BreastScreen AUSTRALIA
A joint Australian, State and Territory Government Program

OFFICE USE ONLY

Date of receipt by SCU	
Date of receipt by NQMC	

DGMA Self-Assessment

DETAILS OF SERVICE/SCU

Name of SERVICE/SCU				
Reporting period	From	Click here to enter a date.	To	Click here to enter a date.
Completed by (name)				

Instructions

1. For each **DGMA requirement**, please list relevant evidence to support your self-assessment and the key contact personnel. The evidence should enable the Data Assessor to consider the robustness of your self-assessment and determine priority areas for further investigation.

– When completing the self-assessment, fill in the 'Evidence Provided' column in response the requirements outlined in the 'Evidence Expected' column (these are drawn from Attachment A of the DGMA Framework).

– All documents referenced in the self-assessment must be provided to the Data Assessor as electronic documents, with relevant sections clearly referenced in the self-assessment.

– If you list a staff member in the 'Evidence Supporting Assessment' column, please indicate on which matter the staff member can provide evidence, e.g. Service Data Manager in relation to data security breaches.

2. Record your self-assessment for each **DGMA requirement** as either Met (M), Unmet (U), Met with Exception (ME), Unable to be Assessed (UA) or Not Applicable (NA). These terms are defined in the Handbook (Section 3.3.4).

– If a DGMA requirement is not the responsibility of your Service/SCU, you should select 'NA' as your self-assessment.

3. Complete the **Assessment Point Risk Rating**, using the tools in Appendix A. This involves recording the risk likelihood, the consequences of the risk, and overall risk rating for each Assessment Point.

SELF-ASSESSMENT

Assessment Point 1: Data security arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
1.	**Data security arrangements**	**Data security policy document**		**N/A**
1.1	Data is secure from unauthorised access, within systems and during transfers between systems.	Documents which demonstrate: 1. Staff practices for user names and passwords; 2. Procedures for granting and terminating access; 3. Systems capacity for role based access levels, permissions and authorisation to data; 4. ICT service providers and their security practices, e.g. self-assessment for services. 5. Service providers of physical data management transfers and their security policies and practices. (Digital media, e.g. USB, CD etc.) *Key SCU/Service contact personnel:*		Choose an item.
1.2	Data identity is obscured.	Documents which demonstrate: 1. Data is de-identified to preserve confidentiality, e.g. records/data files sent to external stakeholders. *Key SCU/Service contact personnel:*		Choose an item.

Assessment Point 1: Data security arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
1.3	Data security breaches are well managed.	Documents which demonstrate: 1. Procedures for managing breaches are in place and being followed, e.g. audit logs, incident records. *Key SCU/Service contact personnel:*		Choose an item.

Assessment Point 1: Risk Rating			List rationale to support the Risk Rating:
Risk likelihood	**Risk consequences**	**Risk rating**	
Choose an item.	Choose an item.	Choose an item.	

Assessment Point 2: Data quality arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
2.	**Data quality arrangements**	**Data quality policy document**		**N/A**
2.1	Data is entered, recorded, managed, monitored and processed in conformance with the definitions and algorithms of the BSA data dictionary.	Documents which demonstrate: 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. *Key SCU/Service contact personnel*		Choose an item.
2.2	The data recorded in systems is accurate and complete.	Documents which demonstrate: 1. Data transcription and reporting. 2. Quality Assurance processes – as per requirement above. *Key SCU/Service contact personnel*		Choose an item.
2.3	Each client within a state or territory program has one unique identifier.	Documents which demonstrate: 1. Systems and validation data. *Key SCU/Service contact personnel*		Choose an item.
2.4	All client records are appropriately dated and identifiable to the relevant health	Documents which demonstrate: 1. Conformance of systems that capture		Choose an item.

Assessment Point 2: Data quality arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
	professionals.	data (validation rules). 2. Conformance of reporting systems. 3. Conformance of work practices (including who signed the form. 4. Service/SCU conformance assurance processes. *Key SCU/Service contact personnel*		
2.5	Data quality problems are identified.	Documents which demonstrate: 1. Culture and staff practices. 2. Regular monitoring and culture around reporting. *Key SCU/Service contact personnel*		Choose an item.

