obscured.	*Discipline Key Area 1.3.*
	1.3	Data security breaches are well managed.	*Discipline Key Area 1.4; Protocol 5.4.*
2. Data quality arrangements are acceptable	2.1	Data is entered, recorded, managed, monitored and processed in conformance with the definitions and algorithms of the BSA data dictionary.	*Discipline Key Area 2.1 & 2.2; Protocol 5.1.*
	2.2	The data recorded in systems is accurate and complete.	*Discipline Key Area 2.3; Protocols 5.2 & 5.3.*

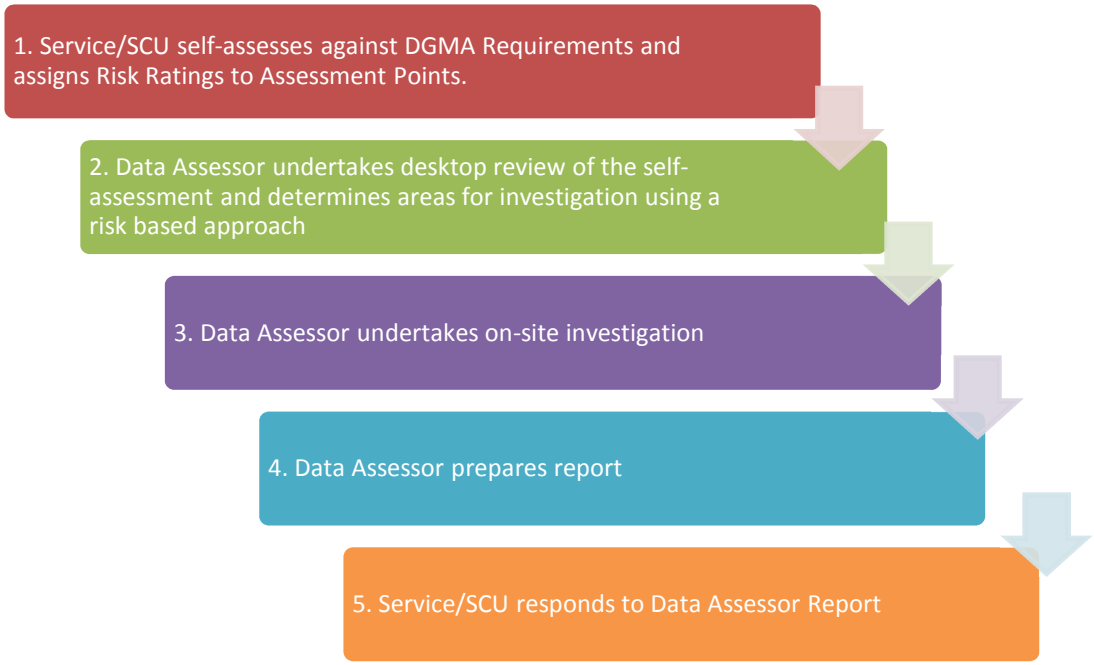
Assessment Point		DGMA Requirement	Source
	2.3	Each client within a state or territory program has one unique identifier.	*Protocol 5.6.*
	2.4	All client records are appropriately dated and identifiable to the relevant health professionals.	*Protocol 5.7.*
	2.5	Data quality problems are identified.	*Discipline Key Areas 2.3 & 3.2; Protocol 5.2.*
3. Data integrity arrangements are acceptable	3.1	Data integrity is maintained in transfers between systems, including local systems, state-wide systems and external systems.	*Discipline Key Areas 3.1, 3.3 & 4.3* *; Protocol 5.2.*
	3.2	The file tracking system used has integrity and reliability.	*Protocol 5.5.*
4. Data organisation and systems management arrangements are acceptable	4.1	The ownership, accountability and responsibility for all key data sets are clearly identified and understood.	*Program Policy Features.* *Protocol 5.4 and Protocol 5.10*
	4.2	Data is used for strategic purposes, quality improvement and for clinical management and for review by the National Quality Management Committee.	*Program Policy Features.*
	4.3	Data is retained, stored and disposed of in accordance with relevant state or territory legislation.	*Protocol 5.8.*
	4.4	Systems are reliable and well supported.	*Discipline Key Areas 4. 1 & 4; Protocol 5.10.*
	4.5	Systems are updated in ways that meet changing requirements and maintain system reliability.	*Discipline Key Area 4.1 & 4.4; Protocol 5.10.*
	4.6	Systems are updated to meet changes to the BSA NAS and BSA Data Dictionary.	*Discipline Key Area 2.4; Protocol 5.10.*
	4.7	Systems conform to relevant standards for how clinical information is recorded, organised and managed.	*Discipline Key Area 4.2.*
	4.8	Systems and data can be restored in event of data corruptions and disasters.	*Discipline Key Area 4.5; Protocol 5.9.*

