Data Management Strategy and Framework

Strategic Regional Environmental and Baseline Assessment program

NORTHERN TERRITORY GOVERNMENT

This SREBA Data Management Strategy and Framework was developed to meet the requirements set out in the SREBA Framework. The SREBA Framework was developed to guide the implementation of a SREBA to ensure alignment with the findings and recommendations of the Final Report of the Scientific Inquiry into Hydraulic Fracturing in the Northern Territory.

Flora and Fauna Division
Department of Environment, Parks and Water Security
PO Box 496
PALMERSTON NT 0831
sreba.ntg@nt.gov.au

Contents

Background

In April 2018, the Northern Territory Government accepted all 135 recommendations of the Final Report of the *Scientific Inquiry into Hydraulic Fracturing in the Northern Territory* (Final Report). A number of the recommendations relate to a Strategic Regional Environmental and Baseline Assessment (SREBA), which is a set of studies to address knowledge gaps and establish appropriate baselines against which the potential impacts of proposed onshore gas activities may be assessed. The SREBA covers six broad domains: water quality and quantity, aquatic ecosystems, terrestrial ecosystems, greenhouse gases, environmental health, and social cultural and economic studies.

The Northern Territory Government subsequently developed a SREBA Framework, which describes the objectives and content of a SREBA and provides detailed guidance notes describing how baseline studies should be undertaken in each domain, and includes the requirement for a SREBA Data Management Strategy which is a key component of addressing Recommendation 15.2 of the Final Report:

- Recommendation 15.2: That the regulator oversees the auditing and the data-collection processes and provides a central repository for all data informing any SREBA.

An integrated, strategic and coordinated approach to data collection over large regions with multiple interest holders assists in ensuring consistency between datasets and maximises their value for region-wide modelling and assessment. The Department of Environment, Parks and Water Security (DEPWS) coordinates the SREBA program for the Beetaloo Sub-basin.

Objectives

The overarching objectives of the SREBA Data Management Strategy are to ensure that SREBA related data and information is:

- Collated, stored and categorised in a manner that allows information to be easily discovered and accessible.
- Controlled, monitored, assured and protected using data governance and security.

Challenges

- Bringing together a diverse range of information collected by baseline studies that reside in different information management systems, formats and standards.

- Presenting the information in a manner that is transparent and assists users in locating information relevant to their needs.

Goals

The four goals of this strategy are to:

1) Ensure SREBA information is discoverable
2) Ensure SREBA information is transparent and accessible
3) Ensure SREBA information is protected and efficiently managed
4) Foster and strengthen data governance to improve data quality

Goal 1: Ensure SREBA information is discoverable

1.1   Develop and implement a SREBA data catalogue to make SREBA information discoverable.

A SREBA data catalogue has been developed and implemented to collect, organise and store SREBA metadata and information where required. The SREBA data catalogue will act as the central repository from which SREBA information is registered and made searchable and discoverable to the public.

1.2   Develop and implement a common metadata standard.

A metadata standard was defined to facilitate the consistent collection of metadata. Metadata will be used to identify, describe and categorise SREBA baseline study data and facilitate the search and discovery of information.

Goal 2: Ensure SREBA information is discoverable transparent and accessible

2.1   Alignment with the NTG Open Data Statement (2019).

Information collected from SREBA baseline studies is to be publicly available provided this does not breach privacy and confidentiality requirements, unduly compromise regulatory or commercial activities and is not culturally sensitive. Data collected by each domain will meet the following minimum standards as outlined in the Open Data Statement 2019 that data will:

- be in a machine-readable format; not be locked into formats and protocols that make it difficult to use and should include Application Programming Interfaces (API) where feasible
- include spatial coordinates or be spatially enabled where appropriate
- use Creative Commons licensing to authorise re-use, avoiding need for users to hold specialised software licenses wherever possible
- be collected from the source directly, where this is appropriate
- be depersonalised/anonymised where the data is about individual people or entities, and validated prior to upload to ensure protection of private or sensitive information (where validation is not successful, the data will not be published)
- be provided with descriptive metadata and categorised to facilitate searching and the ability to find related data
- preserve the value of the data by providing timely access.

Where data and information does not meet the minimum standard, the data and information will be reviewed and managed in accordance with the standards of the originating baseline study.

