National Cancer Screening Register

Privacy Impact Assessment

Department of Health

December 2016

Clayton Utz

Table of Contents

1. Executive summary

This Privacy Impact Assessment (**PIA**) assesses the potential privacy compliance and management issues associated with the National Cancer Screening Register (**NCSR**). This PIA focuses on the information flows and privacy concerns arising from establishing and operating the NCSR.

The NCSR is a single national screening register to collect and report screening data which will commence operations for the National Bowel Cancer Screening Program (**NBCSP)** from 20 March 2017 and for the National Cervical Screening Program (**NCSP**) from 1 May 2017. The NCSR will initially support the NCSP and the NBCSP, with a view to supporting further cancer screening programs in the future.

Establishing the NCSR will involve a substantial amount of data migration and cleansing. The large scale data merging will create a substantial repository of data that various people and entities can access which presents privacy implications. This PIA has made a number of recommendations (summarised in section 2 below) to address the privacy management risks. Amongst others, these recommendations include:

- communicating to individuals what and how information relating to them will be collected, used and disclosed by the NCSR, including through an appropriate privacy notice;
- ensuring that the NCSR privacy policy and privacy notices set out appropriate information for individuals to understand how their information will be handled;
- implementing a privacy governance and management strategy;
- ensuring that individuals are aware of their right to seek correction of their information in the NCSR or opt out of participation in a cancer screening program;
- ensuring that any person with access to information in the NCSR receives privacy training and that appropriate security and access controls are in place to prevent unauthorised disclosure;
- ensuring that an appropriate data access and release policy is implemented to regulate the disclosure of identified and de-identified information in the NCSR to third parties; and
- ensuring that the migration of data from the current registers is handled in a way that minimises the risk of inaccurate matches and duplicate records.

This PIA is set out in a number of sections. The first substantive section (section 3) explains what a PIA is and elaborates on the approach of this PIA, including some assumptions and limitations. Section 4 of this PIA provides some background information on the NCSR and the context of its establishment and discusses how the NCSR will collect, use and disclose personal information and the legislative backing for the NCSR. Section 5 sets out information flows illustrating the various entities collecting, using and disclosing personal information as part of the NCSR. Section 6 analyses the NCSR in light of the APPs while section 7 considers privacy impacts and management strategies on particular issues.

For ease of reference, a glossary is provided in Schedule 1 and definitions are set out in Schedule 2.

2. Summary of recommendations

Below is a summary of the recommendations made in this PIA. The number of each Recommendation reflects the order in which they are made in the text of this PIA. However, to assist with context and for ease of reading, the recommendations are grouped thematically.

PRIVACY POLICY

Recommendation 1 The NCSR should have an easily accessible online privacy policy setting out how the NCSR collects personal information, the kinds of personal information collected, the purposes for which the information is collected, held, used and disclosed, how the information may be accessed and corrected, and how an individual may make a complaint in relation to their personal information held by the NCSR.

Health's Response

Health accepts this recommendation.

Health is developing a privacy policy for the NCSR in consultation with Telstra Health which will explain how the NCSR will handle personal information for each of the Screening Programs. The privacy policy will outline the personal information that will be collected (either from the individual themselves, or from other sources), the legal authority for the collection, use and disclosure for the purpose of the NCSR, who else the information may be disclosed to, the participant's rights to opt out of the NCSR and how they may make a privacy complaint.

The NCSR privacy policy will be included in the Department's website, the NCSR portal and relevant program publications. The privacy policy will also include information about how individuals' Medicare information will be handled by the NCSR (refer to **Recommendation 18**) and how consumers can choose not to participate in the NCSR (refer to **Recommendations 25 and 27**).

In line with current Health policy, consumers will be able to communicate any concerns and complaints through the Department's website, in writing through the NCSR portal, or by phone to the Contact Centre.

Recommendation 18 The Privacy Policy and Privacy Notices should contain concise information about how and from whom the NCSR collects information. It should also detail disclosure, including that screening information is published to the individual's My Health record.

Health's Response

Health accepts this recommendation and is taking steps to include information about how the NCSR will handle individuals' Medicare information in its privacy policy and/or privacy notices. Health will also publish information about the use of Medicare claims data in Program Information and on the Programs' website, including the specific items being collected.

The privacy policy will refer to the NCSR Act which authorises Medicare claims information, which may indicate whether or not the individual has undergone or should undergo screening associated with a designated cancer (that is, bowel cancer and cervical cancer), to be collected and stored in the NCSR. As authorised by the NCSR Act, this information will be used to identify individuals who are to be sent an invitation or reminder to screen for

a designated cancer. Medicare claims information may also be used in deciding whether an individual should not be invited to undergo screening under the NCSP or NBCSP.

Updates to individuals' personal information recorded in Medicare, in particular, address details, will be collected regularly by the NCSR. In addition, where an MBS claim is used to alter a participant's status in the Screening Program, this will be communicated to the participant directly through Program correspondence.

Recommendations 27 The NCSR privacy policy should clearly and prominently set out a participant's opt out rights and how to exercise them.

Health's Response

Health accepts this recommendation.

As part of addressing privacy concerns associated with the collection, recording of, use and disclosure of individuals' information, the NCSP and the NBCSP websites and the NCSR portal will clearly communicate the participant's right to opt out of or defer participation in the NCSR and provide options on how to do so.

In line with the response to Recommendation 25,should individuals not wish to participate in the NCSR, they will be able to call the Contact Centre, visit the NCSR's participant portal, or provide verbal consent to their healthcare provider to complete the opt out form on their behalf during a consultation.

PRIVACY GOVERNANCE AND MANAGEMENT

Recommendation 2 Health should also have a privacy governance strategy to ensure there is oversight of the project from a privacy perspective and a forum in which these strategies can be discussed.

Health's Response

Health accepts this recommendation.

Privacy governance is a component of the NCSR's governance within Health and a strategy will be implemented in collaboration with States and Territories though a Memorandum of Understanding (MoU) with participating States and Territories.

Recommendation 13 As part of the privacy governance framework recommended in Recommendation 2, Health should develop and implement a complaints management framework for any privacy-related complaints received by the Health or Telstra Health in relation to the NCSR. This should include a process for dealing with complaints made in relation to how a State or Territory has handled NCSR information which has been reported to it from the NCSR.

Health's Response

Health accepts this recommendation.

A comprehensive complaints policy and protocols will be developed to manage and respond to complaints. MoUs will be developed and entered into with the States and Territories regarding their access, handling and use of NCSR information, including any action/remediation arising from complaints made about states' handling of NCSR data.

Recommendation 14 Health should review the operation of the NCSR from a privacy perspective periodically (that is, after two or three years of operation) or in accordance with any review of Telstra Health's performance of its obligations under the service agreement as specified in the service agreement (if any).

Health's Response

Health accepts this recommendation and will review the operation of the NCSR two years after its commencement.

This review may be undertaken as a review of the operation of the NCSR from a privacy perspective, or as part of a review of Telstra Health's delivery of its obligations under the Services Agreement (as required), in particular, compliance with requirements relating to privacy, security and confidential information. This review will also examine the implementation of the mandatory reporting of data breaches required by the NCSR Act.

It should be noted that, in addition to the review of the operation of the NCSR, the Australian Government has statutory functions in place to authorise the examination of the operation of the NCSR. For example, the Auditor-General, the Australian National Audit Office and the Information Commissioner, or their delegates, may inspect information in the NCSR held on Telstra Health's premises. From a privacy perspective, the Information Commissioner has a range of powers relating to interferences with privacy, including the power to conduct assessments, investigate potential breaches of privacy, accept enforceable undertaking by agencies and organisations and make a determination which is enforceable in the Federal Court. [1]

COMMUNICATION WITH INDIVIDUALS

Recommendation 3 The NCSR, Health, DHS and the relevant State and Territory Health Departments should communicate to individuals that the NCSR will involve a number of systemised collections of their personal information for the effective administration of the NCSR. These communications should be accessible online and other appropriate media and should be covered in relevant privacy policies.

Health's Response

Health accepts this recommendation and acknowledges that effective communication assists individuals to make informed choices about their privacy.

This recommendation will be addressed as per the response to Recommendation 1 in relation to the NCSR's privacy policies.

Key messages regarding the collection of personal information by the NCSR will be shared with States and Territories and DHS and will be made available prior to the commencement of the NCSR. In line with the response to Recommendation 18, the key messages will include information about how the NCSR will handle individuals' Medicare information.

Communication materials will:

- be developed in consideration of differences in health literacy, appropriate information for Aboriginal and Torres Strait Islander people, and people with culturally and linguistically diverse backgrounds;

[1] Office of the Australian Information Commissioner, *Senate Community Affairs Legislation Committee Inquiry into the National Cancer Screening Register Bill 2016*, p.2

- clearly describe the rationale and purpose for the collection of individual's personal information and will be developed for a range of End Users of the NCSR, including individuals, healthcare providers, government and the contracted service provider; and
- include online, print and other media taking into account the preferred modes of communication of target audiences.

Recommendation 4 The information booklet accompanying the screening invitation letter for the NBCSP should notify individuals of certain matters, including when the NCSR is likely to collect their information, their opt out rights and provide the link to the NCSR's online privacy policy.

Health's Response

Health accepts this recommendation.

The NBCSP Information Booklet and the cervical invitation letters will include information about collection of personal information and individuals' right to opt out of the NCSR.

In line with the response to Recommendations 1, 3 and 27, information about the collection of personal information and individuals' choice to opt out will be addressed in the NCSR's online privacy policy.

In line with the response to Recommendation 18, the Information Booklet will set out how the NCSR will handle individuals' Medicare information.

Recommendation 24 It should be made possible for individuals to self-select preferred methods of correspondence for information from the NCSR and that this is effectively communicated to individuals.

Health's Response

Health accepts this recommendation.

NBCSP pre-invitation correspondence will encourage individuals to go to the NCSR portal to set their communication preferences for different communication types.

The NCSP will implement a welcome letter for Program invitees which will provide options for setting communication preferences.

Recommendation 25 Screening letters sent to individuals should clearly communicate a participant's opt out and deferral rights and how they can elect to opt out of the screening pathway. With respect to the NCSP, this will allow women to choose to opt out of the NCSR so they do not receive invitations, opt- out of receiving certain information or correspondence, indicate that they need to defer their screening for a defined period, request that their information is not disclosed for certain purposes or request that their information is kept anonymous.

Health's Response

Health accepts this recommendation.

The NBCP and NCSP web sites and NCSR portal will provide information on individuals' right to opt out from participation in the NCSR and to defer screening.

In line with the response to Recommendation 27, the information will include options on how to exercise the right to opt out of or defer participation in the NCSR, for example, by calling the Program's Contact Centre.

In line with the response to Recommendation 4, the NCSP welcome letter and NBCSP pre-invitation letters and Information Booklet will provide information on deferral and opt out.

Communication materials will be accessible, written in plain English and take into account consumers with special needs, individuals from a non-English speaking background and disadvantaged and vulnerable individuals. [2]

Recommendation 29 Correspondence sent to individuals to notify or remind them of screening should be of the type(s) self-selected by the participant in line with Recommendation 24. Health should consider making a copy of the correspondence available to the participant upon logging into the NCSR portal.

Health's Response

Health accepts this recommendation.

The NCSR will retain copies of all correspondence provided to individuals (including healthcare providers). The NCSR's design will allow for copies of any correspondence to be made available as part of the User's access to the NCSR.

In line with the response to Recommendation 24, individuals can go to the NCSR portal to change their communication preferences for different communication types and the NCSR design will enable the change in preference to be recorded.

PRIVACY NOTICE

Recommendation 5 A layered privacy notice is developed for the web portal. A layered privacy notice involves initially notifying an individual of the basic privacy issues affecting them, with the option to access more detailed information (for example, through the use of a drop-down box, information boxes which appear when the mouse cursor hovers over particular information or a link to a more detailed description.

Health's Response

Health accepts this recommendation in recognition that a layered privacy notice will assist in communicating how the NCSR will handle individuals' personal information. The first layer will provide a clear summary of key privacy points while the second layer will provide the full privacy policy with detailed information that can be drilled down to further pages addressing use and disclosure, right of individuals to opt out, how to make a complaint, etc.

In line with the responses to Recommendations 3 and 27, the layered privacy notice will clearly set out the rationale and purpose for the collection of individuals' personal information, the participant's right to opt out of or defer participation in the NCSR and options on how to do so.

[2] Office of the Australian Information Commissioner, *Senate Community Affairs Legislation Committee Inquiry into the National Cancer Screening Register Bill 2016*, p.4

TRAINING AND POLICY COMMUNICATION

Recommendation 7 People/entities who have access to the NCSR should undergo privacy training (including familiarisation with key sections of the OAIC's *Guide to securing personal information*) so that they are aware of the obligations imposed by relevant privacy laws, including the need to take reasonable steps to protect personal information from unauthorised access, modification or disclosure.

Health's Response

Health accepts this recommendation.

Information on the privacy laws will be made available to all End Users with access to the NCSR through online training with a check box acknowledgement that the End User is aware of the obligations imposed by relevant privacy laws. This includes the contracted service provider, Health staff, States and Territories and healthcare providers.

The training will focus on the Australian Privacy Principles (APPs) which impose obligations when collecting, storing, using and disclosing personal information for the purpose of the NCSR.

Recommendation 10: Telstra Health should ensure that its security policies and procedures are communicated effectively to their support staff.

Health's Response

Health accepts this recommendation.

Telstra Health's Services Agreement requires its personnel to comply with all relevant security procedures and requirements. It should be noted that all Telstra Health personnel who are involved in managing or operating the NCSR are bound by strict confidentiality undertakings. In addition, Telstra Health personnel who have access to or are likely to have access to NCSR data must possess appropriate security clearances. [3]

Recommendation 26 Healthcare providers should receive basic training relating to the advantages and disadvantages of opting out of the NCSR so they can communicate these to their patients to make informed decisions about whether they wish to opt out.

Health's Response

Health accepts this recommendation

Health will develop a fact sheet for health providers for the NBCSP and NCSP. These will be available on the website and communicate key messages in accordance with the NCSR's and each Program's communication strategies.

Consideration will also be given to including a section on opting out of the NCSR in the training materials currently being developed for the renewed NCSP.

[3] Telstra, *Telstra submission to the inquiry of the Senate Standing Committee on Community Affairs into the National Cancer Screening Register Bill 2016*, p.6

DATA ACCESS AND RELEASE POLICY

Recommendation 22 A data access and release policy should be prepared which covers the disclosure of information from the NCSR for research, including whether the information should be de-identified. Where applicable, the disclosure of information will need to be in accordance with any relevant guidelines, including procedures akin to those made under sections 95 or 95A of the Privacy Act.

Health's Response

Health accepts this recommendation.

The NCSR provides a valuable resource for research into cancer screening. Access to data for approved research purposes is important for the evaluation, monitoring and improvement of the Screening Programs. Access, release and use of information and data held in the NCSR must comply with the NCSR Act as well as with privacy and freedom of information legislation.

Release of data for research purposes will be managed by Health according to the Data Access and Release Policy, which will require compliance with guidelines made under sections 95 and 95A of the *Privacy Act 1988* (as applicable).

Recommendation 23 Further to Recommendation 22, the data access and release policy should address the following matters:

- the permitted uses and secondary disclosures of NCSR information provided to the States and Territories;
- the rules and procedures for when a State, Territory or other third party will receive identified or de-identified information. In particular, identified information should only be disclosed in circumstances where the receiving party requires identified information;
- where identified information is disclosed, it should be appropriately encrypted during transmission to the receiving party and while at rest with the receiving party; and
- where de-identified information is disclosed, it should not be reasonably possible for the information to be re-identified.

Health's Response

Health accepts this recommendation.

In line with the response to Recommendation 22, third parties will only be provided access to de-identified data where approved by Health and in accordance with meeting the requirements and compliance with Health's NCSR Data Access and Release Policy.

Provisions for State and Territory access and use of NCSR data will be in accordance with the negotiated MoU with the States and Territories, which will address access, use and disclosure of NCSR data, physical and personnel security and secondary disclosure.

It should be noted that at the time of writing, a Bill to amend the *Privacy Act 1988* (Privacy Amendment (Re-identification Offence) Bill 2016) was introduced to further protect de-identified data from being re-identified to make it a new criminal offence to re-identify de-identified government data. The amendment 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 data set. The new offences would apply to actions taken on or after 29 September 2016.

NCSR SYSTEM SECURITY AND ACCESS CONTROLS

Recommendation 8 People/entities who have access to the NCSR agree to terms and conditions containing rights and obligations regarding their access to the NCSR. Those terms and conditions should note the potential criminal offences for unauthorised access or disclosure of information on the NCSR (where applicable under the NCSR Act). People/entities with administrative access to the NCSR or access to a large amount of data are held to a higher level of scrutiny and obligations, for example through minimum security vetting.

Health's Response

Health accepts this recommendation.

The NCSR will include features that require healthcare providers and other End Users to accept Terms and Conditions before being given access to the NCSR, which includes that their activities will be audited.

In line with the response to Recommendation 10, Telstra Health staff must possess appropriate security clearances in order to access NCSR data. Telstra Health personnel with administrative access to the NCSR or who have access to aggregated data will be required to obtain Negative Vetting 1 clearance prior to access and use of the NCSR.

Recommendation 9 An audit trail function should be included in the NCSR's design so that issues regarding potential unauthorised access or disclosure are able to be identified and investigated. To the extent possible, this functionality should allow NCSR to proactively search for inappropriate access and detect potential instances of healthcare providers browsing the NCSR for purposes unrelated to the healthcare of their patients.

Health's Response

Health accepts this recommendation.

