Australian Government
Office of the Australian Information Commissioner

Our reference: D2016/007138

Ms Jeanette Radcliffe
Secretary
Senate Standing Committees on Community Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

Via email: community.affairs.sen@aph.gov.au

Dear Ms Radcliffe

Submission on the National Cancer Screening Register Bill 2016

As the Australian Privacy Commissioner and Acting Australian Information Commissioner, I welcome the opportunity to provide the Senate Community Affairs Legislation Committee with this submission on the *National Cancer Screening Register Bill 2016* (the NCSR Bill).

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth statutory agency. The OAIC was established by the Australian Parliament to bring together three functions:

- privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Privacy Act), and other Acts)
- freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (FOI Act)), and
- information management functions (as set out in the *Information Commissioner Act 2010*).

The integration of these three interrelated functions into one agency has made the OAIC well placed to strike an appropriate balance between promoting the right to privacy and broader information policy goals. This includes ensuring that public sector data is made available to the community, provided there are appropriate safeguards in place.

In the digital age, more information is being collected than ever before. While technology is allowing organisations to use and analyse data in innovative ways, often to great social and economic benefit, privacy must be integral to the equation. 'Getting privacy right' will help to engender public trust and gives individuals choice and confidence that their privacy rights will be respected.

The Privacy Act contains thirteen Australian Privacy Principles (APPs) which outline how Australian Government agencies, private sector organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information. Health information is regarded as one of the most sensitive types of personal information. For this reason, the Privacy Act provides extra protections around its handling. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual.

My comments below relate to the handling of sensitive health information for the purposes of the National Cancer Screening Register (the Register).

The use of information in the Register for medical and health research purposes

The Privacy Act recognises the strong public interest in the conduct of medical and health research, and provides a framework to facilitate data access arrangements for these research purposes.

The framework includes:

- the Guidelines under Section 95 of the Privacy Act (s 95 Guidelines), which apply to agencies and provide an exception for acts that would otherwise breach the APPs where those acts are done in the course of medical research (and in accordance with the s 95 Guidelines)
- the Guidelines approved under Section 95A of the Privacy Act (s 95A Guidelines) which apply to private sector organisations, and deal with the disclosure of health information that is necessary for the secondary purpose of research relevant to public health or public safety.

These guidelines, issued by the National Health and Medical Research Council and approved by the Information Commissioner, provide a framework for Human Research Ethics Committees to approve researchers' proposals to use identified information without consent. This framework acknowledges both the need to protect health information from unexpected uses beyond individual healthcare, and the important role of research in advancing public health.

In this context, the NCSR Bill, as currently drafted, may have the impact of bypassing this research framework which is established by the Privacy Act. This is because, the purposes of the Register, which are set out in clause 12 include 'research relating to healthcare, screening or a designated cancer.' Clause 17 then permits 'certain persons' to collect, disclose and use 'protected information' (which includes personal information) for the purposes of the Register. As such, clause 12 together with clause 17, appear to authorise the use of personal information in the Register for research purposes without specifically requiring compliance with the s 95 Guidelines or s 95A Guidelines.

Having said that, I acknowledge that the Explanatory Memorandum to the NCSR Bill does state that where research requires identifiable information from the Register and it is impracticable to obtain individuals' consent, researchers will be required to comply with the guidelines under sections 95, 95A or 95AA of the Privacy Act. However, I recommend that this requirement be made explicit in the NCSR Bill in order to provide a clear and unambiguous information handling requirement.

Medicare claims information

Clause 11 of the NCSR Bill sets out the contents of the Register, which includes 'claims information which may indicate whether or not the individual has undergone or should undergo screening.' However, the Explanatory Memorandum states that, 'Medicare claims information of individuals who are within the coverage of the Register will be collected as part of the establishment and ongoing operation of the Register'. From this statement, it is unclear whether all Medicare claims information associated with an individual will be collected or whether only the claims information relevant to bowel and cervical cancer screening will be collected.

Considering the sensitivity of Medicare claims information, only the specific Medicare claims information necessary for the purposes of the Register should be collected. This limitation should be reflected in the NCSR Bill as well as in and the Explanatory Memorandum.