Goal 3: Ensure SREBA information is protected and efficiently managed

3.1 Review corporate infrastructure to ensure SREBA data is stored in a secure and managed environment in compliance with the Northern Territory's Information Privacy Principles as described in the Information Act 2002.

Data and information gathered for the SREBA baseline studies and for ongoing monitoring and evaluation will be publicly available online so long as privacy, cultural or commercial confidentiality requirements are not breached. Aboriginal cultural and ecological knowledge, and intellectual property will also be protected.

The collection and publication of data for the SREBA baseline studies will adhere to the Northern Territory's Information Privacy Principles as described in the *Information Act 2002*: https://infocomm.nt.gov.au/privacy/ information-privacy-principles.

All SREBA baseline study information is stored in existing DEPWS corporate systems including the SREBA data catalogue where feasible. The DEPWS corporate system environment has existing defined management practises to store and protect data in compliance with IPP 4 of the *Information Act 2002* requiring reasonable steps to be taken to protect data against misuse, modification, disclosure or unauthorised use, and ensure that data is destroyed or personal information de-identified when no longer required.

In order to ensure the protection of the data and information for the SREBA program, the following should be in place:

- protections that accord with the sensitivity of data
- management practices that are sufficient and suited to the type of data
- plans for the continuous management and safeguarding of data appropriately through the lifecycle of use, re-use and disposal
- controls to appropriately share the data and determine the suitability of data for sharing in accordance with Northern Territory Government privacy policies
- data management procedures that align with the Information Privacy Principles of the *Information Act 2002*

3.2 Identify and develop criteria to assess the sensitivity of SREBA information.

Metadata descriptions and records are essential for the management and oversight of sensitive information, as the metadata can describe the sensitive data without directly disclosing confidential information.

SREBA sensitive data management adopts principles set out by the Australian Research Data Council for the publication and sharing of sensitive data, and the standards set out in the National Statement on Ethical Conduct in Human Research (2007) - Updated 2018 | NHMRC. Where required, researchers should obtain Human Research Ethics approval and abide by the guidelines set out by the National Statement on Ethical Conduct in Human Research (2018).

The management and access to sensitive data will be done in accordance with data sensitivity plans and policies for the DEPWS division responsible for curating and managing the data. The level of desensitising data is dependent on the risk and can include processes to denature (generalising) or removal of information.

For SREBA information to be considered commercial-in-confidence, it should meet stringent criteria including that:

- the release of data and information would cause competitive detriment

- the data and information is not already publicly available

- the data it is not readily discoverable by other means.

Goal 4: Foster and strengthen data governance to improve data quality

4.1   Work with baseline studies teams to support data stewardship of the baseline study data

As part of the SREBA Data Management Strategy, key data governance roles for each SREBA baseline study were identified to ensure the management and oversight of SREBA data is undertaken for improved data quality outcomes where practical. These roles are listed in the table below.

Role	Description
Data Owner	Responsible for the management, quality, oversight and use of data for their respective SREBA study domain, including authorising access and release of SREBA baseline study information.
Data Steward	Delegated accountability and responsibility for the ongoing data quality and management of data for their respective SREBA study domain. They work to define and control the data and possess subject matter expertise within their SREBA baseline study domain.
Data Custodian	Responsible for the technical implementation of business rules, collection, storage, security and provision of the data for the SREBA baseline study domain

4.2   Identify and implement data governance workflows

Governance workflows within the SREBA Data Catalogue are to ensure SREBA data is secure, and reviewed and vetted before publishing. These workflows are automated and auditable to provide clear a record of SREBA data uploaded, reviewed, amended and published.

SREBA Data Management Framework

The SREBA Data Management Framework sets out the approach for collecting, preparing, and storing data and to ensure data is accessible to end users.

Data collected for SREBA Baseline studies uses existing processes and systems where appropriate. An overlying data catalogue has been developed for the SREBA program which collates and categorises data and information from existing systems in a centralised information management system to enable the information to be managed and discoverable. SREBA data catalogue is also a repository for new data and information.

Baseline studies undertaken for a SREBA draw on a range of existing information from different sources, as well as generating new data and information. The information will be used by different stakeholders for different purposes, and all stakeholders need to be confident that the data is reliable, and the scope and limitations of the information clearly explained. The SREBA Data Management Framework is to ensure that SREBA-related information maintains integrity as it is collated, summarised, analysed, and reported.