An audit trail is a requirement of the NCSR design, as well as logging of read access. The NCSR will also support 'pop up' messaging to alert users when the system detects access and use consistent with 'browsing' by healthcare providers.

Audit trail functionality is particularly important in ensuring that the requirement in the NCSR Act relating to mandatory notification of data breaches is met, including the requirement for the Secretary of the Department of Health and Telstra Health as the contracted service provider to take certain actions in relation to data breaches.

The data breach reporting obligations require Telstra Health to notify a breach to the Secretary of the Department, in addition to the Information Commissioner, as soon as practicable after becoming aware that there has been, or may have been, a data breach. An audit trail showing the back-end view of system use and transactions will be critical for detecting unauthorised access to individuals' information held in the NCSR and provide evidence during investigations of suspected and known security incidents and breaches to individuals' privacy.

Recommendation 20 Health should review the security and access arrangements to ensure that all reasonable risks of unauthorised access are mitigated.

Health's Response

Health accepts this recommendation and will work with Telstra Health to implement this review.

As part its security and access arrangements, the NCSR will be implemented and operated according to strict IT security requirements, including government Information Security Manual and Protective Security Policy Framework compliance. The NCSR's security arrangements will follow the same three layered accreditation process that is used for all Australian Government solutions, including the My Health Record system. The process includes an audit of the solution architect and controls, and certification that the controls have been implemented and are operating effectively, by an independent Australian Government certified auditor through the Australian Signals Directorate assessment program. This accreditation and assessment process will provide independent assurance that appropriate and effective security controls have been implemented and are operating to effectively process, store and transmit sensitive health information. [4]

Individuals and healthcare providers will be issued user accounts, requiring authentication with strict controls based on their role. In line with the response to Recommendation 9, users' access to the data in the NCSR will be audited.

Recommendation 21 The NCSR has role-based access controls (which are set by the system, not individuals) which limit the access of people/entities to information in a participant's record that is necessary to provide services to the participant or to serve a justified usage.

Health's Response

Health accepts this recommendation.

Role-based access controls are included in the NCSR design to ensure that the recording of, use or disclosure of protected information or key information in the NCSR is limited to those circumstances set out in the NCSR Act.

In line with the response to Recommendation 20, individuals and healthcare providers will be issued user accounts, requiring authentication with strict controls based on their role. In line with the response to Recommendation 9, users' access to the data in the NCSR will be audited.

INDIVIDUALS AMENDING OR UPDATING THEIR INFORMATION IN THE NCSR

Recommendation 11: Health should consider implementing a process similar to that in the My Health Record system for dealing with requests to correct clinical information held in the NCSR. Rather than contacting the NCSR directly, this involves an individual contacting the healthcare provider who authored the document containing their clinical information, who in turn can notify the NCSR whether or not the information should be corrected (providing reasons) which then allows the NCSR to deal with the request and notify the participant of the outcome.

Health's Response

Health accepts this recommendation.

[4] Telstra, *Telstra submission to the inquiry of the Senate Standing Committee on Community Affairs into the National Cancer Screening Register Bill 2016*, p.5-6

Participants will not have direct access to their clinical information in the NCSR; however, if an individual believes their clinical details are incorrect in the NCSR, a system similar to that in the My Health Record system will be adopted to deal with requests to verify/correct clinical information.

Recommendation 12: Individuals (or healthcare providers on the participant's behalf) should be able to update the nominated healthcare provider in the NCSR. Correspondence to nominated healthcare providers should request that healthcare providers notify the NCSR if they should no longer be the nominated healthcare provider. Correspondence to individuals should set out information on the participant's current nominated healthcare provider and easy-to-read instructions on how that can be changed.

Health's Response

Health accepts this recommendation.

Letters to healthcare providers will be reviewed to ensure this is included. Invitees for the NBCSP will be provided with information on how to change their nominated healthcare provider on the Participant Details Form.

Women participating in the NCSP will be advised through the NCSP website on their ability to update the nominated healthcare provider through the NCSR participant portal. This information will also be published on the Program's website.

DATA MIGRATION AND CLEANSING STRATEGIES

Recommendation 15 Health or Telstra Health (as appropriate) should develop and test data migration and data cleansing strategies prior to undertaking migration. Robust strategies will assist in ensuring a high level of data compatibility between the registers and will decrease the risk of inaccurate matches and duplication of records.

Health's Response

Health accepts this recommendation.

This is a requirement in the Services Agreement with Telstra Health, including test runs, data quality analysis and remediation plans.

Recommendation 16 Responsibilities with respect to cleaning and migrating data and the risks associated with it are clearly defined so privacy risks can be managed. This will help with issues around information moving between jurisdictions.

Health's Response

Health accepts this recommendation.

The data migration strategy includes protocols for acceptance of data quality prior to merging records, that is, to ensure that records that cannot be adequately identified in order to be merged will remain separate.

To support data migration, Telstra Health will be responsible for providing a secure migration environment, connectivity and secure file exchange and development and oversight of the Transformation and Mapping Plan. As part of the process, Telstra Health will identify and review records for cleansing and automatic system cleansing and perform System Integration Testing.

To support data migration, state and territories will provide a data dictionary, database schema, table properties, an initial data extract and raw data extracts. They will undertake manual data cleansing, including review and correction, contribute to the review of records for system cleansing and participate in User Acceptance Testing.

Recommendation 17 Health and the States/Territories should work together to identify what specific risk mitigation strategies, if any, are necessary for each State/Territory in order to facilitate migration of data.

Health's Response

Health accepts this recommendation.

This has already occurred through the Standing Committee on Screening and is continuing as part of bilateral discussions and planning between Telstra Health and States and Territories.

RULES MADE UNDER THE NCSR ACT

Recommendation 6 The rules prescribed by the Minister for the purposes of clause 13 of the NCSR Act should address privacy issues concerning the collection of information of individuals who are not participating in the NCSR, including where individuals have opted out of participation. At minimum, the rules should provide that any information received by the NCSR in relation to non-participants (including individuals who have opted out) should be made inaccessible to any person accessing the NCSR in accordance with appropriate security procedures.

Health's Response

Health accepts this recommendation

The Rules will provide that the NCSR will not collect clinical information from any individual who is not participating in the NCSR, but will retain basic demographic details for individuals who have opted out of the NCSR in order to prevent them being re-invited to participate.

In addition, the NCSR's design will allow for basic demographic details to be used to determine if information relating to a non-participating individual is being uploaded to the NCSR by a healthcare provider in compliance with section 13 of the NCSR Act. This functionality in the NCSR will prevent the information from being collected by the NCSR.

From an operational perspective and in line with the response to Recommendation 8, Telstra Health personnel with administrative access to the NCSR will be required to obtain Negative Vetting 1 clearance prior to accessing and using the basic demographic information of individuals who have opted out of the NCSR.

Options are currently being explored for participants to request that a pseudonym be used in connection with their record in the NCSR to ensure the individual's privacy.

MY HEALTH RECORD ACCESS

Recommendation 19 The NCSR should be a participant in the My Health Record system and have the necessary legislative permissions to make changes to a participant's My Health Record.

Health's Response

Health accepts this recommendation

Telstra Health will be a registered repository operator for the purpose of publishing to the My Health Record system. This will ensure that the screening status of individuals in the NCSR can be disclosed to the My Health Record.

INDIGENOUS CONSULTANT

Recommendation 28 Health should consider appointing an indigenous consultant (or other person with relevant expertise) to ensure that the purposes for which the NCSR collects and uses ATSI / CALD status information are communicated with appropriate sensitivity.

Health's Response

Health accepts this recommendation.

Health will seek independent advice on handling communication regarding the collection and use of Indigenous status / Cultural background information to ensure it is appropriately and sensitively communicated.

3. About this PIA

3.1 What is a privacy impact assessment?

A PIA is an examination of a project from a privacy perspective. The primary purposes of a PIA are to:

(a) examine how personal information is collected, used and disclosed as part of a project;

(b) analyse the impacts of the project on personal privacy; and

(c) identify and recommend options for managing, reducing or removing those impacts.

PIAs are conducted to ensure that privacy issues are fully considered in the design and implementation phase of a project. PIAs help ensure that projects meet privacy requirements in legislation and are also consistent with broader community privacy expectations.

3.2 The approach of this PIA

This PIA has been prepared broadly in accordance with the *Guide to undertaking privacy impact assessments* (Office of the Australian Information Commissioner, May 2014) (the **PIA Guide**). That guide recommends that PIAs be conducted in ten steps. Some of those steps involve deciding whether or not a PIA is necessary (a threshold assessment) and planning. This PIA was conducted in five key stages, as shown diagrammatically below at Figure 1.

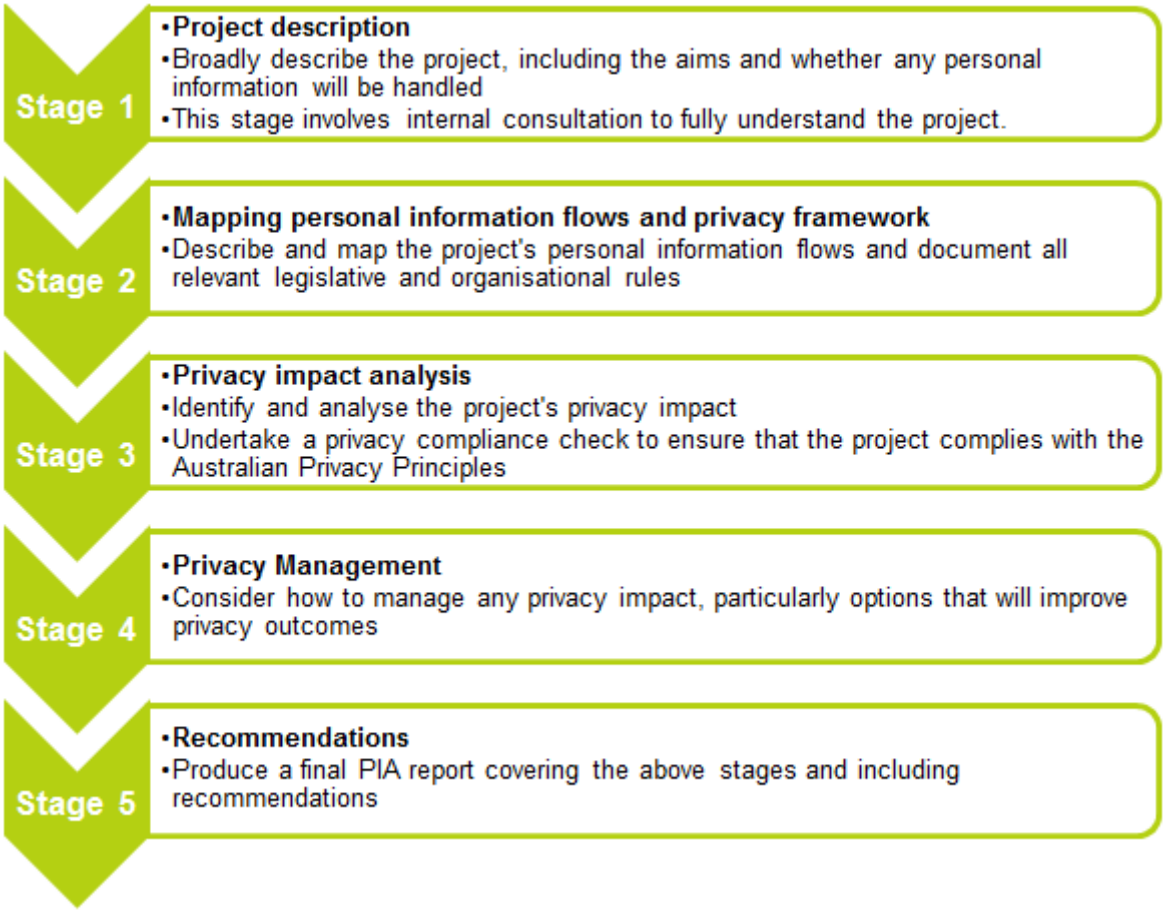


Figure 1 — PIA stages

Schedule 1 contains a glossary and Schedule 2 contains relevant definitions.

This PIA has also been prepared in light of the *APP Guidelines* (Office of the Australian Information Commissioner, April 2015) (the **APP Guidelines**).

3.3 Applicable legislation

The NCSR will operate in accordance with the NCSR Acts which provide a legal basis for the NCSR to collect, use and disclose a wide range of information for the purposes of the NCSR.

This PIA analyses the privacy risks of collecting, using and disclosing information for the purposes of the NCSR against the provisions of the *Privacy Act 1988* (Cth) (the **Privacy Act**) with particular focus on the Australian Privacy Principles (**APPs**) set out in Schedule 1 to the Privacy Act.

Where appropriate, this PIA also analyses the collection, use and disclosure of healthcare identifiers by various entities under the *Healthcare Identifiers Act 2010* (Cth) (the **HI Act**) and also considers linkages between the NCSR and an individual's My Health Record in accordance with the *My Health Records Act 2012* (Cth) (the **My Health Records Act**).

3.4 Scope, limitations and assumptions

In November 2015, an initial PIA was prepared by Clayton Utz to address privacy risks and management strategies relating to the NCSR (**initial PIA**). In the time since the initial PIA was prepared, the design of NCSR has undergone a number of developments. Amongst other developments, a contracted service provider, Telstra Health, has been appointed as the operator of the NCSR, consultations with the States and Territories have progressed and amendments have been made to the NCSR Acts.

This PIA builds upon, but stands alone from, the initial PIA. Where appropriate, this PIA considers the same privacy issues addressed in the initial PIA and makes similar recommendations, but also considers a number of further issues which have arisen since the initial PIA was prepared. These issues include:

- the NCSR Act has been drafted to authorise various collections, uses and disclosures of information for the purposes of the NCSR;
- the appointment of a contracted service provider, Telstra Health, to operate the NCSR; and
- further development of the NCSR system design and the information flows to and from the NCSR.

In light of this background, this PIA has been prepared on the basis that:

- the NCSR Bills and draft business process documents provided to Clayton Utz on 1 August 2016 accurately describe the proposed purposes and collections, uses and disclosures of information by the NCSR and other entities;
- the NCSR Bills passed both Houses of Parliament on 13 October 2016 and received Royal Assent on 20 October 2016 prior to establishment of the NCSR and provides legislative authority for the collection, use and disclosure of personal information in connection with the NCSR's purposes;
- Health, which is an agency for the purposes of the Privacy Act and ultimately has control over and responsibility for NCSR data;
- following a competitive tender process, Telstra Health will be the contracted service provider for the NCSR in accordance with a service agreement between Health and Telstra Health.
- for the purposes of the Privacy Act, any collection, use or disclosure by the NCSR or Telstra Health will be taken to be a collection, use or disclosure by Health;

- as required by section 95B of the Privacy Act, Health will take contractual measures to ensure that Telstra Health does not do an act, or engage in a practice, that would breach an APP if the act or practice had been undertaken by Health; and
- neither Health nor Telstra Health will transfer or store any information collected in connection with the NCSR overseas.

4. Description of the NCSR

The introduction of a renewed clinical pathway for the National Cervical Screening Program (**NCSP**) and the phased implementation of biennial screening under the National Bowel Cancer Screening Program (**NBCSP**) provide the opportunity to introduce a single national screening register (the **NCSR**) that will support both these programs. The NCSP is a joint program, supported by the Commonwealth and State and Territory governments. The NBCSP is a program run by the Commonwealth, with States and Territories as program partners. It is possible that the NCSR will be further developed to support future cancer screening programs at the discretion of the Government.

The implementation of a single register to support the screening pathways for cervical and bowel cancers will assist to achieve a cost efficient, nationally consistent, robust, data assured and clinically effective implementation of the upcoming changes to cervical and bowel screening within Australia.

The NCSR will integrate with the My Health Record system, Health's Electronic Data Warehouse (**EDW**) and other clinical information systems. This will offer improved invitations, recall and follow up of eligible Australians and reduce costs and regulatory burden through improved software integration with general practice, specialists and pathology laboratories. The NCSR is intended to improve the quality and accessibility of data as well as the rate of data capture and data matching.

Currently, the NCSP is supported by eight cervical screening registers hosted by States and Territories and the NBCSP Register is hosted by the Department of Human Services (**DHS**). It is intended that data from participating State and Territory cervical screening registers and data in the NBCSP Register will be migrated to the NCSR. There will also be ongoing data flows to the NCSR, for example from the National HPV Vaccination Program Register (**NHVPR**) which will become part of the Australian Immunisation Register from 1 January 2017, and ongoing disclosure of information from public and private healthcare providers, as well as ongoing reporting to participating States and Territories.

Once the NCSR is implemented, eligible Australians who have opted in to the My Health Record system will have electronic access through the My Health Record system to their screening records wherever they are located in Australia.

Participants may access their screening records via the My Health Record system or the NCSR Participant Portal. Clinical information will be available through the My Health Record system if a healthcare provider uploads clinical information to that system. The NCSR will not provide clinical information to the My Health Record system directly.

5. Information Flows

5.1 Introduction

The establishment and operation of the NCSR involves a number of information flows between various entities, including:

- Health (including EDW);
- Australian Digital Health Agency (as the system operator for the My Health Record system);
- DHS (including Medicare records systems);
- States and Territories (including relevant agencies and organisations handling cervical screening data);
- Australian Institute of Health and Welfare (**AIHW**);
- National Human Papillomavirus Vaccination Program Register (**NHPVR**);
- National Fact of Death Register;
- Healthcare Identifiers Service (**HI Service**);
- National Health Services Directory (**NHSD**);
- Provider Directory Service (**PDS**);
- Participants and their personal representative(s) (within the meaning of the NCSR Act), if applicable;
- healthcare providers (individuals and organisations);
- pathology labs; and
- specialists.