Note that it is not the role of a Data Assessor to undertake a full quality assurance or systems check of the data governance and assessment arrangements of a SCU/Service. Rather, the task of a Data Assessor is to reach a judgment on the identified DGMA

Requirements and Assessment Points on the basis of evidence provided and assessed. As such, the focus will be on key indicators that the Assessment Points are met. This will enable the DGMA to ensure an appropriate assessment outcome, regardless of whether the context was a Service based data governance and management approach or if the PACS/Client Management System was part of a state-wide ICT system.

DGMA Assessment Process

The DGMA is conducted according to the following assessment process:



The assessment process is described in detail in Table 2. The assessment process is similar to the process Services/SCUs go through in relation to assessment against NAS Data Measures.

Table 2 – DGMA Assessment Process

#	Assessment step	Description
1.	**Self-assess against DGMA Requirements**	The SCU or Service being assessed undertakes a self-assessment: • For each DGMA Requirement and determines an achievement rating – that is, whether it is met, unmet, met with exception or unable to be assessed; and - Assigns a risk rating to each Assessment Point, using a risk rating tool which takes into account both the likelihood and severity of the potential negative consequences arising from the Service/SCU's performance against the assessment point. Three possible Risk Rating determination outcomes result through combination of options for consequence and likelihood of a Service/SCU not meeting an Assessment Point. The self-assessment will be undertaken using the detailed DGMA Framework in Attachment B. The SCU/Service documents the outcome of the self-assessment and the supporting rationale using the DGMA Self-assessment Form (BSA302) The DGMA Framework provides guidance on

#	Assessment step	Description
		the how to undertake this assessment, and what evidence should be taken into account. Multi-service jurisdiction SCUs must also provide: - A completed Standard 5 Protocol Responsibility Framework form, indicating how the operational responsibility for the Standard 5 Protocols has been allocated between the SCU and its Services. -
2.	**Data Assessor determines priority areas for investigation**	On the basis of the self-assessment by the Service/SCU, the Data Assessor determines, using a risk-based approach, the specifics for investigation when undertaking the DGMA during a survey. This includes: • indicating to the Service/SCU what further information is required; and • Specifying what processes might require inspection.
3.	**Data Assessor undertakes investigation**	During the accreditation survey, the Data Assessor may interview staff, examine processes and undertake other activities required to make an assessment.
4.	**Data Assessor prepares a DGMA Data Assessor Report**	Once investigations have been concluded, the Data Assessor completes a DGMA Data Assessor Report (BSA303): • Assesses the Service/SCU against each DGMA requirement; • Assigns a risk rating to each Assessment Point, using a risk rating tool (provided in BSA303) which requires the Data Assessor to take into account both the likelihood and severity of the potential negative consequences arising from the Service/SCU's performance against the Assessment Point; • Summarises any performance issues and lists any recommendations for change to data governance and management; • Summarises the Service/SCU's overall performance in data governance and management. The completed DGMA Data Assessor Report is provided to the Service/SCU at the same time as the Survey Report.
5.	**Service response to Data Assessor Report**	The Service/SCU responds to the Data Assessor's assessment by completing a 'Response to Data Assessor Report" form. The Service/SCU will respond to the Data Assessor's assessment against DGMA requirements, Risk Ratings and any comments in the Report.

The outcomes of a DGMA will assist the National Quality Management Committee (NQMC) to arrive at an accreditation decision for the SCU/Service. That is, the impact of the DGMA outcome is part of the overall context of the SCU/Service performance that the NQMC will consider when determining an accreditation outcome.

