Australian Government

Department of Health

NATIONAL CANCER SCREENING REGISTER DATA ACCESS AND RELEASE POLICY

FOR RESEARCHERS AND EXTERNAL AGENCIES

October 2018

Table of Contents

1 SCOPE AND PURPOSE

1.1 Scope

1.1.1 The scope of the Department of Health's (the Department) Data Access and Release Policy for Researchers and External Agencies (the Policy) is data held in the National Cancer Screening Register (NCSR). It outlines the application of the Department's Data Access and Release Policy to data held in the NCSR.

1.1.2 The Policy is intended for researchers and external agencies. Researchers are people working for institutions and universities undertaking research where that research will benefit the health of the wider Australian community. External agencies are entities wishing to access NCSR data for research and evaluation purposes.

1.1.3 The NCSR currently holds information relating to the National Cervical Screening Program (NCSP), including individuals' personal information. It will hold bowel cancer screening information once the National Bowel Cancer Screening Program (NBCSP) transitions to the NCSR at which time the Policy will be updated.

1.1.4 Personal information cannot be used or disclosed unless agreed by the individual to whom the information relates, or if the information is being disclosed back to the person from whom the information was obtained, or if the use or disclosure is otherwise authorised under the NCSR Act or the Privacy Act.

1.1.5 Data that may be requested for human research may be:

- **Identified or identifiable data**: consists of data where an individual is explicitly identified or the identity of an individual can reasonably be ascertained. Examples of identifiers include the individual's name, date of birth or address. In particularly small sets of data, even information such as a postcode or particular medical or health characteristic may be an identifier.
- **Re-identifiable data**: consists of data from which some or all identifiers have been removed but where it remains possible to re-identify an individual whose information is included in the data by, for example, linking different data sets or having enough knowledge of an individual.
- **De-identified data**: consists of data that have never been labelled with individual identifiers, such as summary or aggregated data, or from which identifiers have been permanently removed, and by means of which no specific individual can be reasonably identified. Successfully de-identified data is not personal information, meaning the Privacy Act will generally not apply.[1] [2] [3]

1.1.6 While the Policy applies to both individually identified, identifiable or re-identifiable data (high risk data) as well as de-identified, summary or aggregated data (low risk data), it focuses on high risk data as it comprises personal information.

---

[1] *Guide to Big Data and the Australian Privacy Principles, Consultation Draft* May 2016. Office of the Australian Information Commissioner https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles

[2] *Privacy Business Resource 4: De-identification of data and information*. Office of the Australian Information Commissioner, https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information

[3] *Information policy agency resource 1: De-identification of data and information.* Office of the Australian Information Commissioner, https://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resource-1-de-identification-of-data-and-information

1.1.7 The *National Statement on Ethical Conduct in Human Research 2007* (Updated in May 2015) (the National Statement) relevantly defines human research as those that involve researchers having access to individuals' information as part of an existing published or unpublished source or database.[4]

1.1.8 The release of data will usually be on an ad-hoc/one-off basis. The need for regular extraction of data should be discussed with the Department.

1.1.9 The Policy does not apply to:

- data used for administering the operations of the NCSR, NCSP or the NBCSP (once transitioned to the NCSR), such as human resources data or financial data;
- outputs of data analytics by the NCSR, ie. ad hoc requests;
- media requests - these should be made through the Department's Media Unit at news@health.gov.au; and
- requests under the *Freedom of Information Act 1982* (Cwth) (FOI) – these should be made through Health's FOI Unit. More information about making an FOI request can be found at Health's FOI page.

1.2 Purpose

1.2.1 The purpose of the Policy is to outline the principles that underpin access to and release of data for research activities relating to healthcare, screening, cervical cancer and bowel cancer, to ensure accountability and consistency in the provision of access to data.

1.2.2 The NCSR holds electronic records of individuals participating in the NCSP and supports their program participation wherever they live. It is an integral part of cancer screening service delivery by facilitating invitations and reminders for screening, mailing of bowel test kits and supporting clinical decision-making.

1.2.3 The Department is the custodian of all data and has appointed a service provider to establish and maintain the operation of the NCSR. Telstra Health is the contracted service provider for the NCSR.

1.2.4 Further information regarding the NCSR can be accessed via www.ncsr.gov.au.

[4] p. 7 *National Statement on Ethical Conduct in Human Research 2007 (Updated in May 2015)*. The National Health and Medical Research Council, the Australian Research Vice-Chancellor's Committee. Commonwealth of Australia, Canberra. www.nhmrc.gov.au/guidelines-publications/e72

2 BACKGROUND

2.1 Legal basis - The NCSR legislation

2.1.1 The *National Cancer Screening Register Act 2016* (the NCSR Act) provides that a purpose of the NCSR is to facilitate research relating to healthcare, screening, cervical cancer or bowel cancer in recognition of the importance of data being made available for the purposes of research which benefits the community.