This PIA addresses the information flows between these entities by categorising them as follows:

(a) a high level overview of the major information flows;

(b) data migration from the NBCSP and NCSP;

(c) directory services and authentication;

(d) bowel cancer screening pathway;

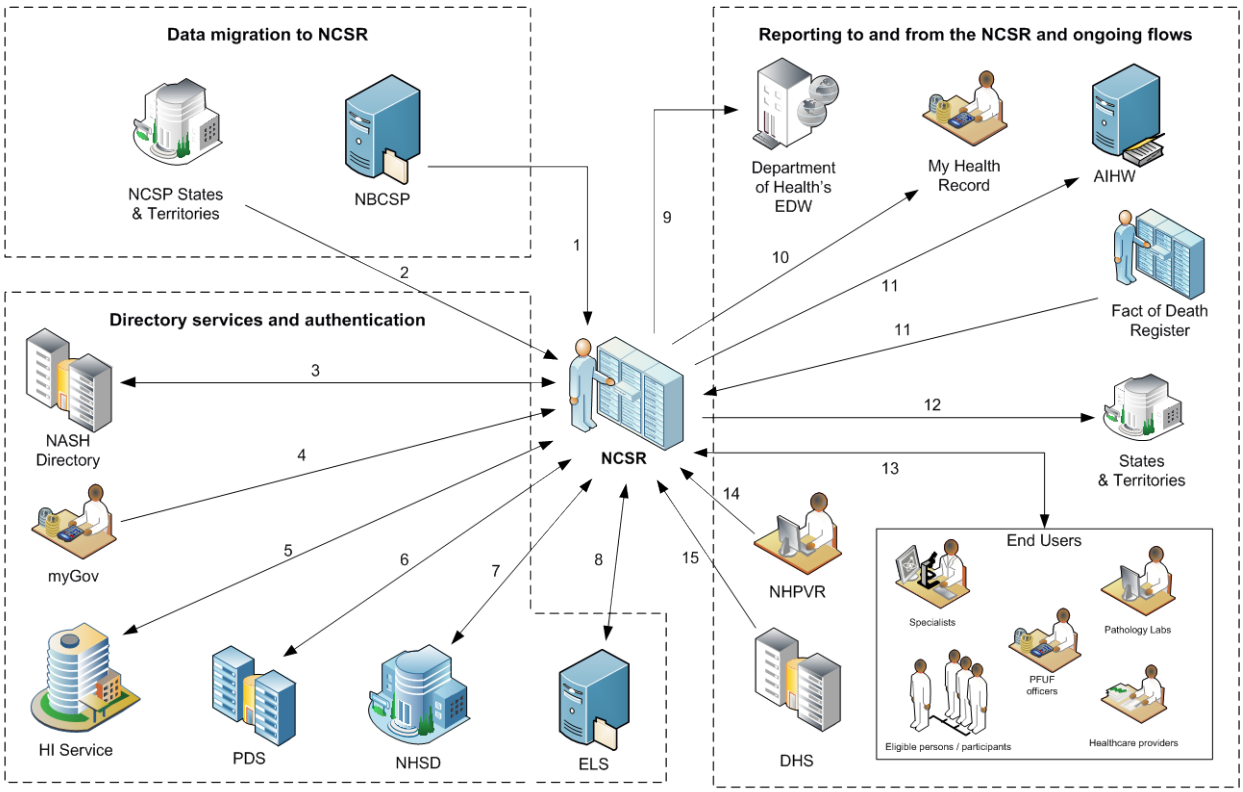
(e) cervical screening pathway; and

(f) reporting and ongoing access to the NCSR.

5.2 Overview

Figure 2 below sets out a high level overview of information flows between the main entities involved with the NCSR.

Figure 2 - Overview of information flows



Flow	Description
1	Migration of bowel cancer screening data to the NCSR.
2	Migration of cervical cancer screening data to the NCSR.
3	Authentication of National Authentication Service for Health (NASH) certificate details provided by healthcare providers only logging into the NCSR.
4	Individuals are able to use their myGov authentication to access the NCSR web portal.
5	Verification of participant details using the healthcare identifiers provided by the HI Service and information provided by DHS through Medicare information, GP systems and pathology laboratories to the NCSR.
6	Transfers of information and individual and organisation healthcare identifiers from Provider Directory Service used to verify individuals, healthcare providers and non-GPs.
7	Transfers of information from National Health Service Directory used to verify healthcare

Flow	Description
	providers and non-GPs.
8	The NCSR is able to look up healthcare provider information using the Endpoint Locator Service (ELS).
9	Disclosure of NCSR data to EDW for production of de-identified statistical and analytical reports.
10	Linkages between the NCSR and My Health Records system, including for updating participants' program status.
11	Collection and integration of aggregated, death information from the Fact of Death Register[5] and reporting of raw data to AIHW.
12	Disclosure of NCSR information (including healthcare identifiers and Medicare numbers) to States and Territories for reporting.
13	Information flows to, from and between various End Users as part of screening pathways and ongoing access to participants' screening information.
14	Transfers of participants' HPV completion status with a date from NHPVR to the NCSR.
15	Transfers of Medicare claims and enrolment data and healthcare provider details to the NCSR.

[5] The Fact of Death Register is coordinated and managed by Queensland in accordance with an agreement between the Commonwealth and States / Territories. It collates death information from the birth, deaths and marriages registers in each State and Territory.

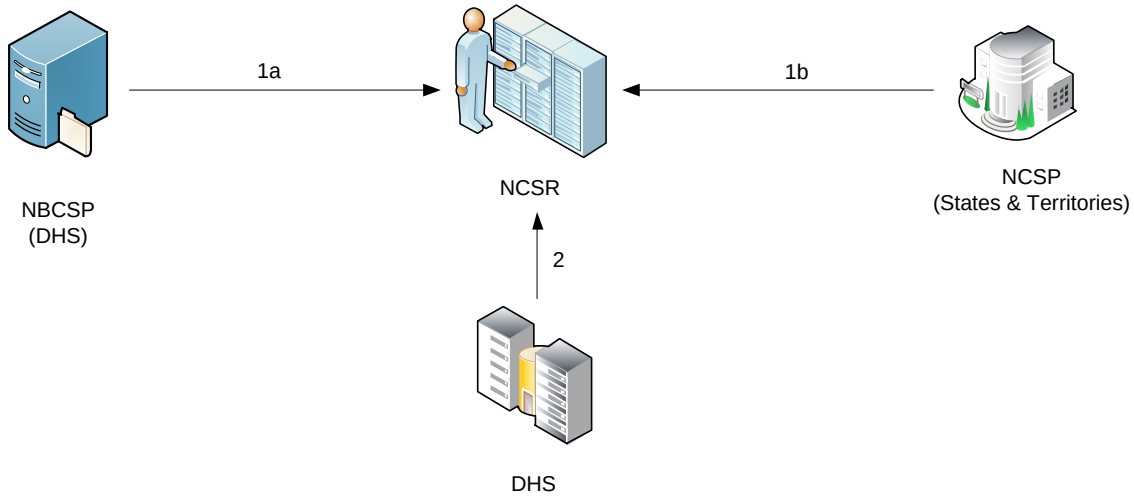
5.3 Data migration

Figure 3 below sets out the information flows associated with the initial migration of:

(a) bowel screening data from the NBCSP (administered by DHS); and

(b) cervical screening data from the NCSP (administered by State and Territory-based cervical screening registers).

Figure 3 - Data migration

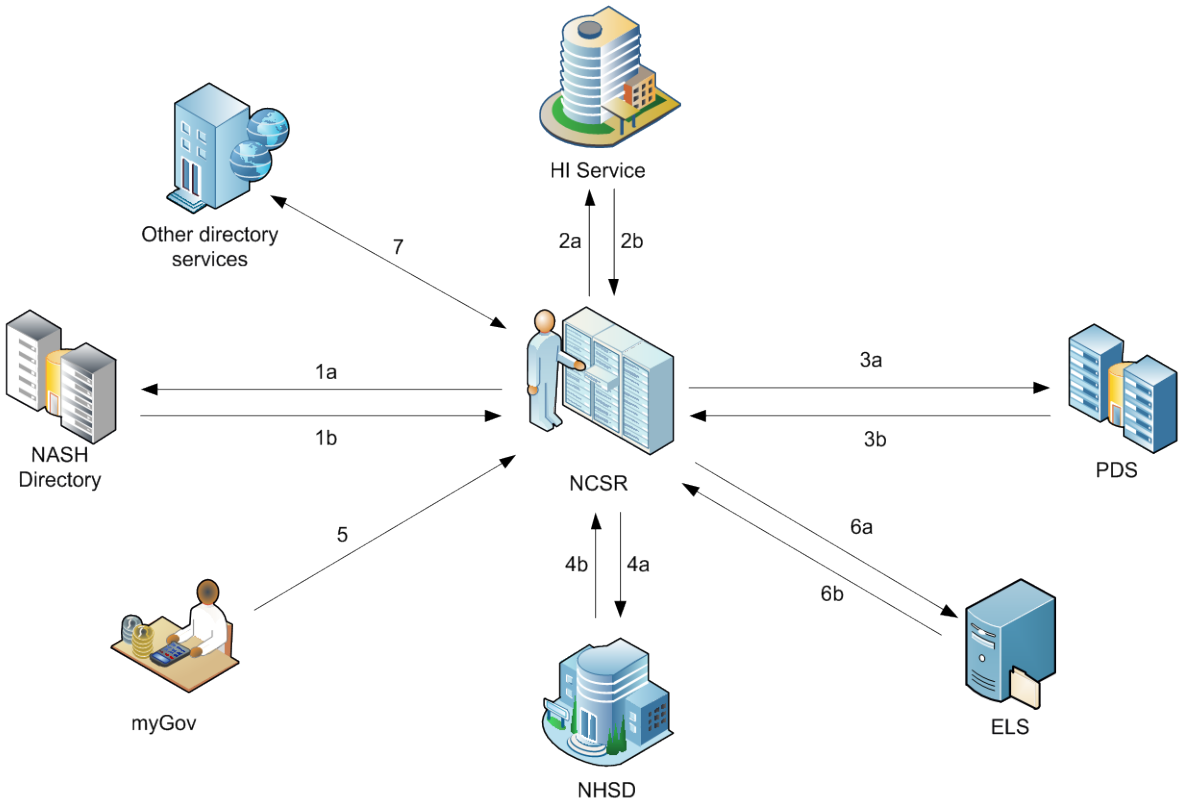


Flow	Description	Legislation	Comment
	Upon migration via an encrypted secure file transfer, NCSR will **collect** client data and Medicare numbers and "program data":		
1a	for bowel cancer screening, from DHS (as part of the NBCSP).	APP 3, 6	Disclosure by DHS and collection by the NCSR authorised by s 17(1) of the NCSR Act.
1b	for cervical screening, from the States and Territories (as part of the NCSP); and	APP 3, 6	Disclosure by States / Territories authorised by Schedule 1 cl 6 of the C&T Act and collection by the NCSR authorised by s 17(1) of the NCSR Act.
2	NCSR **collects** Department of Veterans' Affairs enrolment and Medicare enrolment data from DHS.	APP 3	Collection authorised by s 17(1) of the NCSR Act.

5.4 Directory services and authentication

Figure 4 below shows the information flows outlining the directory services and authentication processes. We understand that, pending policy and design, the HI Service verification process set out below may not be required.

Figure 4 - Directory services and authentication



Flow	Description	Legislation	Comment
1a	NCSR **collects** NASH key information from End Users logging into NCSR portal or software and **discloses** it to NASH directory for authentication.	-	No apparent personal information being transferred.
1b	NASH directory **discloses** and NCSR **collects** NASH key authentication result.	-	No apparent personal information being transferred.

Flow	Description	Legislation	Comment
2a	NCSR **discloses** HIs and personal information to the HI Service to verify the participant's details. This will be triggered whenever an HI is received from any source. Alternatively, for a participant who does not have an HI assigned to them, the NCSR can **disclose** that participant's personal information to the HI Service so that the HI Service can assign an HI.	APP 6 HI Act	Disclosure of personal information by the NCSR and collection by the HI Service authorised under s 17(3)(a) of the NCSR Act. In addition, as a registered repository operator, item 3 of the table to s 12 of the HI Act will apply.
2b	NCSR **collects** HIs and personal information from the HI Service after HI has been verified.	APP 3 HI Act	Collection of personal information and HIs by the NCSR authorised by s 17(1) of the NCSR Act.
3a	NCSR may **disclose** personal information to PDS to verify healthcare providers and non-GPs.	APP 6	Disclosure of any personal information by the NCSR authorised under s 17(3)(a) of the NCSR Act.
3b	NCSR may **collect** personal information and HI from PDS	APP 3 HI Act	Collection of personal information and HIs by the NCSR authorised by s 17(1) of the NCSR Act.
4a	NCSR may **disclose** personal information to NHSD to verify healthcare providers and non-GPs.	APP 6	Disclosure of any personal information by the NCSR authorised under s 17(3)(a) of the NCSR Act.
4b	NCSR may **collect** personal information and HI from NHSD	APP 3 HI Act	Collection of personal information and HIs by the NCSR authorised by s 17(1) of the NCSR Act.
5	An individual who authenticates themselves to the MyGov website by inputting their username, password and, if necessary, answers to secret question, is able to access the NCSR through the web portal, which may involve NCSR **collecting** personal information.	APP 3	Collection of personal information by the NCSR authorised by s 17(1) of the NCSR Act.
6a	NCSR **discloses** healthcare identifier of healthcare provider to ELS to look up healthcare provider details	APP 6 HI Act	Disclosure of any personal information by the NCSR authorised under s 17(3)(a) of the NCSR Act and s 26(3)(b) of the HI Act.

Flow	Description	Legislation	Comment
6b	NCSR **collects** healthcare provider details (may involve personal information) and healthcare identifier from ELS.	APP 3	Collection of personal information and HIs by the NCSR authorised by s 17(1) of the NCSR Act.
7	The NCSR may use other directory services to look up and/or verify information. This may involve **collections** and **disclosures** of personal information.	APP 3, 6	Disclosure by a directory service and collection by the NCSR of any personal information authorised by s 17(1) of the NCSR Act. Disclosure by NCSR and collection by a directory service of any personal information authorised by s 17(3)(a) of the NCSR Act.

5.5 Bowel cancer screening pathway

The bowel cancer screening pathway involves five main steps:

(a) inviting eligible persons to screen;

(b) participating in the program;

(c) screening participants;

(d) assessing participants; and

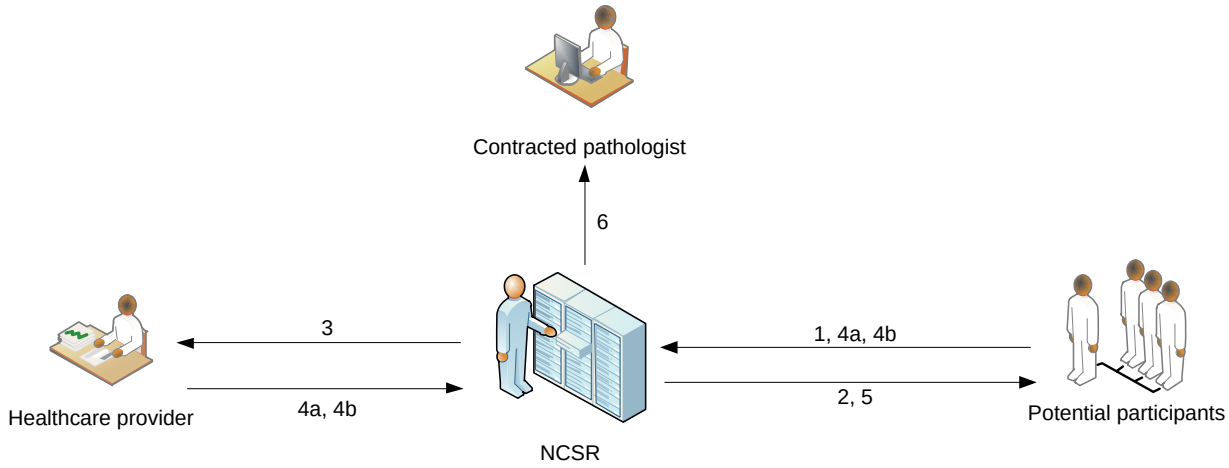
(e) diagnosing participants.

The sections below set out the particular information flows involved between various entities in each of these steps.

5. 5. 1 Activity 1 - Invite eligible person

Figure 5 below sets out the information flows between the NCSR, eligible persons and healthcare providers as part of the invitation to screen process.

Figure 5 - Invite participant



Flow	Description	Legislation	Comment
1	Eligible persons may self-initiate participation by notifying the NCSR. This would involve **collection** of personal information.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
2	NCSR sends "pre-invitation" to eligible persons and "exclusion correspondence" to individuals who are deselected (**disclosure**). The pre-invitation and exclusion correspondence contains personal information including the eligible person's name, address, postcode and, for pre-invitations, that are they are an "eligible Australian".	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(d) of the NCSR Act.
3	If the eligible person has nominated a healthcare provider, the NCSR notifies the eligible person's health care provider of the pre-invite where the healthcare provider has elected to receive correspondence (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(g) of the NCSR Act.
4a	The eligible person, their GP, or a health care worker who is a registered user of the NCSR, may opt out the participant from the	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.