Purposes of the Register

Clause 12 sets out the various purposes of the Register which include 'anything incidental to any of the above paragraphs.' Clause 12 is particularly important when read in conjunction with parts of clause 17(3) which links authorised uses of protected information to the 'purposes of the register'. The relationship between the two clauses means that clause 12 effectively specifies how protected information in the Register may be handled.

Authorising the information to be handled for any purpose that is 'incidental' to the other purposes may be too broad and presents a risk that information may be used or disclosed for more expansive purposes than initially intended. Therefore, I recommend that the wording of the provision be narrowed to only allow uses or disclosures that are *directly related* to the purposes of the Register. This would also reflect the terminology of the APPs which limit secondary uses and disclosures of sensitive information (such as health information) to purposes directly related to the primary purpose.

Communications strategy relating to participation in the Register

The NCSR Bill explains that individuals will be able to request that information notified by healthcare providers relating to the individual not be included in the Register. The Explanatory Memorandum provides further detail on how individuals can 'opt-off' the Register by explaining that individuals can do so by using the Register self-service facility, contacting the Register operator, or during a consultation with their healthcare provider.

Considering the importance of providing individuals with the opportunity to decide whether or not they want their health information uploaded to the Register, I recommend that a broad communications strategy be implemented to ensure the Australian public are aware of the purposes of the Register and their 'opt-off' rights.

I also recommend that any material that includes information about an individual's choice to participate in the Register (or 'opting-off', as this process is referred to in the Explanatory Memorandum) should be clear and prominently presented. A link to the Register's privacy policy should be included in any information booklets, letters or other communications sent to individuals so that individuals can seek out further details on the Register and the handling of their personal information should they wish to. Material should also be accessible, written in plain English and take into account the needs of consumers with special needs, individuals from a non-English speaking background and disadvantaged or vulnerable individuals.

I would also like to make an observation about the language used to describe the process individuals can use to remove themselves from the Register. The My Health Record system uses the terminology 'opt-out', where relevant. Whilst I appreciate that it is the correct use of language to opt-off a register and opt-out of a system, I see value in describing the concept of withdrawing participation in both the My Health Record system and the Register in similar terms. This will ensure that consistent language is used to explain that individuals have a choice about whether or not to include their personal information in the Register or the My Health Record system.

Other considerations

I note there has been discussion related to Telstra Health being the operator of the Register. By way of informing the Committee, organisations such as Telstra are subject to the Privacy Act. I also note that section 95B of the Privacy Act requires Australian government agencies entering into a contract with a contracted service provider (CSP)[1] to take contractual measures to ensure that the CSP (and subsequent sub-contractors) do not do an act, or engage in a practice that would breach an APP if the act or practice had been undertaken by the agency. Agencies will generally need to include specific or practical provisions in their contracts and where particular information handling practices are required to comply with an APP, these should also be addressed in the contract.

Consideration could also be given to whether additional requirements to the Privacy Act should be applied since the collection and retention of large amounts of sensitive health information in a centralised database can pose a number of security and privacy risks, particularly if the database can be accessed from many access points. The Register operator's security requirements could be strengthened by requiring the operator to report data breaches and specifying requirements around the handling of data breaches in a manner consistent with the data breach requirements in section 75 of the *My Health Records Act 2012* (My Health Records Act).

---

[1] Section 6(1) of the Privacy Act defines a contracted service provider (CSP), for a government contract, as an organisation that is or was a party to a government contract and that is or was responsible for the provision of services to an agency (or a State or Territory authority) under the government contract; or a subcontractor for the government contract. Where a small business is a party to a government contract and is responsible for the provision of services to an agency under the contract, the small business will be an organisation (s 6D(4)) and therefore covered by the APPs in relation to the activities it is required to perform under contract. However, an organisation does not include a registered political party, State or Territory authority or a prescribed instrumentality of a State (s 6C(1)). As these entities are not organisations, they are not CSPs for the purposes of the Privacy Act.

Consistency with the My Health Records Act requirements is particularly important if the Register will link to the My Health Record system and if information in the Register will be made available through that system.

Further information

Should the Committee require any further information, please contact Ms Melanie Drayton, Director, Regulation and Strategy Branch

Yours sincerely

Timothy Pilgrim PSM
Australian Privacy Commissioner
Acting Australian Information Commissioner

23 September 2016