Definitions

In the DGMA Framework, the following definitions apply:

Term	Definition

Term	Definition
Accurate and complete	Whether data is considered to be 'accurate and complete' the purposes of a DGMA, is a matter for the individual judgment of the Data Assessor.
Assessment focus area	The issues that needs to be examined in order to determine if the relevant DGMA Requirement is achieved.
Approach to assessment	The specific assessment activities that would be undertaken (applies to both SCU/Service self-assessing and to Data Assessor).
Evidence expected	The type of evidence that should be considered when assessing a DGMA Requirement
Research	As defined in the Australian Code for the responsible conduct of research.
Quality improvement	Quality improvement is the identification and implementation of strategies to enhance the quality of data governance and management. It involves ongoing review of data to identify changes that could improve performance.

A note on ICT systems

Note that references to processes and systems are intended to cover both IT systems and their processes **and** manual systems and their processes. Further, documentation should be interpreted broadly to include IT system based information that can be gained via queries or reports, rather than being contained in paper based documentation.

Assessment approaches need to be cognisant of the fact that in many jurisdictions, the SCU/Service's IT services are subject to overarching control by the relevant jurisdictional Health Department IT Services area. The DGMA is not intended to be an assessment of IT systems external to the SCU/Service. Specifically, for DGMA Requirement 4.4:

- If data is transferred between a PACS or Client Management System operated by a SCU/Service and a system operated by an external party, then the transfer out of or into the PACS or Client Management System is within the scope of the DGMA.
- If the external system is part of an end-to-end PACS or Client Management System process it is considered within the scope of the DGMA;
- The data governance and management of BreastScreen data held by external systems where they are not part of an end-to-end PACS or Client Management System process is not considered within the scope of the DGMA.

Attachment A - DGMA Requirements Sources

The DGMA involves assessing the Service/SCU against defined requirements, outlined in the Handbook (the DGMA Requirements) and NAS Commentary. There are three sources for the DGMA requirements:

- The 4 Program Policy Features;
- Data Discipline Key Areas for each of the four data disciplines; and
- 10 Standard 5 Protocols.

1. Program Policy Features

The Accreditation Handbook outlines four BSA Program Policy features that relate to data governance and management[1]:

- Data are collected, stored and managed using secure, quality, contemporary data management and communication systems that comply with relevant state and national standards, and that enable valid, reliable system and service performance analysis and evaluation;
- Data are used for strategic purposes, quality improvement of services and for clinical management;
- Data are collected in line with the requirements of the BreastScreen Australia Data Dictionary; and
- Data are submitted annually for use in a national program monitoring report and for review by the National Quality Management Committee.

These program features formed the basis for the development of the National Accreditation Standards and supporting protocols.

2. Data Discipline Key Areas

The Handbook indicates that there are four disciplines of data governance and management that will be assessed by the Data Assessor as part of a DGMA:

- Discipline 1 - Data security;
- Discipline 2 - Data quality;
- Discipline 3 - Data integrity; and
- Discipline 4 - Data organisation and systems management

The revised Handbook identifies the key areas under each of the DGMA disciplines on which the Data Assessor will focus when analysing data governance and management. These key areas are shown in **Table 3**.

[1] National Accreditation Handbook approved by the Standing Committee on Screening on 25 February 2015, p 17.