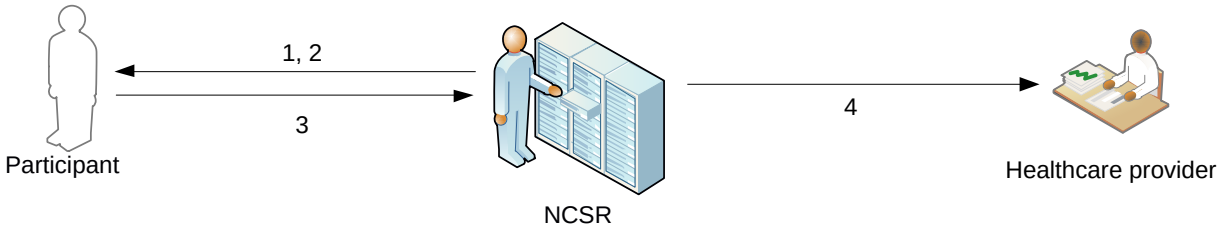
Flow	Description	Legislation	Comment
	screening program upon instruction by the participant. [6] This will involve NCSR **collecting** personal information.		
4b	The NCSR will ask for a reason why the person opted out and **collect** any reason given.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
5	NCSR sends a confirmation letter to the eligible person who has opted out, stating that the person will receive no further correspondence from the NCSR unless they opt back on (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and (12)(1)(i) of the NCSR Act.
6	NCSR notifies contracted pathologist that invitation has been sent (involves a **disclosure** of personal information).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and (12)(1)(j) of the NCSR Act.

[6] The opt-out process is provided for in s 14 of the NCSR Act.

5. 5. 2 Activity 2 - Participate in the program

Figure 6 below sets out the information flows between the NCSR, participants and healthcare providers as part of the initial participation in the program.

Figure 6 - Participate in the program

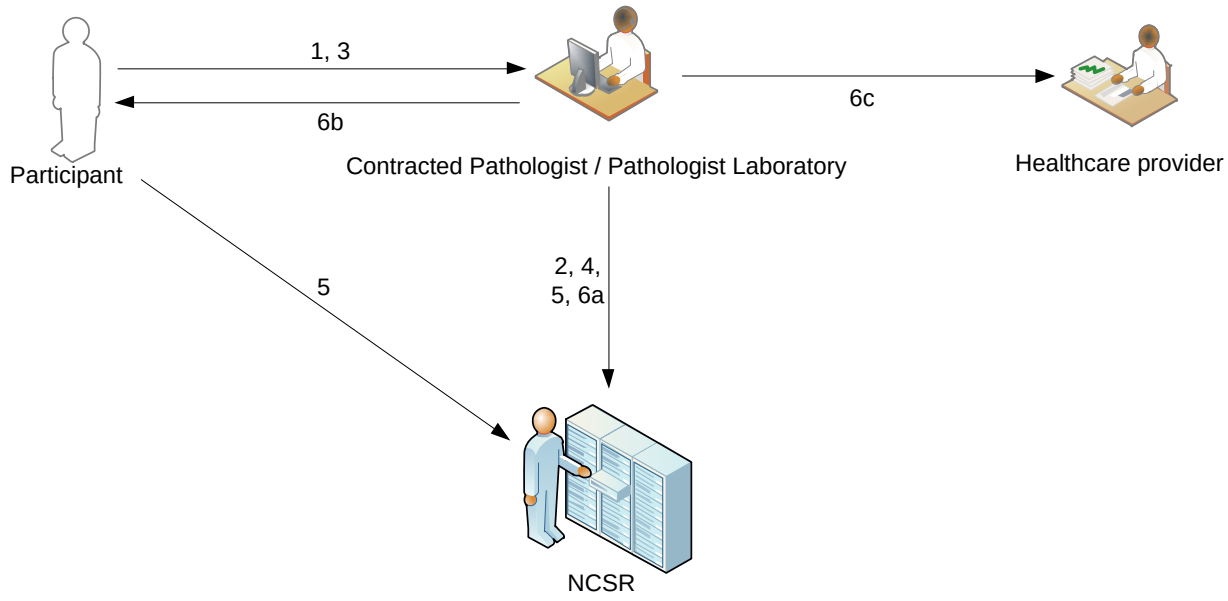


Flow	Description	Legislation	Comment
1	NCSR issues testing kit to participant (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(e) of the NCSR Act.
2	NCSR sends reminders to participant (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(f) of the NCSR Act.
3	Participant may defer screening. This would involve **collection** of personal information by NCSR.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
4	If a participant who defers has nominated a healthcare provider, the NCSR notifies that healthcare provider. This would involve the **disclosure** of personal information.	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(j) of the NCSR Act.

5. 5. 3 Activity 3 - Screen participant

Figure 7 below sets out the information flows in relation to participants, pathologists, healthcare providers and the NCSR as part of the screening process.

Figure 7 - Screen participant



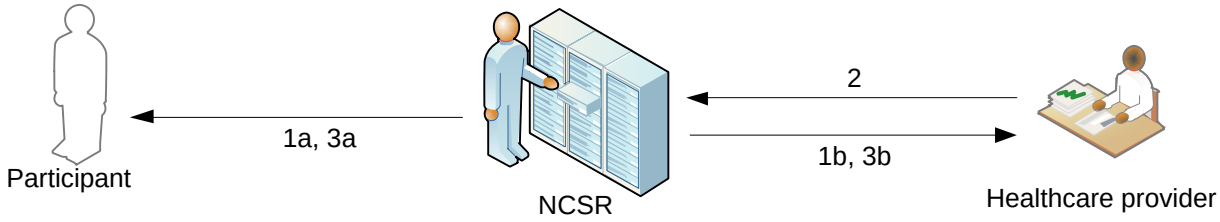
Flow	Description	Legislation	Comment
1	Participant completes test and sends it to the contracted pathologist.	-	-
2	Pathology Laboratory updates participant's details in the NCSR (**collection**).	APP 3	Collection authorised by s 17(1) of the NCSR Act.
3	Pathologist receives participation details form from participant.	-	-
4	Pathologist updates the NCSR with screening test details through an automated process involving batch processing and sending forms or, where necessary, can request the reissuing of a test kit. This involves the **collection** of personal information (namely, demographic details) by the NCSR.	APP 3	Collection authorised by s 17(1) of the NCSR Act.
5	Participant (using the online portal) or pathologist registers participation details in the NCSR. This involves the **collection** of	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.

Flow	Description	Legislation	Comment
	personal information by the NCSR.		
	Pathologist tests the screening kit and then:		.
6a	updates the NCSR with the screening test results (**collection** by NCSR);	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act
6b	sends the results to the participant; and		
6c	sends the results to the participant's nominated healthcare provider if any.		

5. 5. 4 Activity 4 - Assess patient

Figure 8 below sets out the information flows between participants, the NCSR and healthcare providers as part of assessing the participant.

Figure 8 - Assess patient

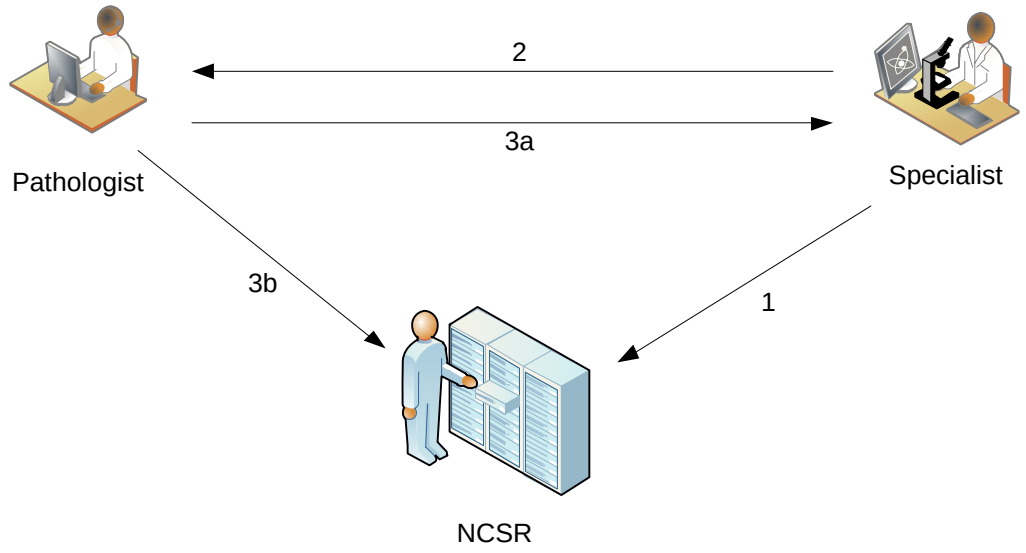


Flow	Description	Legislation	Comment
	NCSR **discloses** personal information by issuing reminders (including a positive reminder follow up, where appropriate) to the:	APP 6	Disclosure by NCSR authorised by ss 17(3)(a), 12(1)(f) and 12(1)(g) of the NCSR Act.
1a	participant; and		
1b	healthcare provider.		
2	After participant visits healthcare provider, healthcare provider makes recommendation and updates NCSR. This involves **collection** of personal information by the NCSR.	APP 3	Collection authorised by s 17(1) of the NCSR Act.
	NCSR **discloses** personal information by issuing reminders (including a no colonoscopy recorded follow up, where appropriate) to the:	APP 6	Disclosure by NCSR authorised by ss 17(3)(a), 12(1)(f) and 12(1)(g) of the NCSR Act.
3a	participant; and		
3b	healthcare provider.		

5. 5. 5 Activity 5 - Diagnose patient and outcomes

Figure 9 below sets out the information flows between the NCSR, pathologists and specialists as part of the diagnosis process.

Figure 9 - Diagnose patient and outcomes



Flow	Description	Legislation	Comment
1	After participant visits specialist, specialist conducts test and updates the NCSR. This will involve **collection** of personal and sensitive information by the NCSR.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
2	Specialist sends specimen to pathologist.	-	-
	After testing the specimen, the pathologist:		
3a	sends the results to the specialist; and	-	-
3b	sends the results to the NCSR and NCSR collects only those tests related to participants (**collection** of personal and sensitive information).	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.

5.6 Cervical cancer screening pathway

Similar to the bowel cancer screening pathway, the cervical cancer screening pathway involves five main steps:

(a) inviting eligible persons to screen;

(b) participating in the program;

(c) screening participants;

(d) assessing participants; and

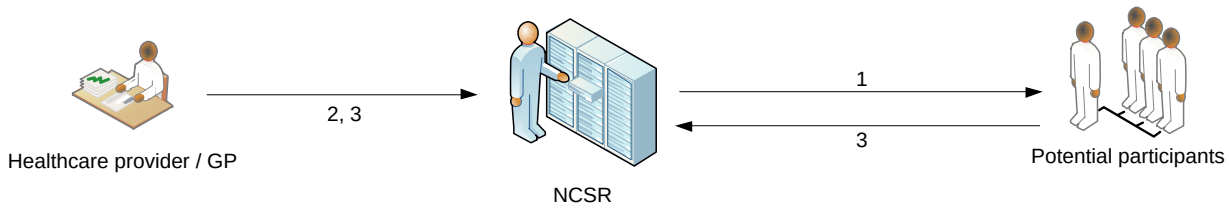
(e) diagnosing participants.

The sections below set out the particular information flows involved between various entities in each of these steps.

5. 6. 1 Activity 1 - Invite eligible person

Figure 10 below sets out the information flows between the NCSR, potential participants and healthcare providers as part of the invitation to screen process.

Figure 10 - Invite participant



Flow	Description	Legislation	Comment
1	NCSR can automatically invite individuals to participate in the cervical cancer screening pathway based on eligibility criteria (**disclosure**). [7]	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(d) of the NCSR Act.
2	An individual voluntarily going to a healthcare provider for an HPV test (who does not receive an invitation letter) may be opted in to the program by their healthcare provider (**collection**).	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
3	The invitee/participant, their GP, or a health care worker who is a registered user of the NCSR, may opt out the participant from the screening program. This will involve NCSR **collecting** personal information. Opting out may involve: • opting out of participation in the NCSR (in which case NCSR will continue to hold information already collected and disclose in accordance with its reporting obligations); • requesting that no information be sent to the person (in which case NCSR will continue to hold and collect information which may be viewed by the participant's healthcare provider; and/or • requesting to defer screening	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.

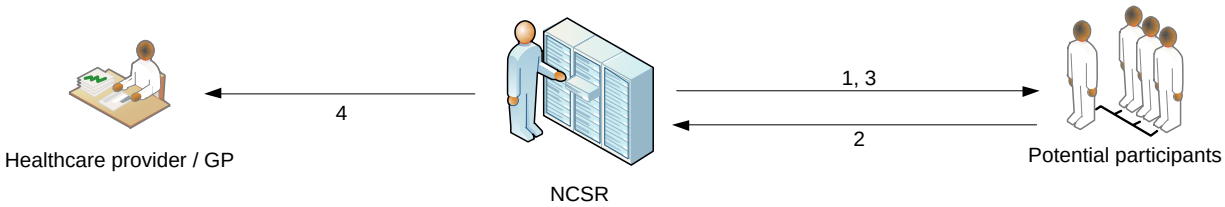
[7] Note that individuals can self-initiate

Flow	Description	Legislation	Comment
	(see Activity 2).		

5. 6. 2 Activity 2 - Participate in the program

Figure 11 below sets out the information flows between the NCSR, participants and healthcare providers as part of the initial participation in the program.

Figure 11 - Participate in the program

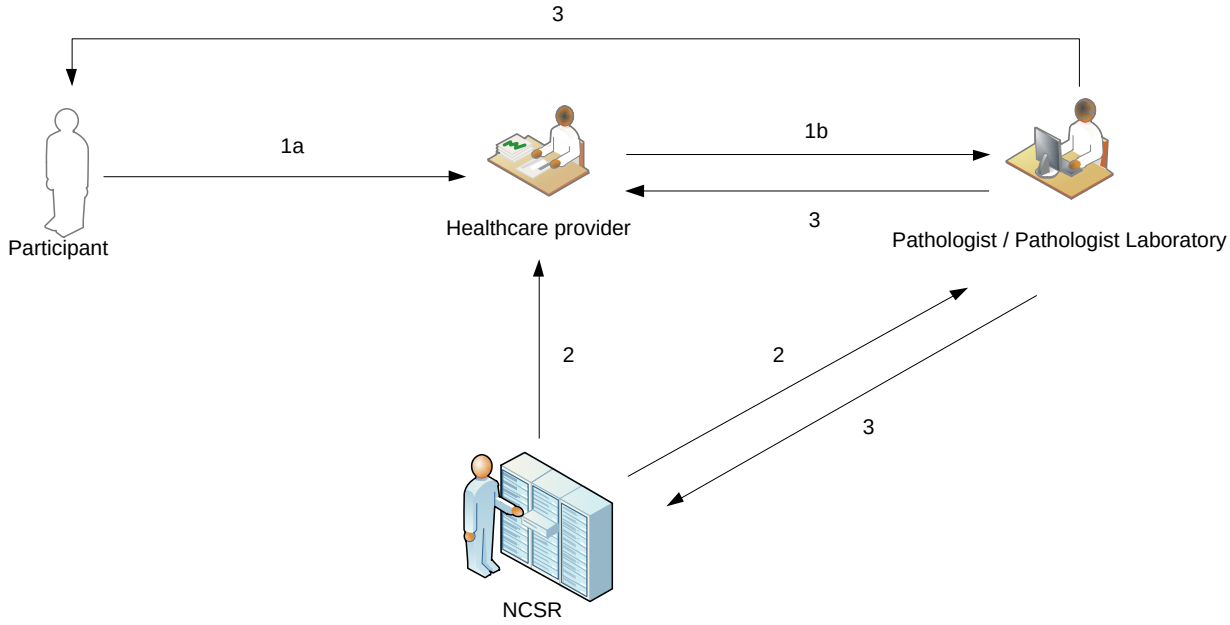


Flow	Description	Legislation	Comment
1	NCSR sends reminders to participant (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(f) of the NCSR Act.
2	Participant may defer screening. This would involve **collection** of personal information by NCSR.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
3	Where an individual has requested to defer screening as set out in Activity 1, NCSR will send the participant a confirmation notification (**disclosure**).	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(d) of the NCSR Act.
4	If a participant who defers has nominated a healthcare provider, the NCSR notifies that healthcare provider where the healthcare provider has elected to receive correspondence. This would involve the **disclosure** of personal information.	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(j) of the NCSR Act.

5. 6. 3 Activity 3 - Screen participant

Figure 12 below sets out the information flows participants, pathologists / pathology laboratories, healthcare providers and the NCSR as part of the screening process.

Figure 12 - Screen participant

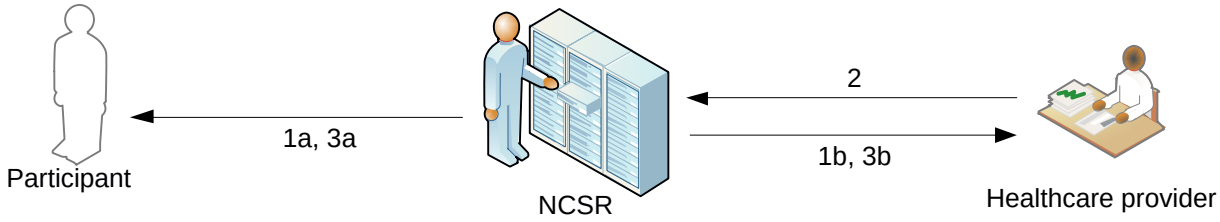


Flow	Description	Legislation	Comment
1a	Healthcare provider conducts test on participant	-	-
1b	Healthcare provider provides initial screening test to pathologist		
2	NCSR may disclose patients' cervical screening history to pathology labs and healthcare providers (GPs).	APP 6	Disclosure authorised by ss 17(3)(a) and 12(1)(g) and (j) of the NCSR Act.
3	Pathologist sends results to participant, healthcare provider and NCSR (**collection**).	APP 3	Collection authorised by s 17(1) of the NCSR Act.

