



ACT
Government

Birth of a Child Pilot Project

Privacy Impact Assessment (PIA) Summary

ACT Government

2024 Privacy Impact Assessment Summary

Introduction

There are over 300,000 births registered in Australia each year, with over 6,000 births registered in the Australian Capital Territory (ACT) . Currently new parents need to complete various forms and have a number of interactions with different government agencies to register their child's birth, and enrol in a range of government services.

The Birth of a Child (BoC) Project is an Australian Data and Digital Council (ADDC) initiative which aims to provide parents of newborn children with a seamless service for:

- (i) registration of the child's birth in their state or territory;
- (ii) Medicare enrolment; and
- (iii) birth verification to access other government payments and services.

The ACT Government, led by the Chief Minister, Treasury and Economic Development Directorate (CMTEDD), is working in partnership with Services Australia on a multi-year BoC Pilot Project to develop and implement systems and processes that streamline:

- (i) notification of births by participating ACT Hospitals (currently limited to the Centenary Hospital for Women and Children, and North Canberra Hospital);
- (ii) registration of the birth of a Child of a participating Birth Mother with the ACT Registry of Births, Deaths and Marriages;
- (iii) applications for birth certificates;
- (iv) enrolment of the Child in Medicare and associated services (including the Australian Immunisation Register and My Health Record); and
- (v) applications for Centrelink payments such as family tax benefit and paid parental leave.

A privacy impact assessment (PIA) was commissioned by CMTEDD to identify and assess privacy impacts and compliance risks for the ACT Government in relation to the implementation of the BoC Pilot Project, and ensure that such issues are appropriately mitigated and managed.

Overall Findings

The PIA found that:

- (i) the largely consent-based approach is a privacy positive way of dealing with personal information, by giving individuals knowledge, choice and control over how their personal information is handled; and the Registrar General (who we are instructed is a separate ACT 'public sector agency'); and
- (ii) the BoC Pilot Project presents a medium level of privacy risk that can be mitigated by implementing the recommendations made in the PIA report.

Summary of Recommendations

Recommendations made in this PIA to eliminate, reduce or manage negative privacy impacts and compliance risks are summarised below.

These recommendations seek to:

- (i) achieve an appropriate balance between the Project's objectives, and the interests of individuals whose privacy will be impacted;
- (ii) where appropriate, maximise opportunities for privacy protection and incorporating a 'privacy by design' approach in relation to the project.

The ACT Government has accepted all the recommendations and have implemented a series of comprehensive measures to address the concerns raised in the PIA.

Recommendation 1

If there are any material changes to the information flows described in Schedule 1, including in relation to the nature and scope of the data, or any Project or use case expansion, we recommend that CMTEDD undertake:

- a privacy threshold assessment; and
- if required, further assessment of privacy impacts and compliance risks (which could be in the form of a supplementary PIA).

Recommendation 2

We recommend that CMTEDD (in cooperation with Services Australia) undertake regular reviews of the BoC Pilot Project, including related systems and processes, to ensure:

- workflow processes and system functionalities are operating as intended;
- any known, new or unanticipated privacy issues are appropriately managed; and
- ongoing compliance with the Territory Privacy Principles (**TPPs**) and Health Privacy Principles (**HPPs**), including to identify potential opportunities to refine data handling practices and maximise privacy protections.

Such reviews should be:

- undertaken at regular intervals particularly during the first 12 months, and periodically thereafter as appropriate; and
- informed by:
 - any feedback or privacy complaints from Birth Parents, Other Parents or any other individuals or participants involved in the Project; and
 - any identified data quality issues.

Recommendation 3

We recommend that CMTEDD ensure the contractual arrangements with the Promadis system provider impose contractual obligations on that provider (including the provider's personnel and subcontractors) to:

- comply with the TPPs (or the Commonwealth Privacy Act as a corresponding privacy law);
- only access and deal with personal information and personal health information for the purposes of fulfilling its obligations under the contract;
- ensure personal information and personal health information is not disclosed, transferred, stored or accessed outside Australia (including back-ups and disaster recovery storage) without the prior written approval of CMTEDD / ACT Government;
- take all reasonable measures (including compliance with relevant ACT and Australian Government ICT security standards and policies) to ensure personal information and personal health information accessed or held by the contracted service provider is protected against:
 - misuse, interference and loss;
 - unauthorised access, modification or disclosure; and
 - cyber risks;
- notify CMTEDD of:
 - any actual or suspected privacy or data breach;
 - a breach of its contractual obligations relating to privacy and data security; and
 - the receipt of a request for access to or disclosure of personal information or personal health information that is required by law or a court/tribunal order;

The contractual arrangements should also:

- ensure that CMTEDD / ACT Government remains in effective control of the data; and
- provide CMTEDD with a right to audit the contracted service provider's compliance with its contractual obligations.

Recommendation 4

We recommend that CMTEDD ensure it engages in proactive contract management in relation to the delivery of the Promadis system by the contracted service provider, including through:

- processes and procedures that ensure there is regular monitoring and review of compliance with contractual obligations, from contract commencement to completion/termination; and
- conducting regular audits of the Promadis system to ensure the handling of personal information and personal health information by the contracted service provider (and any subcontractors) is, having regard to the volume, nature and sensitivity of the relevant information, sufficiently secure and satisfies all contractual obligations in relation to privacy and data security.