Table 3: DGMA Disciplines and their key areas for assessment

Discipline
Discipline 1 - Data security
• Policies that minimise security risks to information and prevent unauthorised access to data. Policies should comply with national standards for information security management including AS/NZS ISO/IEC 27001:2006 and AS/NZS ISO/IEC 27002:2006.
• Role-based access levels, permissions and authorisation to data.
• Solutions that obscure client identities by modifying client-identifiable data while maintaining data quality. This should ensure data can be used for secondary purposes, e.g. national data analysis/research without compromising confidentiality. Data identifiability should be informed by the National Health and Medical Research Council's National Statement on Ethical Conduct in Human Research 2007 (updated 2013).
• Procedures that ensure security risks/breaches to the Client Management System and PACS are identified logged, reported and actioned.
Discipline 2 - Data quality
• Establishing data validation rules, processes and monitoring systems to ensure entered data conform to the data specifications as outlined in the BreastScreen Australia Data Dictionary regarding data-type (i.e. numeric/alphanumeric), field size, data domain etc.
• Developing query reports that relate to the quality of data within the PACS and/or Client Management System. These queries may be used to identify missing data, 'out-of-range' data or data that appear to be inconsistent. They may also be used to identify abnormal trends (e.g. an unexpected increase in recall to assessment/decrease in cancer detection etc.).
• Establishing quality assurance mechanisms to ensure: - the consistent application of algorithms as described in the BreastScreen Australia Data Dictionary. The Data Assessor may request a demonstration of how the results for specific accreditation measures are calculated. - data accuracy (the extent to which data in the Client Management System matches with source data); and - data completeness (extent to which all data that should have been registered have actually been registered).
• Processes to ensure the Client Management System is updated when any changes are made to the BreastScreen Australia NAS or data specifications/definitions within the Data Dictionary.
Discipline 3 - Data integrity
• Solutions that maintain the integrity of data transferred between systems (e.g. between the local BreastScreen Client Management System and statewide PACS or between the BreastScreen Client Management System and, if appropriate, external databases/systems), including processes to test data to eliminate bugs that may cause data loss or corruption during data storage or transfer.
• Establishing appropriate data integrity checks (including both routine and random audits) to ensure data conforms to the data validation rules (developed under Item 2 – Data Quality) after it has been created, stored, retrieved or transferred. These checks should highlight errors, inconsistencies and missing data so that they can be rectified by the Data Manager, or referred

Discipline
to the appropriate person for action.
• Mechanisms to ensure data transferred to other systems (e.g. between the SCU and Services, or externally to third party organisations) are secure and unable to be modified without prior authorisation (e.g. disabling fields). Where data are modified, integrity checks are built-in to ensure that data entered remotely complies with the validation rules developed under Item 2 – Data Quality.
Discipline 4 - Data organisation and systems management
• Establishing support management systems, including appropriate technical support, to address any issues in an effective and timely manner, whilst ensuring the Client Management System/PACS can continue operating to support service delivery requirements.
• Solutions that specify common standards for how clinical information is recorded, organised and managed within the PACS and/or Client Management System. This may include integrating the Healthcare Enterprise (IHE) standards such as Health Level 7 (HL7) Clinical Document Architecture, Digital Imaging and Communications in Medicine (DICOM) or Systematised Nomenclature of Medicine – Clinical Terms Australia (SNOMED CT-AU).
The Data Assessor should assess the extent to which these solutions: • are adhered to, and consistently implemented within the Client Management System/PACS; and • enable interoperability for BreastScreen services within a jurisdiction and where possible, external to the jurisdiction, as well as external third party providers.
• Solutions to ensure seamless communication and information exchange between the statewide Client Management System/PACS and individual BreastScreen Client Management Systems within the jurisdiction.
• A comprehensive Data Management Manual (or equivalent) which includes but is not limited to: - All policies, procedures and protocols that are required for the effective management and governance of data within the PACS and Client Management System; ◆ Change management strategies; and ◆ Training requirements.
• Processes to ensure back-up and disaster recovery of data within the PACS and Client Management System

3. Standard 5 Protocols

The NAS Commentary also specifies a range of data management and information systems protocols that should be developed and maintained by Services/SCUs.

Table 4: Data Management and Information Systems protocols

5.1	The Service and/or SCU conforms with requirements of the BreastScreen Australia Data Dictionary, with regard to: a) collection of all required data items; and b) the definitions and methods used by the Service and/or SCU in the calculation of performance measures.

5.2 The Service and/or SCU undertakes ongoing quality control procedures for data throughout the screening and assessment process, including:

a) review of the completeness and legibility of clinical records;
b) review of the consistency between paper and computer records where required; and
c) verification of the accuracy of the output of system generated reports.

5.3 All relevant staff are instructed in procedures to ensure the quality of the data at all levels of the screening and assessment pathway.

5.4 The Service and/or SCU ensures effective policies, procedures and protocols to achieve a high level of data security, accuracy, integrity and organisation and systems management.

5.5 The Service and/or SCU ensures the integrity and reliability of the file tracking system used.

5.6 Each client has one unique identifier within any State and Territory program.

5.7 All client records held by all units in the Service and/or SCU are dated and identifiable to the relevant health professional for that part of the screening and/or assessment pathway.