5. 6. 4 Activity 4 - Assess patient

Figure 13 below sets out the information flows between participants, the NCSR and healthcare providers as part of assessing the participant.

Figure 13 - Assess patient

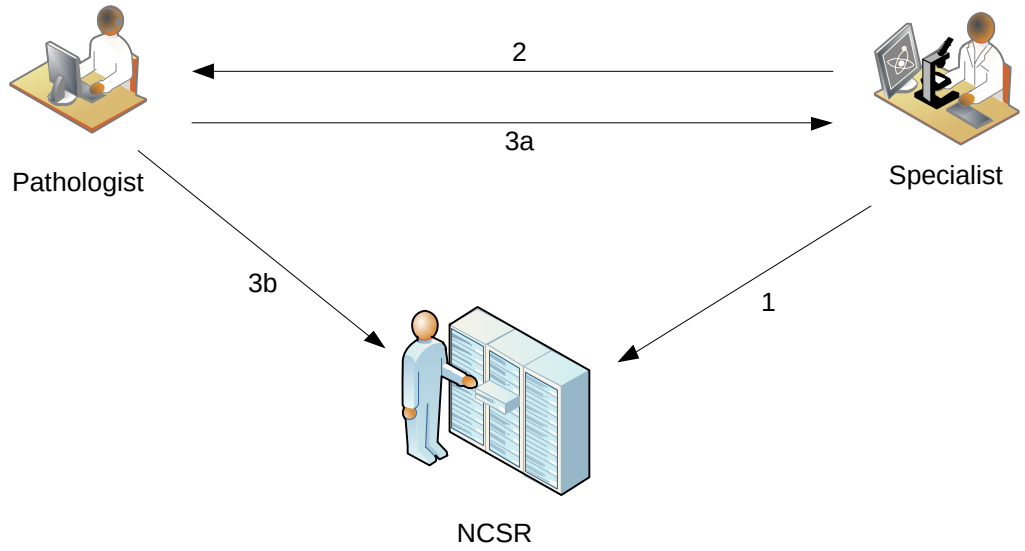


Flow	Description	Legislation	Comment
	NCSR **discloses** personal information by issuing reminders (including a positive reminder follow up, where appropriate) to the:	APP 6	Disclosure by NCSR authorised by ss 17(3)(a), 12(1)(f) and 12(1)(g) of the NCSR Act.
1a	participant; and		
1b	healthcare provider.		
2	After participant visits healthcare provider, healthcare provider makes recommendation and updates NCSR. This involves **collection** of personal information by the NCSR.	APP 3	Collection authorised by s 17(1) of the NCSR Act.
	NCSR **discloses** personal information by issuing reminders (including a no screening recorded follow up, where appropriate) to the:	APP 6	Disclosure by NCSR authorised by ss 17(3)(a), 12(1)(f) and 12(1)(g) of the NCSR Act.
3a	participant; and		
3b	healthcare provider.		

5. 6. 5 Activity 5 - Diagnose patient and outcomes

Figure 14 below sets out the information flows between the NCSR, pathologists and specialists as part of the diagnosis process.

Figure 14 - Diagnose patient and outcomes

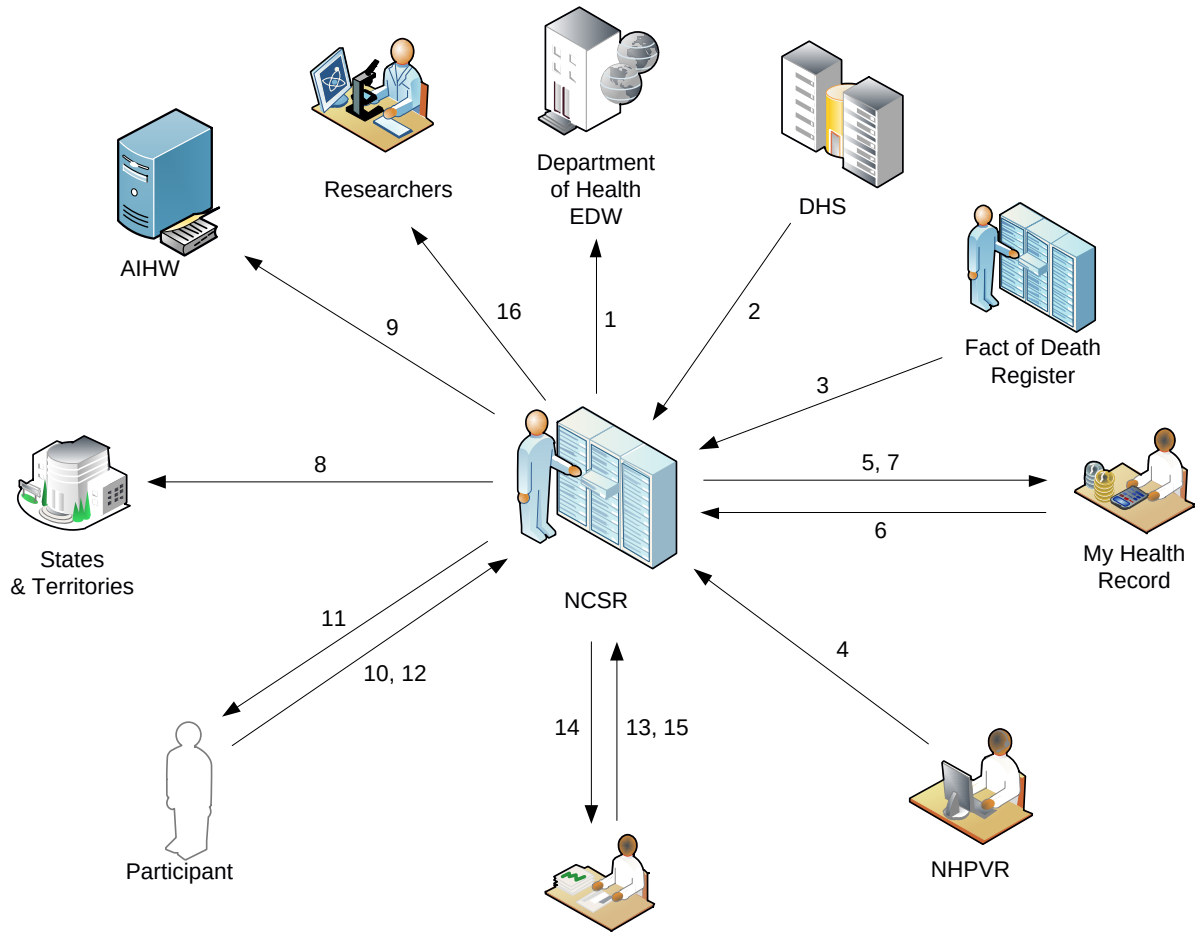


Flow	Description	Legislation	Comment
1	After participant visits specialist, specialist conducts test and updates the NCSR. This will involve **collection** of personal and sensitive information by the NCSR.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
2	Specialist sends specimen to pathologist.	-	-
	After testing the specimen, the pathologist:		
3a	sends the results to the specialist; and	-	-
3b	sends the results to the NCSR and NCSR collects only those tests related to participants (**collection** of personal and sensitive information).	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.

5.7 Reporting and ongoing access

Figure 15 below sets out the reporting and ongoing access information flows between the NCSR and various entities.

Figure 15 - Reporting and ongoing access



Flow	Description	Legislation	Comment
1	Personal information, HIs and Medicare Numbers will be provided to the Department of Health's Data Warehouse (EDW) for joining data from other systems to provide statistical/analytical reports (**use**). Information will be de-identified but re-identifiable using a separate foreign key. The identifiers will not be presented in any of the reports.	APP 6 HI Act	The provision of information to the EDW involves a "use" of information rather than a disclosure. This is because the information stays within Health's effective control. Use of any personal information and HIs authorised by ss 17(3)(a) and 12(1)(b) of the NCSR Act and s 26(3)(b) of the HI Act.
2	NCSR will **collect** potential participants' Medicare enrolment data and Medicare claims data from DHS via a secure file transfer. Healthcare identifiers will be	APP 3, 6 HI Act	DHS authorised to disclose healthcare identifiers under s 26(3)(b) of the HI Act in conjunction with s 17(1) of the

Flow	Description	Legislation	Comment
	provided by the HI Service Operator as part of this process.		NCSR Act. Collection of sensitive information and healthcare identifiers by NCSR authorised by s 17(1) of the NCSR Act.
3	NCSR **collects** and integrates aggregated death information from the Fact of Death Register.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
4	NCSR **collects** participants' HPV completion status with a date from NHPVR.	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
5	NCSR verifies whether the participant has a My Health Record and will **disclose** a HI to My Health Records to confirm whether they have a record for that person.	APP 6 HI Act My Health Records Act	Disclosure of HI authorised by ss 17(3)(a) and 12(1)(a) and (i) of the NCSR Act and s 26(3)(b) of the HI Act. Collection by My Health Record system of HI authorised by s 58A of the My Health Records Act.
6	The NCSR will confirm a HI match with the HI System Operator. Then, My Health Records will check authorisation to publish. NCSR then **collects** the HI and any other information provided.	APP 3 HI Act My Health Records Act	Disclosure by My Health Record system of HI authorised by s 58A of the My Health Records Act. Collection of HI by NCSR authorised by s 17(1) of the NCSR Act.
7	NCSR will then **disclose** to My Health Record a participant's screening status information. Healthcare providers and participants will be able to access My Health Record to view this status.	APP 6 HI and MHR legislation	Disclosure by NCSR of HI and personal information authorised by ss 17(3)(a) and 12(1)(a) and (i) of the NCSR Act and s 26(3)(b) of the HI Act. Collection by My Health Record system of HI authorised by s 58A of the My Health Records Act.
8	NCSR will **disclose** data (including HIs and Medicare numbers) to State and Territory health departments for reporting.	APP 6 HI Act	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(k) of the NCSR Act and s 26(3)(b) of the HI Act.
9	NCSR will provide raw data to AIHW. [8]	APP 6	Disclosure authorised by ss 17(3)(a) and 12(1)(b) of the NCSR Act.

[8] Raw data provided to AIHW is generally de-identified and encrypted inflight. However, AIHW can, through Ethics approval, seek an agreement as an 'integration authority' to use identified data for the purpose of data linkage for reporting.

Flow	Description	Legislation	Comment
10	Participants logging into NCSR portal provide their username and password to the NCSR.	APP 3	Collection by NCSR authorised by s 17(3)(a) of the NCSR Act.
11	NCSR **discloses** to participant the participant's information, including name, address, DOB, gender, ATSI/CALD status and nominated healthcare provider through the NCSR portal.	APP 6	Disclosure by NCSR authorised by ss 17(3)(a) and 12(1)(i) of the NCSR Act.
12	Participant may update certain personal information on the NCSR including address, CALD and ATSI status (involves a **collection** by the NCSR).	APP 3	Collection by NCSR authorised by s 17(1) of the NCSR Act.
13	Healthcare providers (including specialists) and PFUF officers access the NCSR through portal (or software for healthcare provider) involving a multifactor authentication including username, password and, for healthcare providers, a NASH key. Enrolment and authorisation is a one off.	APP 3	Collection by NCSR authorised by ss 17(3)(a) and 12(1)(j) of the NCSR Act.
14	NCSR **discloses** to healthcare provider / specialists or PFUF officer their client's records.	APP 6	Disclosure to (and, where applicable, collection by) healthcare providers authorised by ss 17(3)(a) and 12(1)(j) of the NCSR Act.
15	Healthcare provider / specialist can update participant's demographic details (subject to master data management rules).	APP 3	Collection by NCSR (and, where applicable, disclosure by healthcare providers) authorised by s 17(1) of the NCSR Act.
16	NCSR will **disclose** information to appropriate researchers in accordance with its data access and release policy.	APP 6	Disclosure to healthcare providers authorised by ss 17(3)(a) and 12(1)(n) of the NCSR Act.

6. Privacy Act analysis

6.1 Privacy principles and relevant principles for assessing impacts

This PIA assesses the NCSR against the purposes and objects of the APPs more broadly. In this regard, this PIA particularly focuses on:

- open and transparent management of personal information (APP 1);
- notification of the collection of personal information (APP 5);
- collection of solicited personal information (APP 3);
- use or disclosure of personal information (APP 6);
- security of personal information (APP 11);
- quality of personal information (APP 10);
- access to personal information (APP 12); and
- correction of personal information (APP 13).

In addition, this PIA assesses risks based on reasonable community expectations of privacy. It relies on research which indicates that the community is likely to have privacy concerns about proposals which involve:

(a) new ways of identifying individuals;

(b) requirements for individuals to present identification in more circumstances;

(c) the possibility of negative consequences for the individual; or

(d) the possibility of function creep. [9]

6.2 Open and transparent management of personal information and notification of the collection of personal information (APPs 1 and 5)

Underpinning APPs 1 and 5 is the concept of transparency in the management of personal information. It is important that individuals are given a clear picture about what information (in particular, personal information) is collected by NCSR and how it is used and disclosed as part of the process.

6. 2. 1 APP 1

APP 1 requires that the NCSR:

- take reasonable steps to implement practices, procedures and systems that will ensure the NCSR complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1. 2);
- have a clearly expressed and up-to-date privacy policy about how the entity manages personal information (APP 1. 3 and 1. 4); and
- take reasonable steps to make its APP privacy policy available free of charge in an appropriate form (APP 1. 5) and, upon request, in a particular form (APP 1. 6).

To comply with APP 1, the NCSR should develop a privacy policy and make it publicly available on its website. The privacy policy should contain:

- the kinds of personal information collected and held by the NCSR (APP 1. 4(a));

[9] Office of the Privacy Commissioner, *Managing Privacy Risk* (November 2004), page 16.

- how personal information is collected and held by the NCSR (including that it will be held by the contracted service provider for the NCSR, Telstra Health, on behalf of Health) (APP 1. 4(b));
- the purposes for which personal information is collected, held, used and disclosed (referring to the purposes set out in clause 12 of the NCSR Act) (APP 1. 4(c));
- how an individual may access their personal information and seek its correction (APP 1. 4(d)); and
- how an individual may complain if Health or Telstra Health breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1. 4(e)).

Recommendation 1 The NCSR should have an easily accessible online privacy setting out how the NCSR collects personal information, the kinds of personal information collected, the purposes for which the information is collected, held, used and disclosed, how the information may be accessed and corrected, and how an individual may make a complaint in relation to their personal information held by the NCSR.

More broadly, APP 1 is about ensuring that there is appropriate oversight and governance of privacy issues. In this respect, Health should consider implementing an overarching privacy governance strategy and a forum in which the governance of privacy issues can be discussed.

Recommendation 2 Health should also have a privacy governance strategy to ensure there is oversight of the project from a privacy perspective and a forum in which these strategies can be discussed.

6. 2. 2 APP 5

APP 5 requires that when the NCSR collects personal information, the NCSR must take reasonable steps (if any) to notify (or otherwise make aware) the individuals whose information is collected.

The NCSR must notify (or otherwise make aware) the individuals of the relevant matters in APP 5. 2. The matters that are relevant are:

- that the NCSR (that is, Health) is collecting the information;
- from whom the information is collected and the circumstances of that collection (including that Telstra Health will be operating the NCSR);
- the fact that the collection is authorised under the NCSR Act;
- the purposes for which the NCSR collects the personal information;
- the main consequences for the individual if the information is not collected;
- to whom the NCSR will disclose the information; and
- that the Privacy Policy contains information about how the individual may:
  - access the personal information the NCSR has collected and seek the correction of that information; and
  - complain about a breach of the APPs and how the NCSR will deal with the complaint.

The key points where notification to individuals is required are:

- data migration and looking up information using various directory services;
- inviting participation in the NBCSP or NCSP; and

- interacting with the NCSR online.

Notification in relation to data migration and looking up information using directory services

In our view, APP 5 is unlikely to require the NCSR to specifically notify individuals for each particular and systematic collection of personal information involved in, amongst others, verifying healthcare identifiers with the HI Service or other information with various directory services for the following reasons:

- the APP Guidelines at [5. 4] state that "reasonable steps" to notify individuals or otherwise make individuals aware of the matters in APP 5. 2 "depend upon circumstances that include…the practicability, including time and cost involved";
- given the large number of individuals whose information will be transferred during the migration process, it is impractical to notify each person of the collection of their personal information; and
- given the large number of systemised steps in the NCSR verification and screening programs involving collections of individuals' personal information, it is impractical to notify each person of the collection of their personal information.

In place of individual notifications, the NCSR, Health, DHS and the relevant State and Territory Health Departments should develop a communications strategy prior to the commencement of the NCSR to ensure that individuals are aware of the matters in APP 5. 2.

The same form of notification may be used in relation to information collected in the process of verifying healthcare identifiers through the HI Service and interacting with the My Health Record system. These processes will involve a high volume of disclosures and collections of healthcare identifiers of which it would be impractical to specifically notify individuals.

Recommendation 3	The NCSR, Health, DHS and the relevant State and Territory Health Departments should communicate to individuals that the NCSR will involve a number of systemised collections of their personal information for the effective administration of the NCSR. It should also be made clear to individuals that personal information collected by the NCSR will be communicated to My Health Record. These communications should be accessible online and other appropriate media and should be covered in relevant privacy policies.