2.1.2 The NCSR Act authorises an officer of the Commonwealth to disclose personal information for the purposes of research where it is of a kind that is approved by the Guidelines Under Section 95 of the *Privacy Act 1988* and the Guidelines under Section 95A of the *Privacy Act 1988* (collectively the Guidelines under Section 95 and Section 95A of the Privacy Act) and only if the disclosure is in accordance with those Guidelines.

2.1.3 Implementation of the Policy will be consistent with the applicable legislation. Further information regarding the legal basis for the Policy, including the Guidelines under Section 95 and Section 95A of the Privacy Act, is provided at **Appendix A.**

2.2 Participating States and Territories

2.2.1 In working together to support the successful operation of the NCSR, the Commonwealth has entered into a Memorandum of Understanding (MoU) with States and Territories to provide for data sharing with States and Territories who have agreed to participate in the NCSR (participating States and Territories).

2.2.2 Sharing of data with participating States and Territories enables service delivery, service planning and health promotion activities for participants of the NCSP and the NBCSP (once transitioned to the NCSR) in those States and Territories.

2.2.3 The NCSR Act provides that a participating State or Territory, or an officer, employee, contractor, or other persons authorised by a participating State, Territory or State or Territory authority may collect, make a record of, use or disclose protected information or key information included in the NCSR, if required or permitted by State or Territory law. This applies to disclosure of NCSR information shared by the Commonwealth under the MoU arrangements for the purpose of research.

2.2.4 A list of the States and Territories participating in the NCSR and their contacts is provided at **Appendix B.**

2.3 State and Territory laws related to privacy and freedom of information

2.3.1 Research and other organisations seeking state-specific data from the participating State or Territory on the NCSP and NBCSP (once transitioned to the NCSR) should be aware that State and Territory laws related to privacy generally or health records in particular, may have a bearing on access to personal information for research purposes and/or the way in which proposed research must be conducted. Some jurisdictions have included stricter limitation on the handling of personal information or health records.

2.3.2 Similarly, each State and Territory has legislation equivalent to the FOI which applies to data held by States and Territories relating to the NCSP and NBCSP

(once transitioned to the NCSR). Requests to access state-specific program data will be managed by each State and Territory under their existing freedom of information legislation.

2.3.3 A list of relevant State and Territory privacy and health information legislation is provided at **Appendix C**.

2.3.4 It is the responsibility of researchers to be aware of the legal requirements, wherever relevant.

3 DATA ACCESS AND RELEASE PRINCIPLES

3.1 Data will be managed as an asset

3.1.1 Data held in the NCSR is a national asset and the Department is the custodian of all data. As the data custodian, the Department will have control over information in the NCSR, especially with respect to protection of identified/identifiable and re-identifiable data. This includes establishing adequate controls over the use and disclosure of data when permitting the release of personal information for research purposes and retaining continued accountability for ensuring these controls are maintained at all times.

3.2 Personal information must be protected

3.2.1 The privacy of citizens is of paramount importance. Personal information cannot be used or disclosed unless agreed by the individual to whom the information relates, or if the information is being disclosed back to the person from whom the information was obtained, or if the use or disclosure is otherwise authorised under the NCSR Act or the Privacy Act.

3.2.2 Where a decision is made to release high risk data, the Department will consider whether only elements of data relevant and essential to meet the purpose of a reasonable research request should be made accessible. In agreeing to release high risk data, the Department will develop and implement a legally binding agreement with the recipient of data. The agreement will require researchers to agree to specific terms and conditions for receiving data, specifically that data is used only for the purpose for which it was released.

3.2.3 High risk data must not be published in a format that may potentially identify an individual and must not be used for secondary purposes unless agreed by the individual or required or authorised under legislation.

3.3 Research must have a public benefit

3.3.1 The research request must have a public benefit that can reasonably be expected to support improvement of the health or wellbeing of Australians in relation to cervical screening, cervical cancer, or bowel screening or bowel cancer (once the NBCSP has transition to the NCSR).

3.4 Research must be ethical

3.4.1 Research must consider the moral and ethical factors surrounding the access and use of data. Research involving data on Indigenous participants must comply with the National Statement, *Values and Ethics: Guidelines for Ethical Conduct in*

Aboriginal and Torres Strait Islander Health Research (NHMRC 2003) and the principles of use, storage and access as outlined in the *Guidelines for Ethical Research in Australian Indigenous Studies* (Australian Institute of Aboriginal and Torres Strait Islander Studies 2002) specifically in regard to respect for and valuing of cultural and language diversity.