5.8 The Service and/or SCU complies with relevant state/territory legislation for the retention and storage of client records.

5.9 The Service and/or SCU has disaster recovery systems that address the risk of network failure and data loss from Picture Archiving Communication System (PACS) and Client Management Systems.

5.10 The Service and/or SCU has policies, procedures and guidelines for the development and maintenance of high quality Information, Communication and Technology systems.

The NAS Commentary provides information on a number of issues relevant to the NAS 5.1.1 and 5.1.2 and the attendant protocols:

- Quality control procedures;
- Designated data person;
- Protocol for management of client records;
- Unique identifier;
- Client record identification;
- Storage and retention of client records;
- Appropriate data security;
- Disaster recovery systems and back-up procedures; and
- High quality information, communication and technology systems.

Attachment B – Detailed DGMA Framework

Data Governance and Assessment Framework

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
1	**Data security arrangements are acceptable**				
1.1	Data is secure from unauthorised access, within systems and during transfers between systems.	1. What are current staff practices for user names and passwords? 2. Are there sound management procedures for granting and terminating access? 3. Do the systems have capacity for role based access levels, permissions and authorisation to data? 4. Does the ICT service provider have sound staff practices for security (broad definition of service provider)? 5. Do providers of physical data management transfers (including digital media, e.g. USB, CD) have sound security practices?	1. Staff interviewing (consistent and focused line of questioning). 2. Ditto, but with more emphasis on whether procedure manuals are kept up to date/viewing of physical evidence. 3. Determine the requirements of the software being used by e.g. examining requirements documents, testing/observing operation of the system to see how it works. 4. Understand who service providers are and whether they have sound practices through questions to Service/SCU. 5. As per 4.	1. Procedure manuals. 2. As per 1, above. 3. Different permission levels associated with each role. 4. List of service providers. Evidence around practices of providers (self-assessment document for services to use could be useful, potential tool to come out of framework). 5. List of service providers and their policies.	1, 2 & 3, 4- Relevant international standards.
1.2	Data identity is obscured.	How is data de-identified to	Interviewing and	Output records/data files sent to external	N/A

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
		preserve confidentiality?	observing.	stakeholders.	
1.3	Data security breaches are well managed.	Are procedures for managing breaches in place, and are they being followed?	Reviewing documents and interviewing. (possibly including relevant legislation).	Procedures, Audit logs, incident management records.	N/A
2	**Data quality arrangements are acceptable**				
2.1	Data is entered, recorded, managed, monitored and processed in conformance with the definitions and algorithms of the BSA data dictionary.	1. Conformance of systems that capture data (validation rules) to Data Dictionary. 2. Conformance of reporting systems to Data Dictionary. 3. Conformance of work practices to Data Dictionary. 4. Service/SCU conformance assurance processes.	1. Interviewing, reviewing requirements documentation. 2. As per 1, plus inspecting reports. 3. Interviewing staff with focus on level of training for data users 4. Interviewing.	1. Requirements documentation. 2. Requirements documentation. 3. Relevant training documentation.	Data Dictionary.
2.2	The data recorded in systems is accurate and complete.	1. Data transcription and reporting. 2. Quality Assurance processes – as per previous requirement above.	Reviewing procedures / documentation for data entry and quality assurance.	Demonstration of query reports for outliers (e.g. running reports for missing data) / evidence that have regularly run reports/frequency of reports (at least as frequent as purging of audit log). Procedure and training documentation.	
2.3	Each client within a state or territory program has	Systems and validation.	As above.	As above.	

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
	one unique identifier.	Data.			
2.4	All client records are appropriately dated and identifiable to the relevant health professionals.	1. Conformance of systems that capture data (validation rules). 2. Conformance of reporting systems. 3. Conformance of work practices (including who signed the form. 4. Service/SCU conformance assurance processes.	1. Interviewing, reviewing requirements documentation. 2. As per 1, plus inspecting reports. 3. Interviewing staff with focus on level of training for data users. 4. Interviewing.	1. Requirements documentation. 2. Requirements documentation. 3. Relevant training documentation.	Data Dictionary.
2.5	Data quality problems are identified.	1. Culture and staff practices. 2. Regular monitoring and culture around reporting.	1. Interviewing on procedures for monitoring and providing feedback (*Including asking staff at data-entry level what they do in event of particular problem*). 2. Requesting examples of specific problems identified.	1. Procedure manuals and training documentation. Documented processes (such as request forms). 2. Reports, updates to plans and identified problems. Error logs.	Data dictionary.