Notification at the start of the screening program

The NCSR should notify participants of the collection of their personal information along the screening pathway. This requirement would be satisfied in relation to the NBCSP by including the relevant matters in APP 5. 2 in the information booklet that will accompany the letter inviting a person to participate in the screening program. The booklet should notify individuals of the relevant matters in APP 5. 2 (outlined above), including collection from:

- the participant when they provide information to the NCSR, including information they give when they opt out or defer;
- the participant's GP or healthcare worker, including information they give:
  - when their patient opts out; and/or
  - after they assess the patient and update the NCSR;
- the pathologist when the pathologist updates the participant's:
  - details in the NCSR;
  - screening test details;

- the participant's participation details; or
- screening test results; and

- the specialist when they update the NCSR after conducting a test.

Recommendation 4 The information booklet accompanying the screening invitation letter for the NBCSP should notify individuals of certain matters, including when the NCSR is likely to collect their information, their opt out rights and provide the link to the NCSR's online privacy policy.

In relation to the cervical cancer screening program, we note that individuals may voluntarily undergo screening rather than be invited to screen. In these circumstances, the requirement in APP 5 for the NCSR to notify the participant would arise upon collection of that participant's information by the NCSR. In practice, however, we consider that APP 5 would be satisfied if the healthcare provider providing the screening service notified the participant prior to screening that their information would be collected and used by the NCSR. This could be achieved through the provision of information to practitioners that can be given to patients.

Interaction with the NCSR online

For individuals that interact with the NCSR online via the web portal, it is important that those individuals understand how the NCSR will collect and use personal information. For this reason, the web portal should be accompanied by a layered privacy notice which is accessible to users.

Recommendation 5 A layered privacy notice is developed for the web portal. A layered privacy notice involves initially notifying an individual of the basic privacy issues affecting them, with the option to access more detailed information (for example, through the use of a drop-down box, information boxes which appear when the mouse cursor hovers over particular information or a link to a more detailed description.

6.3 Collection of solicited personal information (APP 3)

The collection of personal information attracts a range of barriers given the privacy concerns with such activities. In particular, APP 3 requires that:

- an APP entity must not collect "*personal information*" (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities (APP 3. 1); and
- an APP entity must not collect "*sensitive information*"[10] unless the person consents to the collection of the information and the information is reasonably necessary for, or directly related to, one or more of the department's functions or activities (APP 3. 3) or an exception applies (e. g. the collection is required or authorised by an Australian law) (APP 3. 4).

Section 5 sets out the information flows between various entities in connection with the NCSR. We understand that the types of personal information which the NCSR will likely collect from individuals as well as other registers, healthcare providers and other external sources (including governmental) include an individual's:

- name;

[10] "Sensitive information" is defined in section 6 of the Privacy Act and includes "health information about an individual".

- address;
- contact details (telephone, email);
- date of birth;
- gender;
- sex (for cervical screening);
- Medicare card number, enrolment and claims data;
- Healthcare Identifier;
- Indigenous status;
- language spoken at home;
- personal representative (within the meaning of the NCSR Act);
- interpreter (if required);
- country of origin and/or cultural identity;
- need for assistance to manage medical condition/disability status;
- nominated healthcare provider;
- nominated additional address for correspondence;
- information regarding screening management, assessment and diagnosis, and screening test results;
- results of related medical procedures performed following a positive test result;
- HPV vaccination status; and
- Fact of Death data.

Clause 17 of the NCSR Act sets out the dealings of information that are authorised under the NCSR Act. In particular, clause 17(1) provides a broad authorisation for a person to collect, record, disclose or use personal information, key information for an individual or information that is commercial-in-confidence if the person does so for the purposes of including information in the NCSR. As indicated by the Note in the NCSR Act on this clause, the intention of clause 17(1) is that it is an authorisation for the purposes of other laws, including the APPs. In this regard, our view is that clause 17(1) satisfies the exception in APP 3. 4(a) and will operate to authorise the NCSR to collect personal information, particularly sensitive information, for the purposes of including the information in the NCSR.

Further, although this PIA focuses on the privacy implications for the NCSR, it incidentally considers whether the ordinary operations of the NCSR could impose privacy risks on other entities. This is particularly relevant for where there may be a disclosure of personal information to another agency or directory service when authenticating or verifying particular credentials. In this regard, clause 17(3) of the NCSR Act will generally authorise persons to collect, record, disclose or use protected information[11] and key information in a number of circumstances. Amongst others, these circumstances include where:

(a) the person does so for the purposes of the NCSR (as set out in clause 12 of the NCSR Act) and is an officer or employee of, or engaged by, the Commonwealth;

(b) the person is a healthcare provider and the information is about screening or a diagnosis and the collection, recording, disclosure or use is for the purposes of providing healthcare to the individual in relation to the designated cancer; and

[11] "Protected information" is defined in section 4 of the NCSR Act to include personal information and information that is commercial-in-confidence that has been included in the NCSR or otherwise obtained in accordance with the NCSR Act.

(c) the collection, recording, disclosure or use is required or permitted by the law of a participating State or Territory and the person is an officer or employee of, or engaged by, that jurisdiction.

In our view, all collections of personal information in connection with the NCSR, as set out in the information flows set out in section 5, will fall within the scope of clause 17(1) or 17(3) of the NCSR Act.

For completeness, we note that collections of healthcare identifiers are also authorised under the HI Act as indicated above in section 5 and explained in further detail in section 7.4 below.

6.4 Unsolicited personal information (APP 4)

APP 4 provides that where an APP entity receives unsolicited personal information, it must determine within a reasonable period whether it could have collected the information under APP 3. If not, the APP entity must as soon as practicable destroy or de-identify the information.

In our view, there is some risk of the NCSR or any other relevant APP entity collecting unsolicited personal information in connection with the NCSR. This is because, in relation to cervical screening, some pathology reports provided to the NCSR may include results for other tests not associated with the screening pathway. Similarly, in relation to bowel screening, specialists may provide reports for individuals who are not participating in the Program.

However, the privacy risks associated with this collection are mitigated as the NCSR will only store information relating to individuals participating in a screening program. Further, the types of information collected directly from individuals by healthcare providers and provided to the NCSR are well-defined and we understand that the NCSR will only store information which has a corresponding pre-programmed data field.

Similarly, any collections of personal information directly from individuals through the NCSR portal will be in relation to particular types of information (namely, updating contact details), with little scope for individuals to provide information which the NCSR has not solicited.

For completeness, we note the relevance of clause 13 of the NCSR Act which provides for mandatory reporting of information to the Commonwealth Chief Medical Officer. While this is not strictly a collection of unsolicited information, the regime of mandatory reporting is such that even if a person has opted out or is otherwise not participating in the NCSR they will have information collected by Health, even though it may not be stored in the NCSR.

In this regard, we recommend that the rules prescribed by the Minister for the purposes of clause 13 of the NCSR Act should address how to deal with information relating to individuals who are not participating in the NCSR, including information which is provided to the NCSR either by pathologists or specialists or in accordance with the mandatory reporting provision in clause 13. At minimum, the rules should provide that any information received by the NCSR which fits the above criteria should be made inaccessible to any person accessing the NCSR in accordance with appropriate security procedures.

Recommendation 6 The rules prescribed by the Minister for the purposes of clause 13 of the NCSR Act should address privacy issues concerning the collection of information of individuals who are not participating in the NCSR, including where individuals have opted out of participation. At minimum, the rules should provide that any information received by the NCSR in relation to non-participants (including individuals who have opted out) should be made inaccessible to any person accessing the NCSR in accordance with appropriate security procedures.

6.5 Use and disclosure of personal information (APP 6)

APP 6 regulates the use and disclosure of personal information. In particular, it provides that an APP entity may only use or disclose personal information which it holds for the purpose for which it was collected unless the individual to whom the personal information relates otherwise consents (APP 6. 1(a)), the use or disclosure or information is required or authorised by law (APP 6. 2(b)), or another exception applies.

The information flows in section 5 set out the uses and disclosures of information that will occur in relation to the NCSR. It also sets out how a use or disclosure will be authorised under the NCSR Act, which is also an authorisation under APP 6. 2(b).

In particular, section 17(1) of the NCSR Act authorises uses and disclosures of personal information, key information or commercial-in-confidence information[12] by persons where the purpose of the use or disclosure is to include the information in the NCSR. In general, our view is that this section does not authorise uses or disclosures of information in the NCSR to other entities, but it does authorise other entities (including government departments, agencies and healthcare providers) to disclose information to the NCSR for inclusion in the NCSR.

Section 17(3) of the NCSR Act provides further authorisations for persons to use and/or disclose protected information and key information. Most relevantly, section 17(3)(a) authorises uses or disclosures of information by Commonwealth employees (for example, Health) or persons engaged by Commonwealth (for example, Telstra Health) for the purposes of the NCSR. Section 12(1) of the NCSR Act sets out a wide range of purposes for the NCSR, including:

(a) establishing and keeping an electronic database of records relating to screening and diagnoses associated with the designated cancers;

(b) collecting, analysing and publishing statistics and other information relating to screening and diagnoses associated with the designated cancers;

(c) monitoring the effectiveness, quality and safety of screening and diagnoses associated with the designated cancers;

(d) providing an individual with an invitation to undergo screening;

(e) providing an individual with a test kit for screening;

(f) advising an individual when the individual is due to undergo a screening test or when action may need to be taken after a screening test;

(g) advising a participant's nominated healthcare provider for screening associated with a designated cancer (if any) when the individual is due to undergo, or when action may need to be taken after, a screening test associated with the designated cancer;

(h) advising a participating State or Territory when action may need to be taken after a screening test for an individual residing in the State or Territory;

(i) providing an individual access to information relating to the individual about screening and diagnoses associated with a designated cancer;

(j) providing healthcare providers access to information about screening and diagnoses associated with a designated cancer in relation to an individual, for the purposes of providing healthcare to the individual in relation to the designated cancer;

(k) providing a participating State or Territory with access to information relating to individuals residing in the State or Territory in connection with screening and diagnoses associated with the designated cancers;

(l) planning, delivering and promoting healthcare and services in relation to the designated cancers;

[12] These terms are defined in section 4 of the NCSR Act.

(m) reporting to international organisations in relation to the designated cancers; and

(n) research relating to healthcare, screening or a designated cancer.

In our view, and as set out in section 5, each disclosure of personal information in relation to the NCSR either falls within the scope of section 17(1) or 17(3) of the NCSR Act. For completeness, we also note that in many instances, the authorisations for disclosure in the NCSR Act will not need to be relied upon, as in many instances the disclosures by the NCSR will fall within the primary purpose for which the information was initially collected by the NCSR (which are reflected in the purposes set out in section 12 of the NCSR Act).

6.6 Cross-border disclosure of personal information (APP 8)

APP 8 places restrictions on APP entities seeking to disclose personal information to an overseas recipient. In particular, APP 8 provides that before an APP entity discloses personal information overseas, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs, unless an exception applies.

We understand that any information held by the NCSR will be stored in locations in Australia and that disclosures to overseas recipients will not occur. On this basis, we consider that there are no significant privacy risks associated with overseas disclosure and APP 8 is unlikely to apply.

6.7 Adoption by organisations of government related identifiers (APP 9)

The adoption of health care identifiers is not prohibited by the HI Act. Therefore, the obligations in relation to the adoption of healthcare identifiers fall under APP 9. APP 9. 1 provides:

> *An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:*
>
> *(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or*
>
> *(b) subclause 9. 3 applies in relation to the adoption.*

Telstra Health (which has been contracted to develop and operate the Register on behalf of the Commonwealth), would not be adopting healthcare identifiers as its own identifier of the participant. Rather, Telstra Health would be operating the Register on behalf of the Commonwealth and the adoption of the healthcare identifier would be for the purposes of the Register and not as Telstra Health's own identifier for the healthcare recipient or provider.

Therefore, APP 9 does not operate in the circumstances of the Register. This means no authorisation under the NCSR Act or the HI Act is required for the adoption of healthcare identifiers by Telstra Health.

6.8 Security of personal information (APP 11), unauthorised access and section 95B of the Privacy Act

APP 11. 1 requires that if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference, loss, unauthorised access, modification or disclosure.

As indicated in the information flows set out above in section 5, the NCSR will have multiple access points (for example, individuals and healthcare providers will be able to access the NCSR portal, and healthcare providers will be able to access the NCSR through particular software). Each access point increases the risk to the NCSR and information contained therein to an extent which is proportionate to who is likely to be using the access point,

what information can be accessed through that access point, and the system security protections regulating that access point.

It is beyond the scope of this PIA to undertake a comprehensive threat analysis or evaluate in detail the precise security and access arrangements for the NCSR, especially in circumstances where these are largely regulated by a commercial-in-confidence services agreement. However, from a privacy perspective, what is important is that the outcome required by APP 11 is met, namely that reasonable steps are taken to protect information from:

(a) misuse, interference and loss; and

(b) unauthorised access, modification or disclosure.

However, we note a number of key privacy risk mitigation strategies relating to the access of data, some of which are already incorporated into the system design of the NCSR and some further strategies which should be considered. Mitigation strategies already incorporated into the design of the NCSR include:

- the services agreement between Health and Telstra Health requires Telstra Health to develop a data protection plan which is consistent with the Protective Security Policy Framework (**PSPF**), which identifies responsibilities and sets out requirements relating to managing security risks, and the Information Security Manual (**ISM**), which sets out the standard which governs the security of government ICT systems;
- access by individuals to their information through the NCSR portal will be protected by a username and password, and the ability to amend information on the NCSR will not extend to clinical information;
- access by healthcare providers through the NCSR portal will be protected by a username, password and NASH credential and will require the healthcare provider to disclose certain information about a client to access his or her information. Direct access by healthcare providers to the NCSR through the practice management software involves similar protections;
- information in the NCSR will be stored as encrypted data in accordance with appropriate encryption standards to prevent easy identification of personal information through an unauthorised access point; and
- the NCSR information hosting locations will be in Australia and information is unlikely to be disclosed overseas (unless expressly approved by Health).

However, to mitigate the risk of unauthorised or inappropriate access to the NCSR (including by health providers who, depending on final design, may have access to browse the NCSR for individuals who may not be their patients), we recommend a number of mitigation strategies to be considered, including:

- any person or entity which has access to the NCSR should receive privacy training so that they are aware of the obligations imposed by the APPs and any other relevant privacy laws. This applies particularly to healthcare providers as they have significant access to the NCSR. Training can be delivered in an online format and should include a direction that the NCSR must not be accessed to find information about individuals other than in connection with providing healthcare services to those individuals related to the designated cancers;
- similarly, any person or entity which has direct access to the NCSR (namely, healthcare providers and Telstra Health staff) should sign terms and conditions upon first accessing the NCSR (and again whenever the terms and conditions of use are updated) agreeing that they will not use NCSR information except in connection with providing healthcare services to a particular individual; and
- Telstra Health should ensure that its security policies and procedures are communicated effectively to their support staff.

Recommendation 7	People/entities who have access to the NCSR should undergo privacy training (including familiarisation with key sections of the OAIC's *Guide to securing personal information*) so that they are aware of the obligations imposed by relevant privacy laws, including the need to take reasonable steps to protect personal information from unauthorised access, modification or disclosure.
Recommendation 8	People/entities who have access to the NCSR should agree to terms and conditions containing rights and obligations regarding their access to the NCSR. Those terms and conditions should note the potential criminal offences for unauthorised access or disclosure of information on the NCSR (where applicable under the NCSR Act). People/entities with administrative access to the NCSR or access to a large amount of data should be held to a higher level of scrutiny and obligations, for example through minimum security vetting.
Recommendation 9	An audit trail function should be included in the NCSR's design so that issues regarding potential unauthorised access or disclosure are able to be identified and investigated. To the extent possible, this functionality should allow NCSR to proactively search for inappropriate access and detect potential instances of healthcare providers browsing the NCSR for purposes unrelated to the healthcare of their patients.
Recommendation 10	Telstra Health should ensure that its security policies and procedures are communicated effectively to their support staff.

For completeness, we note that the OAIC has asked that this PIA consider what measures must be put in place to address section 95B of the Privacy Act.

Section 95B(1) of the Privacy Act requires agencies (such as Health) entering into a Commonwealth contract[13] to take contractual measures to ensure that a contracted service provider[14] (such as Telstra Health) does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency. Section 95B(2) requires that agencies must ensure that such a Commonwealth contract does not authorise a contracted service provider for the contract to do or engage in such an act or practice, while section 95B(3) further requires agencies to ensure that the contract with the service provider contains provisions to ensure that any subcontract does not authorise an act or practice that would breach an APP if done by the agency.

The services agreement between Health and Telstra Health is commercial-in-confidence and its contents cannot be disclosed in this PIA. In any event, disclosing the system security particulars of how Telstra Health intends to protect information in the NCSR could itself expose security risks in Telstra Health's system and make it a target for attacks. However, for the purposes of this PIA, we note that there is a wide range of privacy obligations imposed on Telstra Health by the agreement, including a provision to the effect of sections 95B(2) and (3). In this regard, our view is that the contractual measures taken by Health and the obligations imposed on Telstra Health by Health to implement sufficient security measures meet the requirements of APP 11 and section 95B of the Privacy Act.

[13] "Commonwealth contract" is defined in s 6 of the Privacy Act to mean a contract to which the Commonwealth or an agency is or was a party and under which services are or were to be provided to an agency.

[14] A "contracted service provider" for a government contract means an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency under the government contract and includes a subcontractor (s 6 Privacy Act).

6.9 Access to, and quality and correction of, personal information (APPs 10, 12 and 13)

APPs 10, 12 and 13 deal with similar privacy concerns. APP 10 requires APP entities to take reasonable steps (if any) to ensure the accuracy of information that it collects, uses and discloses. APP 12 broadly requires that APP entities must provide individuals with access to personal information it holds and APP 13 requires APP entities to take reasonable steps (if any) to correct information as requested by an individual.