The Sensitive Data Management section outlines the process for managing access to data that is culturally sensitive or commercial-in-confidence, to ensure that privacy is protected and meets the requirements of the *Northern Territory Information Act 2002*. This includes consideration of protecting Aboriginal cultural and ecological knowledge and intellectual property.

Principles

The SREBA Data Management framework aligns with the Northern Territory Government principles-based approached to open data that recognises the value of data, compliance with legislation in the protection of sensitive data and the benefits of data sharing across government. In line with these principles and the guidance in the SREBA Framework, the SREBA Data Management framework is underpinned by the following principles:

- Open access to data and information wherever possible
- Protection of data that is culturally sensitive or commercial-in-confidence,
- Protection of privacy, including meeting the requirements of the Northern Territory Information *Act 2002*.
- Ensuring that the source and any licencing requirements of third-party data can be tracked.

SREBA data governance elements

The SREBA data governance elements described in this section are aligned with the data lifecycle illustrated below. The SREBA data governance elements are described in general and actual implementation of governance elements will vary between SREBA study domains.

Data Collection

The scope of data and information to be collected is determined in the detailed Scope of Works (SoW) developed for each Study Domain at the commencement of a SREBA, based on the Technical Guidance Notes in the SREBA Framework, and environmental and social attributes of the region. The scope of works will ensure that the scale and scope of the required data collection is:

- Necessary for the purpose and not co-incidental
- Efficient and focused on the purpose of a scope of works
- Abides by the Information Privacy Principles of *Information Act 2002*
- Meets ethical standards for the study domain

Metadata

Metadata is data that describes data and is used to describe information such as survey data, spatial data and reports. It assists in organising, making data discoverable and defining the scope of use. Core metadata was defined and collected for each study domain to describe SREBA data and information to make relevant information easier to find and manage.

Data Protection and Storage

All SREBA related information is stored in existing DEPWS corporate systems including the SREBA data catalogue. The DEPWS corporate system environment has existing defined management practises to store and protect data in compliance with IPP 4 of the *Information Act 2002* requiring reasonable steps to be taken to protect data against misuse, modification, disclosure or unauthorised use, and ensure that data is destroyed or personal information de-identified when no longer required.

In order to ensure the protection of the data and information for the SREBA program, the following procedures and processes are in place:

- protections that accord with the sensitivity of data
- management practices that are sufficient and suited to the type of data
- plans for the continuous management and safeguarding of data appropriately through the lifecycle of use, re-use and disposal
- controls to appropriately share the data and determine the suitability of data for sharing in accordance with Northern Territory Government privacy policies
- data management procedures that align with the Information Privacy Principles of the Information Act 2002.

Data Use and Sharing

For transparency all data and information collected from SREBA baseline studies will be made publicly available provided this does not breach privacy and confidentiality requirements, unduly compromise regulatory or commercial activities and is not culturally sensitive. The Sensitive data management included in this Data Management Strategy outlines the procedures and steps for managing sensitive data collected during SREBA baseline studies.

Where the Northern Territory Government owns the copyright for a report, data or information, permission will be granted for public use through a Creative Commons license.

The SREBA Data Management Strategy aligns with the Open Data Statement 2019 of the Northern Territory Government which commits to:

- make data publicly available for citizens and businesses to create value through digital innovations that will benefit the NT community and economy
- improve accountability and transparency across government
- promote public participation by encouraging feedback about open data and requests for new data
- openly publish data that does not infringe on the personal or commercial interests of others.

Data and information generated through SREBA studies will be available and accessible through the SREBA Data Catalogue available at: srebadata.nt.gov.au

Sensitive data management

Data gathered for the SREBA studies and for ongoing monitoring and evaluation will be publicly available online as long as doing so does not breach privacy, cultural or commercial confidentiality requirements. This SREBA Sensitive data management includes consideration of protecting Aboriginal cultural and ecological knowledge, and intellectual property.

The collection and publication of data for the SREBA studies will adhere to the Northern Territory Government Information Privacy Principles as described in the Information Act 2002: https://infocomm.nt.gov.au/privacy/ information-privacy-principles.

Metadata descriptions and records are essential for the management and oversight of sensitive information, as the metadata can describe the sensitive data without directly disclosing confidential information.

SREBA sensitive data management adopts principles set out by the Australian Research Data Council for the publication and sharing of sensitive data, and the standards set out in the National Statement on Ethical Conduct in Human Research (2007) - Updated 2018 | NHMRC. Where required, researchers should obtain Human Research Ethics approval and abide by the guidelines set out by the National Statement on Ethical Conduct in Human Research (2018) (See Appendix 1).