Recommendation 5

To ensure there are clear privacy and data governance arrangements in place between Services Australia and ACT Government for the BoC Pilot Project, and noting that the draft Letter of Agreement provided for this PIA is specific to the Registration of Birth (**RoB**) service, we recommend ensuring that:

- documented arrangements are implemented for all relevant Project components (i.e. the Proof of Birth (**PoB**) data transfer and use cases, and Notification of Birth (**NoB**) service, in addition to the Letter of Agreement for the RoB service); and
- there is alignment between those arrangements, having regard to the cross over purposes for which personal information included in various datasets may be collected, used and disclosed.

We also recommend updating the draft Letter of Agreement for the RoB service to:

- refer to CMTEDD (rather than Access Canberra) as the party representing the ACT Government;
- recognise and address the roles and responsibilities of, and obligations with respect to, the Registrar-General, Canberra Health Services and ACT Health (and consider whether the Registrar-General and Canberra Health Services should be included as additional named parties representing ACT Government);
- specify or clearly describe the personal information and data involved in the Project, and to which the Agreement (including obligations relating to personal information and data) applies;
- define 'Privacy Law' in relation to the ACT Government with reference to the *Information Privacy Act 2014* (ACT) and *Health Records (Privacy and Access) Act 1997* (ACT);
- set out the purposes for which personal information will be provided by one party to the other (or in the case of the ACT Government, the relevant entity), and for which each party may collect, use and disclose that information; and
- address:
 - the data quality obligations of Services Australia;
 - protocols between the parties for resolving any data quality issues;
 - obligations and processes relating to privacy complaints; and
 - what is to be done with personal information if the Project or arrangements between the parties end (e.g. deletion/destruction or transfer to a party).

Recommendation 6

We recommend updating the CMTEDD Information Privacy Policy to ensure it addresses the personal information handling practices of BDM (i.e. both the Registrar-General, and CMTEDD staff assisting the Registrar-General) in the context of the Registrar-General's birth registration functions and activities. This should include information relating to disclosures to Australian Government agencies (i.e. Services Australia).

Recommendation 7

In relation to the myGov RoB tasks for the Birth Mother and Other Parent, we recommend that:

- the Indigenous status data field makes clear that provision of Indigenous status information is voluntary, and an explanation is provided about the purpose for which that information will be provided to and used by BDM;
- the consent check box ('I agree to share this information with Access Canberra') and the hyperlinked information ('How Access Canberra will use your information') make clear that information will be shared with, and collected, used and disclosed by, both Access Canberra (CMTEDD) and the Registrar-General; and
- the abovementioned hyperlinked information ('How Access Canberra will use your information') also address:
 - the fact that the information provided by the parent (other than Indigenous status information) to register their Child's birth is required under the BDMR Act and Regulation;
 - that information about the Child and parents will be used for the purposes of enabling a parent to apply for, and for BDM to issue, a birth certificate (including facilitating access to and pre-populating the SmartForm);
 - the purposes for which Indigenous status information will be collected and disclosed by the BDM (i.e. provision of that voluntary information to the Australian Bureau of Statistics, for statistical purposes); and
 - disclosures by BDM to the Hospital and other parent to process a birth registration application (including to verify information provided by the parents or Hospital),

and include a link to the CMTEDD Information Privacy Policy.

Recommendation 8

We recommend that CMTEDD ensure a privacy collection notice is included in the 'Order Birth Certificate' SmartForm, which addresses the relevant matters set out in TPP 5.2.

We also recommend that the SmartForm obtain the parent's consent to use and disclose personal information relating to themselves and their Child to issue a birth certificate, including information provided in their birth registration application.

Recommendation 9

We recommend that CMTEDD and Services Australia together ensure that:

- prior to the commencement of the Newborn Enrolment Trial, all relevant ICT systems and components involved in the BoC Pilot Project including:
 - Promadis and the APIs, and any changes to that system as part of the project (e.g. birth certificate URL notification sent to parents, and the SmartForm); and
 - the integration of Digital Health Records and Promadis with Services Australia systems,

have been subject to cyber security assessments (including penetration testing), as assessed against applicable Australian Government and ACT Government security standards; and

- regular cyber security audits and testing is undertaken thereafter.

Recommendation 10

We recommend ensuring that:

- ACT Health has data breach and cyber incident response plans in relation to Digital Health Records; and
- there are also data breach and cyber incident response plans in place for BDM (Registrar General and CMTEDD) that cover Promadis and the SmartForm,

and that the scope of those plans contemplates potential data and cyber risks that may arise from the integration of the relevant ACT systems with Services Australia systems.

Recommendation 11

We recommend that CMTEDD ensure there is a data retention and destruction plan in place, to ensure that SmartForms and related data is only retained for such minimum periods as is:

- required by Access Canberra and BDM for the purposes of their functions and activities; or
- is otherwise required under the Territory Records Act in relation to the retention of territory records.