3.5 Research must be consistent with applicable legislation

3.5.1 In striking a balance between the benefits of research to the community and the legal obligation to protect personal privacy, the Department must ensure that the access, release and use of data complies with the NCSR Act and the Privacy Act, including the Guidelines under Sections 95 and 95A of the Privacy Act.

4 DATA ACCESS AND RELEASE PROCESS

4.1 Health's Data Governance and Release Framework

4.1.1 The Policy adopts the Department's Data Governance and Release Framework (the Framework) for data access and release. The aim of the Framework is to enable greatest possible use of the Department data while ensuring privacy and confidentiality are preserved, and to ensure consistent decisions are made regarding data access requests.

4.1.2 In line with the Framework, this Policy incorporates a Risk Assessment model that uses the Five Safes Principles: safe project, safe data, safe people, safe settings and safe output.

4.2 Types of data

4.2.1 Requests for data may fall into two data types, or may be a combination of two data types:

- Low risk: de-identified, summary or aggregated data; and
- High risk: identified, identifiable and re-identifiable data.

4.2.2 Requests for data can only apply to data held in the NCSR, not program data held by participating States and Territories.

4.3 State and Territory data

4.3.1 Researchers may approach a participating State or Territory to request data held by the State or Territory in relation to the NCSP or the NBCSP (once transitioned to the NCSR). State and Territory contact details for data requests is located at **Attachment B**. The State or Territory will use their existing legislation and data access and release policies and processes when making a decision regarding the release of their state-held data. (A list of relevant State and Territory privacy and health legislation is provided at **Appendix C**.) If no policy exists, the State or Territory may adapt the principles in this Policy when assessing the research proposal or data request.

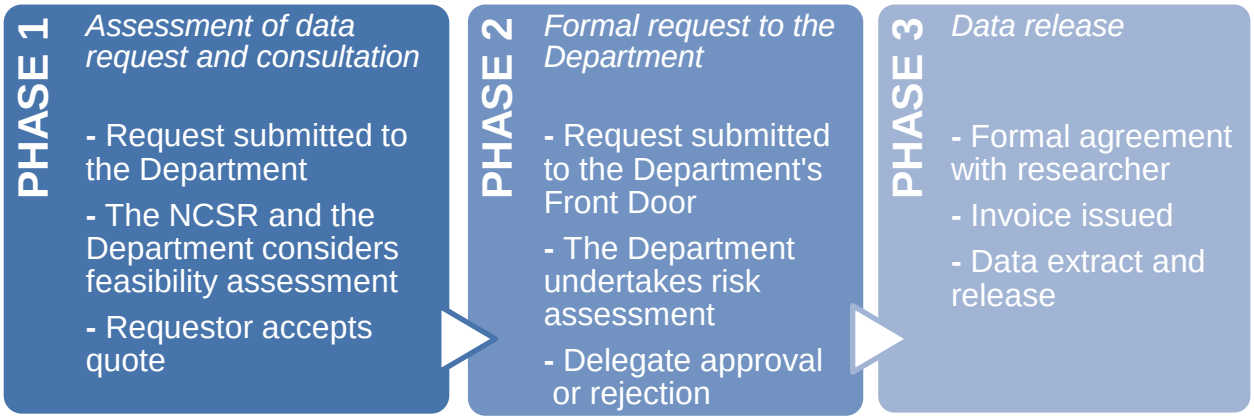
4.3.2 A State or Territory may refer a data request to the Department for action. Data requests referred from States and Territories will undergo the procedures outlined in the Policy.

4.3.3 Where a researcher has approached the Department for state-specific data, the Department will consult the participating State or Territory during the initial assessment process regarding the research request. The Department will consult the relevant State or Territory regarding any research that uses that jurisdiction's data and notify the State or Territory regarding the proposed release of any data/research at the State/Territory level.

4.4 Outline of the NCSR Data request process

4.4.1 The diagram below shows a high level summary of the steps the Department undertakes when processing data requests.

Note: Low risk data requests are risk assessed in the first phase of the process, however **Medium risk** and **High risk** data requests are risk assessed in the second phase. The flowchart at **Appendix D** demonstrates this detail.



4.5 Steps for data access

4.5.1 The steps for data access and the guiding principles underpinning each of the steps are provided below and at the flowchart at **Appendix D**.

Phase 1 - Initial assessment of data request and consultation

4.5.2 In the first instance, requestors are required to complete the *NCSR Data Request Form* via the online smart form or submit the printed form via email to ncsr.data.requests@health.gov.au managed by the Cancer Policy, Screening and Services Taskforce at the Department.

4.5.3 The Form facilitates requestors to provide sufficient information regarding the proposed research, including the types of data required and the variables, such as date range, location, population groups and supporting documentation. The Form also collects information required by the Department to undertake the necessary risk assessments required under Phase 1 and Phase 2.