Sensitive data can include textual, numerical and\or spatial information, with the management and access to sensitive data done in accordance with data sensitivity plans and policies for the DEPWS division responsible for curating and managing the data. The level of desensitising data is dependent on the risk and can include processes to denature (generalising) or removal of information.

Commercial-in-confidence data

For SREBA data to be considered commercial-in-confidence, it should meet stringent criteria including that:

- the release of data and information would cause competitive detriment,
- the data and information is not already publicly available,
- the data it is not readily discoverable by other means.

If SREBA data and information do not meet these criteria, it will not be considered commercial-in confidence.

Disposal

The *Information Act 2002* prescribes that disposal schedules be established for the types of records held by government. At the time of development disposal schedules have not been developed for SREBA related data and information. Disposal schedules of SREBA related information will require review and approval by SREBA Study domain data owners.

Roles and responsibilities

As part of the SREBA Data Management Strategy, key data governance roles will be identified for each SREBA Study Domain.:

Role	Description
Data Owner	Responsible for the management, quality, oversight and use of data for their respective SREBA study domain, including authorising access and release of SREBA baseline study information.
Data Steward	Delegated accountability and responsibility for the ongoing data quality and management of data for their respective SREBA study domain. They work to define and control the data and possess subject matter expertise within their SREBA baseline study domain.
Data Custodian	Responsible for the technical implementation of business rules, collection, storage, security and provision of the data for the SREBA baseline study domain

SREBA Workflows

The SREBA Data Management Framework table below illustrates the steps in the SREBA approval workflow and the role responsible in the process.

Step	Action	Responsibility
SREBA data and information creation	SREBA baseline studies data and information is created by the relevant SREBA Study Domain	SREBA Study Domain
Review and assessment	SREBA data and information is submitted to Data Steward for review to ensure the content meets requirements and quality guidelines as required by the SREBA Study Domain	Data Steward
Obtain approval	Obtain necessary approvals from the SREBA Study domain Data Owner for the release and publication of data	Data Owner
Delivery of Data	Release and Publication of data within the SREBA Data Catalogue and NTG Corporate Systems	Data Steward Data Custodian

References

ARDC Ltd. (2022). Publishing Sensitive Data Viewed online at: https://doi.org/10.5281/zenodo.6565165

National Health and Medical Research Council (2018). *National Statement on Ethical Conduct in Human Research.* https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018

Northern Territory Government (2019) Open Data Statement | Digital Territory

Pepper R, Anderson A, Ashworth P, Beck V, Hart B, Jones D, Priestly B, Ritchie D and Smith R (2018) Final report of the scientific inquiry into hydraulic fracturing in the Northern Territory. https://frackinginquiry.nt.gov.au/inquiry-reports/final-report.