In relation to APP 10, our view is that it is reasonable to rely on the entities (government agencies and healthcare providers) from which the NCSR collects the majority of its information. In this regard, we note that the APP Guidelines at [10. 7] provide that:

> *In some circumstances it will be reasonable for an APP entity to take no steps to ensure the quality of personal information. For example, where an entity collects personal information from a source known to be reliable (such as the individual concerned) it may be reasonable to take no steps to ensure the quality of personal information.*

We consider that individuals and their healthcare providers (including doctors, specialists and pathologists) are reliable and trusted sources of the kinds of information which will be gathered in relation to those individuals. The NCSR also involves verification processes which will assist in ensuring accuracy in identifying the persons providing information and identifying the participant to whom the information relates.

Further, the NCSR allows for individuals and their healthcare providers to access information relevant to themselves/their patients (namely, through the NCSR portal or healthcare provider software). This satisfies APP 12 (which requires the NCSR to give individuals access to information about them). This is also likely to meet the requirements in APPs 10 and 13 as individuals may amend certain of their details (for example, their address, CALD and ATSI statuses and update their nominated healthcare provider) when they access the NCSR through the portal.

In addition, we understand that Health is considering whether to contact participants from time to time to ensure that their demographic details in the NCSR are up to date. The privacy implications of this are considered in further detail below in section 7.12; however, we consider that this approach would constitute a reasonable step towards improving the accuracy and completeness of NCSR information for the purposes of APP 10.

The fact that individuals will not be able to amend their clinical information on the NCSR is unlikely to breach APP 13. This is because it is reasonable for the NCSR to be satisfied of the accuracy of the clinical information that it collects from healthcare providers who, by virtue of their role, are in a better position than a patient to understand and communicate clinical information to the NCSR. However, to achieve a more privacy positive result, Health should consider adopting a process similar to that adopted by the My Health Record system, whereby:

(a) if an individual considers that their health information in the NCSR is incorrect, they must first approach the healthcare provider who authorised the document seeking correction;

(b) if the healthcare provider believes that the health information uploaded to the NCSR should be corrected, the healthcare provider may amend the information directly;

(c) if the healthcare provider believes that the health information uploaded to the NCSR is already accurate, complete and up-to-date, the healthcare provider notifies the NCSR of this result, providing reasons why correction would be inappropriate; and

(d) the NCSR sends the participant a written notice refusing to correct the information which, as required by APP 13. 3, sets out:

(i) the reasons for the refusal (except to the extent that it would be unreasonable to do so);

(ii) the mechanisms available to complain about the refusal; and

(iii) any other matter prescribed by the relevant regulations.

Recommendation 11 Health should consider implementing a process similar to that in the My Health Record system for dealing with requests to correct clinical information held in the NCSR. Rather than contacting the NCSR directly, this involves an individual contacting the healthcare provider who authored the document containing their clinical information, who in turn can notify the NCSR whether or not the information should be corrected (providing reasons) which then allows the NCSR to deal with the request and notify the participant of the outcome.

6. 10. 1 Ensuring accuracy of nominated healthcare provider

Clause 14(1)(a) of the NCSR Act provides that individuals may request that a particular healthcare provider(s) be their nominated healthcare provider for screening associated with a designated cancer.

We have been specifically asked to consider how best to ensure that the nominated healthcare provider for an individual which is recorded in the NCSR is accurate, which is a matter which directly relates to APPs 10, 12 and 13. Individuals attend different healthcare providers for a range of reasons, including (amongst others) proximity, specialty, convenience and cost. Similarly, individuals may see a particular healthcare provider one year about an issue and a different healthcare provider the next year about the same issue. Consequently, there is a possibility that an individual who no longer attends the nominated healthcare provider forgets to update the NCSR to reflect this change. This has privacy implications as the NCSR would erroneously sends information to an outdated nominated healthcare provider.

In our view, this is a risk which cannot be fully mitigated in practice, as to do so would require individuals to remember and proactively update the NCSR. However, in our view, there are three mitigation strategies which the NCSR could pursue:

- the NCSR portal should allow individuals to update their nominated healthcare provider, as this will allow proactive individuals to mitigate their own privacy risk;
- the NCSR portal should allow healthcare providers to update their status as the nominated healthcare provider (in circumstances either where they have received a new patient or are aware that a patient is no longer using that healthcare provider);
- in any correspondence issued by the NCSR to a nominated healthcare provider, there should be a statement to the effect that requests the nominated healthcare provider to notify the NCSR if the healthcare provider knows they are no longer the correct nominated provider; and
- any correspondence issued by the NCSR to a participant should include information on the participant's nominated healthcare provider, an explanation of information provided to the nominated healthcare provider and easy-to-read instructions on how to change the nominated healthcare provider.

Recommendation 12 Individuals (or healthcare providers on the participant's behalf) should be able to update the nominated healthcare provider in the NCSR. Correspondence to nominated healthcare providers should request that healthcare providers notify the NCSR if they should no longer be the nominated healthcare provider. Correspondence to individuals should set out information on the participant's current nominated healthcare provider and easy-to-read instructions on how that can be changed.

In our view, these privacy risk mitigation strategies comply with APPs 10, 12 and 13 and would be reasonable for the NCSR to implement.

6.10 Best practice and continuous improvement

As the NCSR is a new project, to ensure best practice and continuous improvement, Health should consider developing and implementing a complaints management framework for any complaints received by Health or Telstra Health in relation to the NCSR. That framework should deal with how to analyse complaints and their outcomes to improve the operation of the NCSR.

Recommendation 13 As part of the privacy governance framework recommended in Recommendation 2, Health should develop and implement a complaints management framework for any complaints received by the Health or Telstra Health in relation to the NCSR. This should include a process for dealing with complaints made in relation to how a State or Territory has handled NCSR information which has been reported to it from the NCSR.

Further, in order to ensure that the NCSR is operating as intended and that privacy issues are being appropriately dealt with, the operation of the NCSR should be reviewed periodically. Conducting a review can uncover any unintended operations/activities and privacy issues. Exposing these is important for the proper functioning of the NCSR and to ensure it is providing the service it was designed to provide without unnecessarily encroaching on privacy. In contrast, failing to conduct a review will miss an opportunity to improve the NCSR and to check whether it is operating appropriately. In the absence of scrutinising the operation of the NCSR, it will be uncertain whether it is operating as intended and whether the recommendations in this PIA remain sufficient to manage the privacy issues identified.

The review should particularly consider whether there were any complaints or issues raised about the management of personal information by Health or Telstra Health. More broadly, the review should be undertaken to ensure that the NCSR is operating as intended and that the recommendations in this PIA remain sufficient to manage the privacy issues identified.

The review should be conducted periodically (that is, after two or three years of operation) or in accordance with any review by Health of Telstra Health's performance as a contracted service provider as set out in the service agreement (if any). This will ensure that the NCSR has been operated for a sufficient period of time to enable enough history and experience to be built up so that the review is meaningful.

Recommendation 14 Health should review the operation of the NCSR from a privacy perspective periodically (that is, after two or three years of operation) or in accordance with any review of Telstra Health's performance of its obligations under the service agreement at specified in the service agreement (if any).

7. Further privacy issues and management strategies

This section sets out a number of privacy issues raised by the OAIC and other entities which have been consulted as part of preparing this PIA. In particular, these privacy issues relate to:

(a) migrating data to a single national register;

(b) the scale of the NCSR;

(c) handling individuals' Medicare information;

(d) linkages between the NCSR and other data sources (including the My Health Record system);

(e) access to the NCSR and data held therein;

(f) disclosure of information in the NCSR for research purposes;

(g) reporting to participating States and Territories;

(h) sending screening invitations;

(i) the opt out provisions in the NCSR Act;

(j) the privacy implications of mandatory reporting under the NCSR Act;

(k) the privacy implications of using ATSI/CALD status information; and

(l) the privacy implications of different means of communication.

7.1 Migrating data to a single national register

Establishing the NCSR involves large scale data merging. Data from the eight separate State/Territory hosted cervical screening registers and the current NBCSP Register will need to be migrated to the NCSR.

This raises a number of privacy positives and privacy risks. On one hand, migrating data from various separate registers to the one register will create an integrated system which supports the implementation of the renewed NCSP and the implementation of biennial screening under the NBCSP. This will provide a single, cost-effective service to collect and report screening data. It will enable participants and healthcare providers to provide, update and receive information. It will also allow healthcare providers to identify patient's screening eligibility and history to support clinical decision making.

On the other hand, there is a risk that there will be inaccurate matches of data between the various registers, lost data and duplication of data, which may result in incomplete and/or inaccurate records. This risk is exacerbated by the fact that legacy data will be merged as well.

Further, inaccurate matches and incomplete/inaccurate records may also lead to compromised clinical decision making. There may be confusion as to what information has been provided to the participant, what tests an individual has undertaken and the results of those tests. This may jeopardise the participant's journey along the clinical pathway. It may also pose a threat to the quality and availability of information needed to deliver the correct services to the correct individuals.

Migrating data from various sources and involving different jurisdictions and governments poses a risk that there will be confusion as to who is responsible for the above (for

example, inaccurate data matches, incomplete records and compromised clinical decision making).

There is also a risk that States and Territories will have barriers or challenges to migrating their data to the NCSR, though the legal barriers to this migration should be overcome by virtue of section 6 of the C&T Act.

To address the risks outlined in this section, it is recommended that:

Recommendation 15 Health or Telstra Health (as appropriate) should develop and test data migration and data cleansing strategies prior to undertaking migration. Robust strategies will assist in ensuring a high level of data compatibility between the registers and will decrease the risk of inaccurate matches and duplication of records.

Recommendation 16 Responsibilities with respect to cleaning and migrating data and the risks associated with it are clearly defined so privacy risks can be managed. This will help with issues around information moving between jurisdictions.

Recommendation 17 Health and the States/Territories should work together to identify what specific risk mitigation strategies, if any, are necessary for each State/Territory in order to facilitate migration of data.

7.2 Scale of the NCSR

Large scale data merging is involved in establishing the NCSR. This will create a much larger repository of personal information than that currently held in the separate registers.

There are a number of efficiency advantages resulting from consolidating several sources of screening information into one record per individual. However, the significant amount of personal information to be stored centrally on the NCSR carries with it privacy risks from a number of perspectives (for example, in relation to access and security which are addressed in other parts of this PIA).

The large centralised repository of information presents a risk that people/entities that have access to the NCSR will have access to information which is not necessary for them in performing their respective functions and/or to efficiently and effectively provide services to people recorded in the NCSR.

Further, the large scale of and nature of the information in the NCSR also make it an attractive target for people/entities that do not have access to the NCSR to try to gain access to data through other means. The C&T Act will amend the *Freedom of Information Act 1982* (**FOI Act**) to exempt the NCSR from FOI requests made in respect of information held in the NCSR. This exemption will protect the privacy of individuals whose information is stored in the NCSR and is broadly justifiable on the grounds that there are few circumstances (if any) in which the disclosure of NCSR information could be said to be in the public interest.

A number of recommendations made in this PIA address these risks. In particular, see Recommendations 8, 9, 20 and 21 which deal with system security for the NCSR and conditions for people with access to the register, as well as Recommendations 22 and 23 which set out matters which the data access and release policy for the NCSR should address.

7.3 Handling individuals' Medicare information

The NCSR will acquire a substantial amount of individuals' Medicare information. In particular, the NCSR will acquire Medicare enrolment and claims data at the data migration stage and then as a regular, ongoing process to identify potential candidates to invite for screening and excluding candidates from receiving invitations or reminders.

We understand that the NCSR system has been designed according to the best practice of collecting, using and disclosing only the minimum amount of Medicare information that is required for the purposes of the NCSR. Relevantly, Medicare enrolment data that is proposed to be collected includes Medicare number, Medicare PIN, HI, name, address, date of birth, sex, Medicare entitlement type, and ATSI status. Medicare claims data proposed to be collected similarly includes HI, claim code, specified claim code item, provider detail, date of service provided, status of the claim and claim type (Medicare or DVA).

There are a number of privacy positives and privacy risks associated with this approach. On one hand, the minimum amount of Medicare information about an individual is collected, used and disclosed by the NCSR which minimises the privacy impact on those individuals. Without this level of access to Medicare information, the NCSR would not be able to operate efficiently and could impose further privacy risks on individuals if it had to seek separately such information from the relevant entities as relevant.

However, some privacy risks remain, including that individuals' Medicare enrolment data will be made visible to other individuals, healthcare providers and NCSR staff and will be disclosed to other entities including Health EDW and the States and Territories for ongoing reporting. Health should consider managing individuals' expectations in relation to how these privacy risks will be addressed by including in its privacy policy and/or privacy notices how individuals' Medicare information will be handled by the NCSR. Health should also consider notifying individuals of the specific Medicare information being collected, used and disclosed by the NCSR in relevant public communications.

Recommendation 18 The Privacy Policy and Privacy Notices should contain concise information about how and from whom the NCSR collects information. It should also detail disclosure, including that screening information is published to the individual’s My Health record.

Despite these privacy risks, our view is that the NCSR Act authorises the collection, use and disclosure of individuals' Medicare information where such collection, use or disclosure is for the purposes of the NCSR Act and no further privacy recommendation is required. For completeness, we note that section 6.6 above sets out our view why APP 9 (adoption, use and disclosure of government identifiers) does not provide a barrier to the NCSR collecting Medicare information (including Medicare numbers).

7.4 Linkages between the NCSR and other data sources including the My Health Record system

The NCSR will have capacity to access clinically relevant information (e. g. past diagnosis of cervical and bowel cancer) in external databases and link with data to determine whether a person is eligible, including using Medicare information to determine whether an individual will be invited to screen. For example, there will be data linkages between the NCSR and the HPV Register, the Fact of Death register and the My Health Record system (although the NCSR will not collect clinical information from the My Health Record system).

One privacy positive of these data linkages between the NCSR and other databases is that it provides an integrated system, in particular it ensures that individuals are not invited to screen where that would be inappropriate. It also increases the likelihood of data matches and creating a complete record for each individual. However, linkages with other systems raise privacy risks: namely, they could leave the other registers and databases vulnerable to excess access by the NCSR as the NCSR may have access to information that is not relevant for determining eligibility or the clinical pathways.

Many of these linkages between the NCSR and other entities involve the collection, use and disclosure of healthcare identifiers. Section 5 sets out the authorisations for handling healthcare identifiers in this way.

There are privacy positives and privacy risks associated with using healthcare identifiers to match data and establish linkages between the NCSR, HPV Register and My Health Record system. Using the healthcare identifier to match data will ease integration and data flow between the systems. The use of healthcare identifiers increases the consistency and accuracy in matching the correct identity and decreases the risk of duplication of records.

However, using healthcare identifiers for this purpose expands their use, which is a potential privacy risk. However we note that this use is within the object and framework of the HI Act in that it is designed to ensure that healthcare providers can correctly match information about an individual in relation to a health service.

7. 4. 1 Linkage with My Health Record system

The NCSR is designed to link with, but not duplicate, the My Health Record system. This presents a number of privacy positives and privacy risks, as outlined below.

We understand that the intended use of data published to the My Health Record is primarily centred on:

- promoting program uptake through better interaction between healthcare providers (particularly GPs) and eligible Australians; and

- contextualising clinical information within an individual's My Health Record.

The information likely to be disclosed by the NCSR to the My Health Record system involves some personal information including healthcare identifiers and screening eligibility and status information. The NCSR will not disclose a participant's clinical information to the My Health Record system, which is consistent with the digital health objective of promoting direct publishing of clinical data to the My Health Record by healthcare providers.

As noted in the information flows in section 5 and as discussed further in section 6.5, data linkages between the NCSR and My Health Record involve a number of collections, uses and disclosures of information. These collections, uses and disclosures must be in accordance with the APPs and, where applicable, the HI Act and My Health Records Act.

Most of the legal analysis is set out in these sections above; however, it is worth noting that the NCSR itself will likely be a "healthcare provider" for the purposes of the My Health Records Act and HI Act, as it is an entity that provides healthcare. [15]

As a "registered repository operator" within the meaning of s 5 of the My Health Records Act, the NCSR will be authorised to adopt the healthcare identifier of a healthcare recipient (item 3 s 17 of the HI Act) and that of a healthcare provider (item 2 s 25B of the HI Act) for the purposes of the My Health Record System.

Recommendation 19 The NCSR should be a participant in the My Health Record system and have the necessary legislative permissions to make changes to an individual's My Health Record.

7.5 Access to the NCSR and data held on the NCSR

Various people/entities (such as Telstra Health, healthcare providers, pathology labs, contracted pathologists and individuals) will have access to the NCSR and the personal information of a significant number of individuals contained on it.

[15] "Healthcare" is defined in the My Health Records Act and HI Act to mean a "health service" within the meaning of that term in s 6FB of the Privacy Act. Our view is that the activities performed by the NCSR fall within sections 6FB(1)(a), (c) and (e) of the meaning of health service, and therefore within the meaning of healthcare for the purposes of the My Health Records Act and HI Act.

7. 5. 1 Individuals' access to the NCSR

A significant part of the design of the NCSR is that individuals will have access to view their demographic information but not their clinical records (which will be accessible either through the My Health Records system or the participant's healthcare provider). Providing individuals with access to their own demographic information on the NCSR provides a level of transparency to individuals. It gives them visibility of their information and the ability to interact with the NCSR (for example, by updating contact details or selecting a preferred communication channel).

However, this presents security and access control issues, the most significant of which is the risk of unauthorised access to an individual's information.

To address this risk, it is recommended that:

Recommendation 20 Health should review the security and access arrangements to ensure that all reasonable risks of unauthorised access are mitigated.