4.5.4 The data request will be referred from the Department to the NCSR to review the data requirement to determine their precise data needs and the feasibility of the request.

4.5.5 The NCSR will provide the Department an assessment of the data request together with a recommendation regarding the feasibility of servicing the proposed research request.

4.5.6 Where the request for data is state specific, the relevant participating State or Territory will be consulted during the initial assessment state.

4.5.7 The Department will consider the NCSR's assessment of the data request, feedback from the jurisdiction(s) where relevant, and a risk assessment for low risk data requests (de-identified, summary or aggregated data) will be prepared.

4.5.8 Requestors may be required to pay for the cost of their data request which quantifies the effort required to extract and customise the required data. The Department will consider cost recovery on a case-by-case basis and, in consultation with the NCSR provider, will provide an indicative cost based on estimated time in hours and the requirements of the data request.

4.5.9 The quote will be prepared by the Department which will include a fee for the NCSR to cover the processing of the request, including the cost of extraction and quality assurance. The quote will be provided to the requestor at Step 5 for consideration. Requestors must accept the quote in order to progress through the process to obtain data.

4.5.10 Human Research Ethics Committee (HREC) approval is required to be obtained (if not already granted) in Phase 1. All research involving human participants is required to undergo ethical review.

4.5.11 The quote can be used by the requestor to provide evidence to the HREC that the researcher has engaged with the Department, and that the Department as the data custodian understands the type of data being requested for research purposes.

4.5.12 Requestors seeking access to data must provide evidence of ethics approval from a properly constituted HREC. The HREC will advise the Department and the research applicant whether or not the reviewed research proposal is acceptable on ethical grounds and, where the research has not been approved, provide reasons linked to the National Statement, for those decisions.

Note: Under the NCSR Act, a HREC must give approval for the collection, use or disclosure of health information for the purpose of human research relevant to public health or public safety, in accordance with the Guidelines under Sections 95 and 95A of the Privacy Act. Where proposed research has the consent of individuals, compliance with the Guidelines under Sections 95 and 95A of the Privacy Act as set out in the Policy is not required. However, release of data is subject to the HREC making a judgement that the research proposal meets the requirements of the National Statement, including that the consent from individuals is valid. For consent to be valid, it must be free, informed, competent and current.

Phase 2 – Formal request to Health

4.5.13 Once the Department's quote has been accepted by the researcher and evidence of HREC approval has been submitted, researchers requesting access to medium risk and high risk data can proceed through to Phase 2.

> **Note:** Researchers requesting low risk data consisting of de-identified, summary or aggregated data will not be required to complete Step 6 to Step 8 of the process flowchart at **Appendix D**, as the risk assessment will occur at Step 3 of Phase 1 for those data requests.

4.5.14 Researchers requesting medium risk to high risk data consisting of identified, identifiable and re-identifiable data will be required to submit their *NCSR Data Request Form* together with evidence of HREC approval to the Department's Front Door for risk assessment processing.

4.5.15 Other information that will facilitate consideration of the data request includes the project outline and any risk assessment already undertaken. Where the proposed research has the consent of individuals, evidence of consent from individuals, or how this will be obtained, must be provided.

4.5.16 The Department will undertake an assessment of the consequences vs likelihood of data disclosures in consultation with the NCSR. The risk assessment will consider if the data release risks can be reduced to an appropriate level, however, if it is deemed the risks cannot be mitigated effectively (e.g. residual risks too high), the request will be denied. The assessment process will also determine the value of the data request in meeting NCSP outcomes, as well as consider risks to the population screening programs (which is not confined to protection of personal information). For example, depending on how aggregated data is used, while it is classified as low risk, it can become high risk from a NCSR Program rather than personal privacy perspective.

4.5.17 Appropriate delegation for approving data release will be assigned according to the data disclosure risks identified in the risk assessment. The Department's delegate will consider the outcome of the risk assessment in making a decision to release the requested data. Delegate approval is required prior to extraction and release of data.

4.5.18 The authority to release data lies with the Department. The Department must be satisfied that the proposed research for which personal information is required has been approved by a HREC for the particular purpose in accordance with the Guidelines under Sections 95 and 95A of the Privacy Act or that the researcher has the consent of the relevant individuals to obtain their personal information.

4.5.19 The Department as the data custodian may decline to release data on grounds unrelated to ethical issues, for example, NCSR Program considerations. HREC approval does not guarantee the Department's delegate support for the release of data.