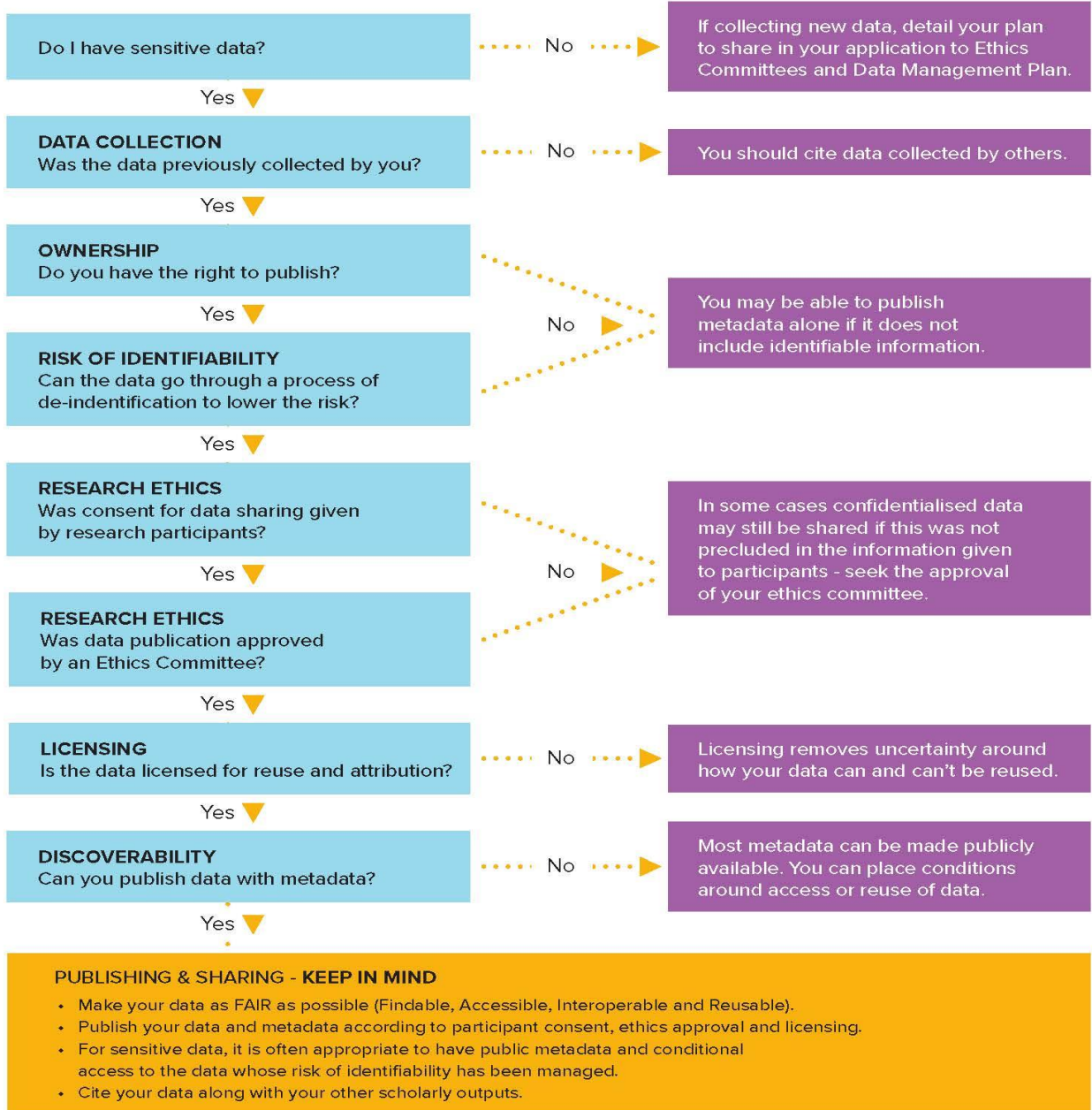# Appendix 1: Flowchart for publishing sensitive data

PUBLISHING SENSITIVE DATA

When and how to publish sensitive data as openly and ethically as possible.

For more information see: ardc.edu.au/resources/working-with-data

Sensitive data identifies individuals, species, objects or locations, and carries a risk of causing discrimination, harm or unwanted attention.

ARDC
Australian Research Data Commons

Do I have sensitive data? — No → If collecting new data, detail your plan to share in your application to Ethics Committees and Data Management Plan.

Yes ▼

DATA COLLECTION
Was the data previously collected by you? — No → You should cite data collected by others.

Yes ▼

OWNERSHIP
Do you have the right to publish?

Yes ▼

RISK OF IDENTIFIABILITY
Can the data go through a process of de-indentification to lower the risk?

No → You may be able to publish metadata alone if it does not include identifiable information.

Yes ▼

RESEARCH ETHICS
Was consent for data sharing given by research participants?

No → In some cases confidentialised data may still be shared if this was not precluded in the information given to participants - seek the approval of your ethics committee.

Yes ▼

RESEARCH ETHICS
Was data publication approved by an Ethics Committee?

Yes ▼

LICENSING
Is the data licensed for reuse and attribution? — No → Licensing removes uncertainty around how your data can and can't be reused.

Yes ▼

DISCOVERABILITY
Can you publish data with metadata? — No → Most metadata can be made publicly available. You can place conditions around access or reuse of data.

Yes ▼

PUBLISHING & SHARING - KEEP IN MIND
- Make your data as FAIR as possible (Findable, Accessible, Interoperable and Reusable).
- Publish your data and metadata according to participant consent, ethics approval and licensing.
- For sensitive data, it is often appropriate to have public metadata and conditional access to the data whose risk of identifiability has been managed.
- Cite your data along with your other scholarly outputs.

NCRIS
National Research
Infrastructure for Australia
An Australian Government Initiative

The ARDC
is enabled
by NCRIS