Assessment Point 2: Risk Rating			List rationale to support the Risk Rating:
Risk likelihood	**Risk consequences**	**Risk rating**	
Choose an item.	Choose an item.	Choose an item.	

Assessment Point 3: Data integrity arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
3.	**Data integrity arrangements**	**Data quality policy document**		**N/A**
3.1	Data integrity is maintained in transfers between systems, including local systems, state-wide systems and external systems.	Documents which demonstrate: 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. *Key SCU/Service contact personnel*		Choose an item.
3.2	The file tracking system used has integrity and reliability.	Documents which demonstrate: 1. Staff processes for file tracking are being followed. *Key SCU/Service contact personnel*		Choose an item.

Assessment Point 3: Risk Rating			**List rationale to support the Risk Rating:**
Risk likelihood	**Risk consequences**	**Risk rating**	
Choose an item.	Choose an item.	Choose an item.	

Assessment Point 4: Data organisation and systems management arrangements are acceptable

#	DGMA Requirement	Evidence Expected	Evidence Provided	Self-assessment
4.	**Data organisation and systems management arrangements**	**Data quality policy document**		**N/A**
4.1	The ownership, accountability and responsibility for all key data sets are clearly identified and understood.	Documents which demonstrate: 1. All key data sets have been clearly identified. 2. A clear system of accountability and responsibility for the key data sets. *Key SCU/Service contact personnel*		Choose an item.
4.2	Data is used for strategic purposes, quality improvement and for clinical management and for review by the National Quality Management Committee.	Documents which demonstrate: 1. How the data is used to drive quality activities. 2. Provision of data for national program monitoring report. *Key SCU/Service contact personnel*		Choose an item.
4.3	Data is retained, stored and disposed of in accordance with relevant state or territory legislation.	Documents which demonstrate: 1. Management of paper records. 2. Management of digital records. *Key SCU/Service contact personnel*		Choose an item.
4.4	Systems are reliable and well supported.	Documents which demonstrate: 1. Reliability of the systems (including PACs, reporting systems, client management system). 2. Support mechanisms. *Key SCU/Service contact personnel*		Choose an item.

4.5	Systems are updated in ways that meet changing requirements and maintain system reliability.	Documents which demonstrate: 1. Processes used for identifying when change is required and for updating systems and processes. *Key SCU/Service contact personnel*		Choose an item.
4.6	Systems are updated to meet changes to the BSA NAS and BSA Data Dictionary.	Documents which demonstrate: *Key SCU/Service contact personnel*		Choose an item.
4.7	Systems conform to relevant standards for how clinical information is recorded, organised and managed.	Documents which demonstrate: 1. Use of standards in design and implementation of system. *Key SCU/Service contact personnel*		Choose an item.
4.8	Systems and data can be restored in event of data corruptions and disasters.	Documents which demonstrate: 1. Disaster recovery arrangements. *Key SCU/Service contact personnel*		Choose an item.

Assessment Point 4: Risk Rating			**List rationale to support the Risk Rating:**
Risk likelihood	**Risk consequences**	**Risk rating**	
Choose an item.	Choose an item.	Choose an item.	

Appendix A

Definitions for Likelihood

Almost certain:	Strong evidence to indicate the Assessment Point is not met due to: • Satisfactory documentation not provided/available; and • Inconsistent practice/s in place; and • Inconsistent understanding and/or application of protocols across SCU/Service.
Likely:	Some evidence to indicate that the Assessment Point is not met due to: • Limited documentation provided/available; and • Practice/s inconsistent with understanding and/or application of protocols across SCU/Service.
Unlikely:	No evidence to indicate that the Assessment Point is not met due to: • Satisfactory documentation provided/available; and • Consistent practice/s in place; and • Consistent understanding and/or application of protocols across SCU/Service.

Risk-rating Tool

When assigning risk ratings in a self-assessment, a Service/SCU is to use the following tool: Please note that the Risk-rating Tool is consistent with the risk rating approach used by the National Surveyor in the Survey Risk Management Framework approved by the NQMC.

		Consequences: *Estimated severity of outcomes resulting from the assessment point being unmet*		
		Minor	**Significant**	**Severe**
Likelihood: *Estimated chance that the Service/SCU is not meeting the assessment point.*	**Almost certain**	Medium	Medium	High
	Likely	Low	Medium	Medium
	Unlikely	Low	Low	Medium