Phase 3 – Data release

4.5.20 Where only de-identified data has been approved for release for research purposes, the NCSR will determine the appropriate methods of de-identification of data prior to release to ensure that personal information is protected and used for its intended purpose. De-identification may include combining data into categories, for example, combining age groups and expressing data in ranges, or altering identifiable information in a small way such that the aggregate information or data is not significantly affected but the original values cannot be known with certainty.[5]

4.5.21 Researchers will be required to sign a legally binding agreement in order for the Department to release high risk data (identified or identifiable data) for research purposes. The agreement will require researchers to agree to specific terms and conditions for receiving data, specifically that the data is used only for the purpose for which it was released.

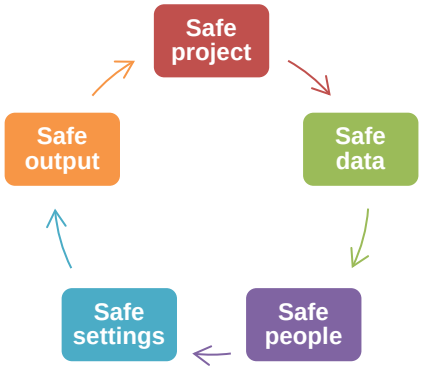
4.5.22 Upon execution of the formal agreement, the Department will provide the researcher an invoice for the data request and the timeline for release of data. For the final step of the process, the Department will authorise the NCSR to extract and release data to the researcher in a timely manner.

[5] *Privacy Business Resource 4 – De-identification of data and information*, April 2014. Office of the Australian Information Commissioner https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information.pdf

5 RISK ASSESSMENT

5.1 The Risk Assessment Model

5.1.1 In undertaking the risk assessment, the Department in consultation with the NCSR will adopt the Five Safes Principles as the basis for considering data access and release requests and assessing disclosure risk.



5.1.2 Questions that will be considered as part of the risk assessment process include, but are not limited to, the following:

Safe project

- Is this the project a valid question that can be answered with the requested data?
  - Consider the legal, moral and ethical considerations that relate to the use of data
  - Has the project been assessed by a HREC (if required)?
- Is there a possibility of distortion or misrepresentation of information on output and whether this poses a risk to reputation for data subjects or the Department?

Safe data

- Is there disclosure risk in the data itself?
  - Consider the potential for identification in the data as well as the sensitivity or uniqueness of data characteristics that could lead to identification
- Was consent sought? Are there direct and recognisable identifiers?

Safe people

- Can the requestor be trusted to use data appropriately?
  - Consider the knowledge, skills and incentives of the data users to appropriately store and use data in accordance with the expected or required standards of behaviour
- Will the data user have the basic technical ability to understand the restriction and not contribute to inadvertent breaches of privacy?

Safe settings

- Are the facilities for the conduct of the project appropriate to protect data from deliberate and accidental information disclosure?
  - Consider the practical controls on how data will be accessed, including the physical environment and procedural arrangements to assess likelihood of deliberate or accidental disclosure.
- How effective are the controls around authorised access to data and the likely effectiveness of controls on unauthorised access?

Safe outputs

- How will the outcomes of the project be communicated to the intended audience?
  - Consider the risk that sensitive information could be published in the analysis products, the best approach to the type of data and where the focus should be when controlling output risks.
- Could the outcome trigger reputational harm to the persons represented in the data, the Department or the government?

5.2 Risk management

5.2.1 Depending on the risk rating of the assessment undertaken, for example low risk to extreme high risk, the data request may be referred to the Department's Data Request Assessment Panel for further risk management where required.

6 AGREEMENT FOR DATA RELEASE

6.1 Terms and conditions of use of high risk data

6.1.1 The legally binding agreement for the handling of identified, identifiable and re-identifiable data will include terms and conditions relating to:

(a) Using the information only for the purpose specified on the *NCSR Data Request Form*, that is, medical research relevant to healthcare, screening, cervical cancer and bowel cancer;

(b) Ensuring data is not published in a format that could potentially identify an individual consumer;

(c) Taking reasonable steps to protect personal information from misuse and loss and to protect information from unauthorised access, modification or disclosure:

- Data must be stored securely and only those named in the request form may have access to it
- Any changes to staff who hold data must be notified to the Department
- New staff must agree to the terms and conditions for the handling of identified, identifiable and re-identifiable data;

(d) Agreeing to other applicable limitations on usage of identified/identifiable data, such as:

- The information must not be used for commercial purposes
- No attempt must be made to derive information about individuals
- No contact with individuals identified in the data must be made unless prior arrangements have been made with the Department
- Data must not be provided to a third party
- Data must not be linked to another dataset without prior approval from the Department.

6.1.2 The Department may also impose other conditions on a case-by-case basis, including requesting that:

- Data is not published without first informing the Department
- The Department is acknowledged in all publications and reports where data has been used
- A copy of all released reports or published manuscripts is provided to the Department prior to their release.