7. 5. 2 Other entities' access to the NCSR

Allowing various people and entities to have access to the NCSR will greatly assist in providing an efficient and effective service as it ensures that the necessary people/entities have access to all relevant information. However, there are obvious privacy risks to individuals recorded on the NCSR if access is not well managed.

There is a risk that people or entities accessing the NCSR will have access to information through the NCSR that they would not otherwise have. Further, there is a risk that people/entities may have access to information on a participant's record which the participant does not want them to see: for example, if a participant sees one GP for their HPV test and a different GP for general consultation, the participant may not want the results from one to be visible to the other. We understand that, as healthcare providers may have access to a participant's entire clinical history on the NCSR (and not just for their patients) so as to maximise a healthcare provider's ability to provide quality healthcare services, this is a possibility and we have included recommendations in section 6.8 to mitigate this privacy risk.

We understand that Health proposes that healthcare providers will be able to run audits of their patient database against the NCSR and/or look up their patients on the NCSR to see their patients' status and to assist with encouraging their patients to participate in a screening program. Health is further considering whether indigenous healthcare workers will be able to look up their patient cohort in the NCSR to identify eligible patients to offer screening tests as part of an alternative screening pathway pilot. In both instances, prior consent by the eligible person may not have been granted but these actions would be in the context of healthcare providers providing healthcare services to their patients and would be authorised under the NCSR Act.

To address the risks outlined in this subsection, it is recommended that:

Recommendation 21 The NCSR has role-based accessed controls (which are set by the system, not individuals) which limit the access of people/entities to information in a participant's record that is necessary to provide services to the participant or to serve a justified usage.

For example, pathologists may not need access to all of an individual's biographical information in order to provide services to that individual as part of the NCSR. In addition, administrative staff that perform functions in relation to the NCSR (whether retained by the Department or Telstra Health) would not ordinarily require access to clinical information stored in the NCSR. These types of role-based restrictions are important in order to avoid privacy risks associated with "browsing" records.

In addition, as various people/entities are able to access the NCSR, maintaining the security of information held on it is difficult. There is increased risk of misuse, interference and loss of data as well as unauthorised access, modification and disclosure (see APP11). There is also a risk that people/entities with access to the NCSR may not be sufficiently aware of the privacy obligations in the APPs in order to comply with them. We have previously addressed APP 11 and issues of unauthorised access, as well as recommendations in relation to managing those risks, in section 6.8 above.

7.6 Disclosure of information in the NCSR to the Health EDW and for research purposes

As set out in section 5.6, the NCSR will use healthcare identifiers by sharing personal information with Health's EDW. This information is likely to contain healthcare identifiers and Medicare numbers and will be used by Health's EDW for joining data from other systems to provide de-identified statistical and analytical reports.

Section 6.5 further sets out the use of such personal information and healthcare identifiers will be authorised by a combination of clauses 17(3)(a) and 12(1)(b) and (n) of the NCSR Act, and section 26(3)(b) of the HI Act. The combined effect of these provisions is to authorise disclosures of NCSR information for the purposes of research, or collecting, analysing and publishing statistics and other information relating to screening and diagnoses associated with designated cancers.

However, even though disclosures for research purposes are authorised by legislation, Health should consider whether information to be disclosed for research purposes can and should be de-identified prior to disclosure. This would mitigate the privacy impacts imposed on individuals from having their identified information disclosed to third parties.

Recommendation 22 A data access and release policy should be prepared which covers the disclosure of information from the NCSR for research, including whether the information should be de-identified. Where applicable, the disclosure of information will need to be in accordance with any relevant guidelines, including procedures akin to those made under sections 95 or 95A of the Privacy Act.

7.7 Reporting to participating States and Territories

As explained in section 4, the NCSR has a reporting functionality. Participating State and Territory Health Departments will have access to identifiable data for individuals residing in their jurisdiction and will be able to run their own reports to enable planning for service delivery. This access is authorised under subsection 17(3)(c) of the NCSR Act.

Access to identifiable data in the NCSR will be managed through a MoU with participating States and Territories which will address access, use and disclosure of NCSR data, physical and personnel security and secondary disclosure of data reported by the NCSR.

The flow of information from the NCSR to participating States and Territories is set out in section 5.6 and is discussed in section 6.5. The legislative basis for this disclosure is a combination of clause 17(3)(a) and clause 12(1)(h) and (k) of the NCSR Act. Together, these provide that a person may collect, make a record of, disclose or otherwise protected information for the purposes of the NCSR, which include providing participating States and Territories with access to information relating to individuals about screening and diagnoses associated with designated cancers and advising participating States or Territories when action may need to be taken after a screening test for an individual. Where reporting of information to a State or Territory involves the disclosure of an individual's healthcare identifier, this will be authorised by the above sections in conjunction with section 26(3)(b) of the HI Act.

This presents a number of privacy positives. Designing the NCSR so that it has a reporting capability has positive flow-on effects: for example, it can inform policy and provide activity statements, benchmarking and forecasting.

However, identified reports provided to State and Territory Health Departments may involve an unnecessary disclosure of personal information. Further, even where reports are provided on a de-identified basis, those reports may contain values that are so low that it is possible to re-identify the individual.

To address these privacy risks, the disclosure of NCSR information to the States and Territories, and subsequent purposes for which the States and Territories may use the information, should be subject to a data access and release policy. In particular, this policy should set out permitted uses and secondary disclosures of NCSR information from the States and Territories to other entities, including State or Territory agencies or non-governmental organisations responsible for supporting that jurisdiction's involvement in the NCSP.

To address the risks outlined in this subsection, it is recommended that:

Recommendation 23 Further to Recommendation 22, the data access and release policy should address the following matters:

- the permitted uses and secondary disclosures of NCSR information provided to the States and Territories;
- the rules and procedures for when a State, Territory or other third party will receive identified or de-identified information. In particular, identified information should only be disclosed in circumstances where the receiving party requires identified information;
- where identified information is disclosed, it should be appropriately encrypted during transmission to the receiving party and while at rest with the receiving party; and
- where de-identified information is disclosed, it should not be reasonably possible for the information to be re-identified.

7.8 Sending invitations to screen

An important function of the NCSR is communicating with certain Australians to notify them where it may be appropriate for them to consider screening for bowel or cervical cancer. This involves a number of processes including commencing with identifying the cohort of eligible Australians who should receive screening invitation letters and concluding with updating the NCSR with an individual's screening results. These processes are, for the bowel cancer screening pathway, set out in the information flows at section 5.5.

As the bowel cancer screening pathway involves a number of collections, uses and disclosures of personal information, there are a number of privacy implications. The current National Bowel Cancer Screening Program, operated by DHS on behalf of Health, involves a series of template letters (pre-invitation, invitation, positive and negative results). We understand that these letters will continue to be used for the NCSR, updated to reflect the change in the Department and program. As indicated in sections 6.2 and 6.5, these letters are broadly privacy positive as they play an important role in notifying individuals of the information being collected by the NCSR (APP 5) and any personal information disclosed in them is consistent with APP 6 (as it is for the primary purpose for which the information is collected or is authorised by the NCSR Act).

We note, however, that given that the NCSR will be using Medicare enrolment and claims data, individuals who have not previously been screened for cervical and/or bowel cancer may be contacted. Collecting a wider range of data and capturing women who have not

previously taken an HPV test and individuals who have not yet been screened for bowel cancer, expands the number of individuals who are tested, which will hopefully lead to an increase in the early detection of cancer. However, this can create some privacy risks as there may be some cultural or other sensitivities around inviting women to have an HPV test who have not requested one. Women may not want to receive, or feel comfortable receiving, such information. Similarly, individuals may not want to be contacted regarding bowel cancer and receive a bowel screening test kit.

To address the risks outlined in this subsection, it is recommended that:

Recommendation 24 That it be possible for individuals to self-select preferred methods of correspondence for information from the NCSR and that this is effectively communicated to individuals.

For completeness, we note that individuals can also choose to opt out of the NBCSP entirely, which mitigates the privacy risks associated with sending screening invitations. The privacy implications of the opt out provisions in the NCSR Act are considered in further detail in section 7.9 below.

7.9 Opt out provisions in the NCSR Act

The NCSR Act sets out provisions allowing individuals to opt out of participation in the NCSR at any time. In general terms, opting out:

- means that an individual will receive no further invitations to screen (or test kits or advice that they should undertake particular action post-screening) unless they opt back on;[16] and
- allows, if desired, an individual to request that their information, which was mandatorily provided to the Commonwealth Chief Medical Officer in accordance with clause 13 of the NCSR Act, not be included in the NCSR;[17] but
- does not mean that an individual can request the NCSR to delete information about them which the NCSR already holds. [18] However, we understand that where a person opts out, the NCSR will hide that person's screening history so that no person other than Telstra Health (or Health) can view that person's information. In this regard, we also note that a person can also request that a pseudonym be used in connection with their record in the NCSR (see section 6. 3 which considers APP 2).

Individuals will also be able to request deferrals or suspensions of screening.

Two key issues relating to the opt out provisions in the NCSR Act are how the opt out (or screening deferral) mechanism will be implemented in practice and how individuals will be made aware of their rights to opt out. These issues are interrelated and addressed together below.

Individuals should be made aware of their right to opt out or defer screening in a number of ways. First, for the bowel screening program, the pre-invitation and invitation letters sent to eligible participants in the screening pathways should make clear that individuals have the right to opt out of participation or defer screening at any stage of the screening program and should clearly state that a person may opt out by phone, email, online at the NCSR website or via a paper form. Similarly, for those people invited to the cervical screening program, the right to opt out of participation in the screening program or defer screening should be clearly and prominently set out in the invitation communication. Where the NCSR receives notification that a person has opted out in one of these ways, it should consider confirming the participant's intention to opt out via a phone call (seeking the reasons for the

[16] See clause 14(1)(b) of the NCSR Act.
[17] See clause 14(1)(c) of the NCSR Act.
[18] We understand this policy position was taken as retrospective deletion of NCSR data impacts upon other considerations (for example, the use of NCSR data for research purposes).

opt out, optionally provided) and/or with a letter confirming to the individual that they have opted out and will receive no further communications from the NCSR unless they opt back on. Where an individual has deferred screening, the NCSR should confirm with the person in writing the date to which the screening has been deferred.

Secondly, we understand that healthcare providers which are registered with the NCSR will have the ability to opt out their patients directly through the NCSR portal or software. Healthcare providers should receive training to ensure they can communicate to their patients the purposes of the NCSR, what benefits and privacy impacts the NCSR might have for the individual, and the right to and implications of opting out (including the right not to have mandatorily reported-information included in the NCSR). This is particularly relevant for the cervical screening program where an eligible person attending their healthcare provider for an HPV test may elect to participate in the cervical screening program based on a recommendation from their healthcare provider without receiving an invitation.

Thirdly, the opt out rights and processes should be clearly set out in the NCSR privacy policy.

Recommendation 25 Screening letters sent to individuals should clearly communicate an individual's opt out and deferral rights and how they can elect to opt out of the screening pathway. With respect to the NCSP, this will allow women to choose to opt- out of the NCSR so they do not receive invitations, opt out of receiving certain information or correspondence, indicate that they need to defer their screening for a defined period, request that their information is not disclosed for certain purposes or request that their information is kept anonymous.

Recommendation 26 Healthcare providers should receive basic training relating to the advantages and disadvantages of opting out of the NCSR so they can communicate these to their patients to make informed decisions about whether they wish to opt out.

Recommendation 27 The NCSR privacy policy should clearly and prominently set out a participant's opt out rights and how to exercise them.

7.10 Privacy implications of mandatory reporting under the NCSR Act

We have been asked to consider specifically the privacy implications of mandatory reporting under the NCSR Act.

Clause 13 of the NCSR Act provides that certain individual healthcare providers for certain types of screening tests or diagnoses must notify the Commonwealth Chief Medical Officer within a certain time of particular information relating to the screening test or diagnosis. The individual healthcare providers and the types of information to be reported will be prescribed by rules made under the NCSR Act. A breach of this provision by an individual healthcare provider carries a civil penalty.

Legislative provisions of this kind subordinate an individual's privacy rights under the Privacy Act and the APPs to other purposes. This is appropriate in certain circumstances, including where there is a policy decision about the relative importance of different matters: in this case, the NCSR Act prioritises an individual's health over an individual's privacy.

The privacy implications of clause 13 cannot be fully determined at the time of this PIA as the rules prescribing the individual healthcare providers who must report and the information they must disclose have not yet been drafted. However, there are a number of factors mitigating the privacy impacts on individuals imposed by clause 13, including that, as we understand:

- clause 14(1)(c) of the NCSR Act will allow a person to request that their information, which was notified to the Commonwealth Chief Medical Officer in accordance with clause 13, not be included in the NCSR;
- mandatory reporting will likely only apply (at least initially) to cervical cancer screening information and diagnoses, and not bowel cancer screening; and
- mandatory reporting will apply only in respect of individuals residing in participating States or Territories. This means that healthcare providers in jurisdictions that are not participating may still be required to notify the Commonwealth Chief Medical Officer if the person they have provided services to resides in a jurisdiction that is participating.

In this regard, our view is that the privacy impacts on individuals imposed by mandatory reporting under the NCSR Act are appropriately mitigated to the extent possible without compromising the policy objective of collecting particular health information in connection with cancer screening and diagnoses.

7.11 Privacy implications of using ATSI / CALD status information

One of the NCSR's functions is to identify and engage individuals in sections of the community which under screen (that is, individuals in populations which do not screen as often as other sections of the community). Identifying individuals in under-screening populations involves considering a number of demographic details, including, amongst others, ATSI / CALD status information which the NCSR may collect from Medicare data.

Whilst the collection and use of ATSI / CALD status information is authorised under the NCSR Act and does not appear to raise any novel privacy risks (when compared with using other demographic information to identify potentially eligible persons), we understand that there may be sensitivities regarding how such information regarding status is shared, particularly in circumstances where the information is collected from Medicare.

In light of this, we recommend that the communication strategy mentioned in Recommendation 3 also include strategies for sensitive communication in relation to collection of information regarding ATSI and CALD status. It may be helpful for the Department to engage a consultant to provide advice to the Department on those issues.

Recommendation 28 Health should consider appointing an indigenous consultant (or other person with relevant expertise) to ensure that the purposes for which the NCSR collects and uses ATSI / CALD status information are communicated with appropriate sensitivity.

7.12 Privacy implications of different means of communication

We understand that the NCSR may, from time to time, contact participants to ensure that their details in the NCSR are correct and to notify or remind participants of upcoming screenings. Such communication may take the form of an SMS, email or letter and are likely to contain personal information and possibly information about the person's previous screening history (namely, clinical outcomes).

As indicated in section 5, these disclosures of personal information from the NCSR are permitted under APP 6 in accordance with section 17(3) of the NCSR Act. Further, for the purposes of APP 6, the means of communication (SMS, email or letter) does not matter.

However, from a privacy risk perspective, each means of communication has its own inherent risks and none is entirely secure (for example, letters can be taken out of post boxes, mobile phones can be lost and emails can be hacked). In each of these situations, not only might the participant have his or her personal information revealed to an unauthorised third party, but the individual may not receive or be aware of the communication in the first place, such that they would not know that they should notify the NCSR of the missing correspondence.

In practice, we do not think the risk of unauthorised access can be fully mitigated. However, to ensure that correspondence reaches the participant in an appropriate way, the correspondence sent to a participant should be of the type(s) self-selected by the participant in line with Recommendation 30. Further, Health should consider making a copy of the correspondence available to the participant upon logging into the NCSR portal.

Recommendation 29 Correspondence sent to participants to notify or remind them of screening should be of the type(s) self-selected by the participant in line with Recommendation 24. Health should consider making a copy of the correspondence available to the participant upon logging into the NCSR portal.

Schedule 1 — Glossary

Glossary of Terms

APP	Australian Privacy Principle
APP Guidelines	*APP Guidelines* (Office of the Australian Information Commissioner, Version 1. 1, February 2014)
ATSI	*Aboriginal and Torres Strait Islander*
C&T Act	*National Cancer Screening Register (Consequential and Transitional Provisions) Act 2016* (Cth)
CALD	*culturally and linguistically diverse*
DHS	Department of Human Services
Health	Department of Health
HI Act	*Healthcare Identifiers Act 2010* (Cth)
HI	"healthcare identifier" within the meaning of the Healthcare Identifiers Act
HI Service	Healthcare Identifiers Service
ISM	The *Australian Government Information Security Manual*
My Health Records Act	*My Health Records Act 2012* (Cth)
NBCSP	National Bowel Cancer Screening Program
NCSP	National Cervical Screening Program
NCSR	National Cancer Screening Register
NCSR Act	*National Cancer Screening Register Act 2016* (Cth)
NCSR Acts	Collectively, the NCSR Act and C&T Act
NHPVR	National Human Papillomavirus Vaccination Register
Privacy Act	*Privacy Act 1988* (Cth)
Telstra Health	A standalone business unit of Telstra Corporation and contracted service provider for the operation and management of the NCSR in accordance with a services agreement with Health

Schedule 2 — Definitions

collects: an entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

discloses: an entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.

uses: an entity uses personal information when it handles and manages that information within the entity's effective control.

Medicare claim data includes:

- Healthcare Identifier,
- Claim Code,
- Specified Claim code item (the procedure which was undertaken)
- Provider detail,
- date service provided,
- Status of the claim,
- Claim Type (DVA or Medicare).

Medicare enrolment data includes:

- Medicare Number,
- Medicare PIN,
- Healthcare Identifier,
- Name,
- Address,
- DOB,
- Sex,
- Medicare Entitlement Type,
- CALD,
- ATSI,
- Record status,
- Number status,
- Medicare IRN,
- DVA number.

personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

sensitive information means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.