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
3	**Data integrity arrangements are acceptable**				
3.1	Data integrity is maintained in transfers between systems, including local systems, state-wide systems and external systems.	1. Use of standards (in design and implementation of system). 2. Implementation. 3. Handling of mismatches (technical component and procedural component). 4. Overall regular checking of data.	1. Review extent to which systems use standards (Note - may be need for follow up with people with technical expertise). 2. Review of rules around matching (which database implements in back-end). 3. Reviewing the technical rules of how the system handles mismatching and work procedures for offline processes. 4. Review reports detailing procedures scheduled and not completed, or procedures performed but with incorrect status recorded.	1. System requirements. 2. System requirements. 3. System requirements and procedural documentation. 4. System requirements procedural documentation.	International Standards (HL7, DICOM, SNOMED).
3.2	The file tracking system used has integrity and reliability.	Are Staff processes for file tracking being followed?	Interviewing – focused questions on ability to track and locate files.	Evidence that a system of file management/tracking is in place.	N/A

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
4	**Data organisation and systems management arrangements are acceptable**				
4.1	The ownership, accountability and responsibility for all key data sets are clearly identified and understood.	Have all key data sets been clearly identified? Is there a clear system of accountability and responsibility for the key data sets?	Interviewing manager to determine how data ownership, accountability and responsibility are managed.	1. Plans outlining data governance arrangements. 2. Organisational charts indicating organisational hierarchy, accountabilities and reporting structures 3. Job descriptions of data manager and other key staff outlining key responsibilities. 4. If data is used for research purposes, then evidence that appropriate permissions (ethics committee approvals) are obtained. 5. If external contractors are used for updating data\data remediation\data matching etc. then evidence that responsibilities and accountabilities are documented.	N/A
4.2	Data is used for strategic purposes, quality	How the data is used to drive quality activities.	Interviewing manager to determine how data is	Evidence of knowledge management strategy.	

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
	improvement and for clinical management and for review by the National Quality Management Committee.		used to inform quality improvement.		
4.3	Data is retained, stored and disposed of in accordance with relevant state or territory legislation.	1. Management of paper records. 2. Management of digital records.	1 & 2 – Investigate understanding of applicable legislation / demonstration of how legislation is being followed.	1 & 2 – Plans relating to regulatory compliance.	Relevant State/Territory legislation.
4.4	Systems are reliable and well supported.	1. Reliability of the systems (including PACs, reporting systems, client management system). 2. Support mechanisms.	1. Interviewing and asking for evidence of up-time/down-time of systems, and reportable problems (e.g. data validation not working properly). 2. Interviewing/ reviewing details of support arrangements.	1. Logs of problems and issues. 2. Evidence of a Service level agreement that is being followed.	
4.5	Systems are updated in ways that meet changing requirements and maintain system reliability.	Processes used for identifying when change is required and for updating systems and processes.	1. Interviewing manager. 2. Reviewing relevant process documentation.	Relevant policy documents.	
4.6	Systems are updated to meet changes to the BSA NAS and BSA Data Dictionary.	Processes used for identifying when change is required and for updating systems and processes.	3. Interviewing manager. 4. Reviewing relevant process documentation.	Relevant policy documents. Evidence updates have been made.	

#	DGMA Requirement	Assessment focus area	Approach to assessment	Evidence expected	Supporting resources
			5. Spot checking to ensure updates have been made.		
4.7	Systems conform to relevant standards for how clinical information is recorded, organised and managed.	Use of standards in design and implementation of system.	As above re requirements of systems (*note may be need for follow up with people with technical expertise*).	System requirement documentation.	Data dictionary. International Standards (HL7, DICOM, SNOMED).
4.8	Systems and data can be restored in event of data corruptions and disasters.	Disaster recovery arrangements.	Interviewing manager. Reviewing plans relating to disaster recovery / business continuity.	Plans relating to disaster recovery / business continuity.	