6.1.3 The Department reserves the right to specify other compliance requirements as a condition of approving release of data.

6.1.4 All data released by the Department will be accompanied by explanatory material that:

- Identifies the scope of data and the assumptions or interpretations made in selecting that data as relating to a given topic
- Makes clear any limitations or qualifications relating to the provenance, quality, completeness, or currency of data
- Makes clear any requirements on the recipient in terms of re-use of data, including requirements to ensure that the accompanying explanatory material always accompanies data when it is circulated or published.

6.1.5 Where applicable, available information (including metadata) will be provided with the release of data to ensure data is interpreted correctly. Any qualifications and limitations that would apply to data released will also be provided.

7 CONTACT INFORMATION

7.1.1 Cancer Policy, Screening and Services Taskforce:
ncsr.data.requests@health.gov.au

7.1.2 The Department's Front Door for data requests:
data.release@health.gov.au

8 REVIEW OF THIS POLICY

8.1.1 To ensure currency and relevance of the Policy to the needs of researchers and obligation of the Department to protect personal privacy, this document will be reviewed after 6 months of operation of the NCSR and thereafter at twelve month intervals.

9 DEFINITIONS

Aggregated data means any data set where the data is created by extracting data from one or more existing data assets, manipulating it and storing the results.

AIHW means the Australian Institute of Health and Welfare.

APPs means the Australian Privacy Principles.

APP entity means an agency or organisation within the meaning of the *Privacy Act 1988* (Cth).

Australian Code means the *Australian Code for the Responsible Conduct of Research.*

Contracted service provider means the service provider engaged by Health to undertake the design, build and operation of the NCSR. Telstra Health, a subsidiary division of Telstra Corporation Limited is the current service provider responsible for delivering the operational and support services required to enable and facilitate the NCSR services in order to meet specific outcomes.

Data means information or data (including identified and identifiable unit records) held in the NCSR. It includes identified and identifiable unit records held in the NCSR for the purpose of supporting the operation of the NCSP.

Data integration means combination of information from different data sources to produce new datasets.

De-identified data means a record that cannot be linked to an individual ('non-identifiable').

Guidelines under Section 95 and Section 95A of the Privacy Act means collectively the *Guidelines Under Section 95 of the Privacy Act 1988* and the *Guidelines Under Section 95A of the Privacy Act 1988*.

High Risk Data means identified/identifiable and re-identifiable data.

HREC means Human Research and Ethics Committee.

Human research has the same meaning as in the *National Statement on Ethical Conduct in Human Research 2007 (Updated in May 2015)* and includes researchers having access to individually identifiable, re-identifiable or non-identifiable information as part of an existing published or unpublished source or database.

Identified data means data in which an individual is explicitly identified.

Identifiable data means data in which the identity of an individual can be reasonably ascertained.

IA means Integrating Authorities that undertake high risk data integration projects involving Commonwealth data for statistical and research purposes.

Low Risk Data means summary, aggregated or de-identified data.

National Statement means the *National Statement on Ethical Conduct in Human Research 2007 (Updated in May 2015)* developed jointly by the National Health and Medical Research Council and the Australian Research Vice-Chancellor's Committee.

NBCSP means the National Bowel Cancer Screening Program.

NCSP means the National Cervical Screening Program.

NCSR means the National Cancer Screening Register.

NCSR Act means the *National Cancer Screening Register Act 2016*.

NCSR Consequential and Transitional Provisions Act means the *National Cancer Screening Register (Consequential and Transitional Provisions) Act 2016*.

Participating State or Territory has the same meaning as in section 4 of the NCSR Act.

Personal information has the same meaning as in the *Privacy Act 1988* (Cth).

Policy means the *Data Access and Release Policy for Researchers and External Agencies.*

Privacy Act means the *Privacy Act 1988* (Cth).

Protected information has the same meaning as in section 4 of the NCSR Act.

PSPF means the Australian Government Protective Security Policy Framework which provides policy, guidance and better practice advice for governance, personnel, physical and information security.

Research means research, compilation or analysis of statistics.

Section 95 Guidelines means the *Guidelines* under *Section 95 of the Privacy Act 1988.*

Section 95A Guidelines means the *Guidelines* under *Section 95A of the Privacy Act 1988.*

Telstra Health see **Contracted service provider**.

The Department means the Australian Government Department of Health.

Appendix A Legal Basis

1. The NCSR legislation

The NCSR legislation, comprising the NCSR Act and the *National Cancer Screening Register (Consequential and Transitional Provisions) Act 2016* (the Consequential and Transitional Provisions Act), creates a legislative framework for the establishment and ongoing operation of the NCSR. The NCSR legislation commenced on 21 October 2016.

The NCSR Act regulates the collection, use and disclosure of information in the NCSR. Such information may include an individual's personal information and key information, such as contact details, information about screening tests undergone or to be undergone by the individual, test results/outcome data and results of relevant follow-up procedures. It may also include information about the individual's diagnosis with, or a precursor to, cervical cancer or bowel cancer, or clearance from cervical cancer or bowel cancer.

'Personal information' in the NCSR Act has the same meaning as in the *Privacy Act 1988* (Cth) (the Privacy Act).

'Personal information' held in the NCSR, that is information about an identified individual or an individual who is reasonably identifiable, or which is derived from information in the NCSR or derived from a use or disclosure of information included in the NCSR or obtained under or in accordance with the NCSR Act, is 'protected information' for the purpose of the NCSR Act (section 4 of the NCSR Act). Subject to exceptions, it is an offence for a person to make a record of, disclose or otherwise use 'protected information' where it is not authorised by the NCSR Act (section 18 of the NCSR Act).

Under the NCSR Act, 'protected information' includes commercial-in-confidence information as well as personal information. While the NCSR Act treats both commercial-in-confidence information and personal information as 'protected information', the research provision in the NCSR Act applies to personal information only.

The NCSR Act provides that a purpose of the NCSR is to facilitate research relating to healthcare, screening, cervical cancer or bowel cancer (paragraph 12(1)(n) of the NCSR Act), in recognition of the importance of data being made available for the purposes of research which benefits the community.

The NCSR Act authorises an officer of the Commonwealth to disclose personal information for the purposes of research where it is of a kind that is approved by the *Guidelines Under Section 95 of the Privacy Act 1988* and the *Guidelines Under Section 95A of the Privacy Act 1988* (collectively the Guidelines under Section 95 and Section 95A of the Privacy Act) and only if the disclosure is in accordance with those Guidelines (sub-section 17(5) of the NCSR Act).

2. The *Privacy Act 1988*

2.1 Re-identification of de-identified government data

At the time of drafting, the Privacy Amendment (Re-identification Offence) Bill 2016 has been introduced into parliament which seeks to further protect de-identified information published or released by Commonwealth entities from being re-identified. The amendments to the Privacy Act included in the Bill if passed will make it a criminal offence to re-identify de-identified government data. It would also make it an offence to counsel, procure, facilitate, or encourage anyone to re-identify de-identified data, and to publish or communicate any re-identified dataset. The new offences would apply to actions taken on or after 29 September 2016.

Entities that would be subject to the amendments to the Privacy Act proposed in the Bill include organisations, including small businesses, as well as individuals. It has a wider scope than the rest of the provisions in the Privacy Act which do not apply to acts of small businesses conducted outside of a Commonwealth contract or individuals conducted outside of the course of business.

This wider scope reflects the importance of a general deterrent to the re-identification of de-identified personal information, rather than a deterrent limited to entities subject to the Privacy Act.[6]

3. The Guidelines under Sections 95 and 95A of the Privacy Act and research

The Guidelines under Sections 95 and 95A of the Privacy Act provide a framework for making decisions about whether particular types of research involving the handling of personal information obtained by Commonwealth agencies should be conducted to ensure that such information is protected against unauthorised collection or disclosure.

Compliance with the Guidelines under Sections 95 and 95A of the Privacy Act allows the handling of health information where not otherwise authorised under the Privacy Act. The Guidelines under Sections 95 and 95A of the Privacy Act do not replace the Australian Privacy Principle (APPs) or the Privacy Act but must be used in conjunction with the APPs and the Privacy Act.

3.1 Guidelines under Section 95 of the Privacy Act 1988

Health is bound to protect personal information in accordance with the Privacy Act. Health must comply with the *Guidelines Under Section 95 of the Privacy Act 1988* (Section 95 Guidelines) in order to disclose personal information to a researcher without an individual's consent in circumstances where it would not otherwise be authorised under the Privacy Act.

The Section 95 Guidelines include requirements for seeking and obtaining approval from a Human Research Ethics Committee (HREC) for release of identified or identifiable information. It contains procedures for weighing the public interest in the research against the public interest in the protection of privacy. In these situations, an agency may collect, use or disclose records containing personal information for medical research purposes without breaching the Privacy Act if the proposed medical research has been approved by a properly constituted HREC in accordance with the Section 95 Guidelines.[7]

In reaching a decision under the Section 95 Guidelines, a HREC will:

- Identify and consider the APPs that might be breached in the course of the proposed research, including whether it is necessary for the research to use identified or potentially identifiable Data, and whether it is reasonable for the research to proceed without the consent of the individuals to whom the information relates; and
- Ensure that the committee has the competence to determine if the public interest in the proposed research outweighs, or does not outweigh, the public interest in the protection of privacy. If the public interest in the proposed research does not outweigh the public interest in the protection of privacy, then the HREC will not approve the handling of personal information for that research.

3.2 Guidelines under Section 95A of the Privacy Act 1988

The *Guidelines Under Section 95A of the Privacy Act 1988* (Section 95A Guidelines) relevantly provide a framework for HRECs and those involved in conducting research to weigh the public interest in research relevant to public health or public safety against the public interest in the protection of privacy. It contains procedures to follow in preparing proposals to be submitted to an HREC for approval to collect, use or disclose health information held by organisations without an individual's consent and procedures for HRECs to follow when considering proposals.[8]
The application of the Section 95A Guidelines are significantly broader than for the Section 95 Guidelines. The section 95A Guidelines apply to the collection, use or disclosure of health information by organisations in the private sector for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety, and to the collection of health information held by organisations for the purpose of health service management.

---

[6] Explanatory Memorandum, Privacy Amendment (Re-identification Offence) Bill 2016, Attorney General's Department.
[7] *Guidelines Under Section 95 of the Privacy Act 1988*. National Health and Medical Research Council /www.legislation.gov.au/Details/F2014L01500/Supporting%20Material/Text
[8] *Guidelines Under Section 95A of the Privacy Act 1988*. National Health and Medical Research Council https://www.legislation.gov.au/Details/F2014L00243

In reaching a decision under the Section 95A Guidelines, a HREC will:

- Consider whether the proposal complies with the relevant APPs in the course of the collection of health information or the use and disclosure of health information;
- Consider whether the purpose of the proposed activity can be achieved using de-identified data and whether it is impracticable to collect, use or disclose health information for the proposed activity with the consent of the individual(s) involved; and
- Determine if the public interest in the proposed activity substantially outweighs, or does not substantially outweigh, the public interest in the protection of privacy.

3.3 Human Research Ethics Committees (HRECs)

There are more than 200 HRECs available in institutions and organisations across Australia. For more information on HRECs, including a list of HRECs that apply the Guidelines under Section 95 and the Guidelines approved under Section 95A of the Privacy Act 1988, please visit the National Health and Medical Research Council (NHMRC) website.

4. *Freedom of Information Act 1982*

The Consequential and Transitional Provisions Act amends the *Freedom of Information Act 1982* (Cth) (the FOI Act) to permit information in the NCSR to be exempt from disclosure under section 38 of the FOI Act in response to a FOI request where it would be an offence to disclose under s18 of the NCSR Act.

The FOI exemption will ensure that the privacy of individuals is protected by limiting disclosure of personal information held in the NCSR in response to a FOI request.

Appendix B States and Territories Contact Details

Following are the contact details for data requests from States and Territories participating in the NCSR for the purposes of supporting the implementation of the NCSP and the team contacts in each participating State and Territory:

State or Territory	Key contacts
New South Wales	Program Manager CINSW ScreeningAndPreventionData@health.nsw.gov.au
Victoria	Program Manager Screening and Cancer Prevention (03) 9096 0402
Queensland	Director Cancer Screening Unit CSSB@health.qld.gov.au
Western Australia	WA Cervical Cancer Prevention Program Cervicalscreening@health.wa.gov.au
South Australia	Prevention and Population Health Branch Julie.Patterson@sa.gov.au (08) 8226 7029
Tasmania	Population Screening and Cancer Prevention cscsadministration@ths.tas.gov.au (03) 6166 6910
Northern Territory	Manager Cancer Screening Services CervicalScreenNTRegister.DOH@nt.gov.au (08) 8922 6445
Australian Capital Territory	Prevention and Population Health cancerscreening@act.gov.au healthinfo@act.gov.au

Appendix C State and Territory Legislation

Relevant State and Territory privacy and health information legislation:

- *Public Health Regulation 2000* (ACT)
- *Health Records (Privacy and Access) Act 1997* (ACT)
- *Information Privacy Act 2014* (ACT)
- *Public Health Act 2010* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Public and Environmental Health Regulations* (NT)
- *Information Act* (NT)
- *Public Health Act 2005* (QLD)
- *Information Privacy Act 2009* (QLD)
- *South Australian Public Health Act 2011* (SA)
- Information Privacy Principles Instruction (SA)
- *Public Health Act 1997* (TAS)
- *Personal Information Protection Act 2004* (TAS)
- *Cancer Act 1958* (VIC)
- *Health Records Act 2001* (VIC)
- *Privacy and Data Protection Act 2014* (VIC)
- *Improving Cancer Outcomes Act 2014* (VIC)
- *Health (Cervical Screening Register) Regulations 1991* (WA)

Appendix D Data Access and Release Policy - Process Flowchart