# Citizen Space –Privacy Impact Assessment

14th July 2022

# Part 1: Overview of PIA

## What is a Privacy Impact Assessment (PIA)?

A PIA is a systematic assessment that identifies the impact a project instituted by a Commonwealth agency might have or is having on the privacy of individuals.

The Australian Government Agencies Privacy Code requires that a Commonwealth agency (which includes the NHMRC) undertake a PIA for 'all high privacy risk' projects or initiatives that involve new or changed ways of handling information that may include personal information.

In a practical sense, the process of assessing a project's potential privacy impacts involves analysing the project or process and evaluating the flow of any personal information (including collection, use and disclosure) against the 13 Australian Privacy Principles (APPs) set out in Schedule 1 to the Privacy Act.

Frequently, undertaking a PIA becomes an iterative process in which changes to privacy procedures may be made by the agency in response to issues identified during the review process itself.

In most cases, the final output of a PIA would include notes setting out an analysis of the project against each of the APPs, and a set of recommendations for managing, minimizing or eliminating any processes that the reviewer considers may still require attention in order to meet the requirements of the APPs and the Privacy Act more generally.

## Description of the Citizen Space project and interested parties

The aim of the Citizen Space project is to create a unified platform for conducting NHMRC's consultations (referred to generically in this PIA from time to time as surveys) including the receipt, review, redaction, analysis and publication of responses. This project is a key step required to decommission several websites running on NHMRC's servers as part of a broader project to move all NHMRC's websites to the cloud as part of the Australian Government's Secure Cloud Strategy. A secondary aim of the project is to empower business areas to take greater control of putting together their own consultations as part of a move towards more distributed publishing.

The platform NHMRC is looking to deploy is Citizen Space: a cloud-based solution originally developed as a joint initiative with the UK government, and now used by a range of Australian Commonwealth government departments – including the Department of Health.

Citizen Space is proposed to be used for both public and private consultations. In the case of the former the consultation is visible during all its various milestones on the Citizen Space platform. In the case of the latter there is no visibility whatsoever and the consultation is private. In both scenarios, often a pool of potential participants can be invited to take part via email.

NHMRC recognise consultations as a critical part of its work.

Every time the agency runs a consultation it acknowledges the power and expertise of a diverse community of stakeholders, health professionals, administrators, and consumers to help NHMRC achieve its mission and mandate to:

- recognise opportunities
- identify gaps
- tackle and resolve complex issues
- and inform and shape decision making.

This project scope includes the initial rollout of Citizen Space, associated policy and Standard Operating Procedures (SOPs), and the ongoing maintenance of the platform.

Citizen Space would replace the previous ad-hoc approach to conducting consultations spread across the following:

- www.nhmrc.gov.au
- consultations.nhmrc.gov.au
- online.nhmrc.gov.au (*recently decommissioned*)
- Survey Monkey

This PIA is being conducted before the rollout of Citizen Space to allow it to shape the design of the project. Decisions surrounding the design of the project need to be finalised by the end of August 2022.

## Scope of this privacy impact assessment

The scope of this PIA is the rollout and management of Citizen Space. It considers the following:

- Personal information collected while conducting consultations, system administration, security, and associated information flows.
- The handling of personal information collected in the creation of administrator accounts used to conduct consultations and manage the system.
- How the agency can encourage limiting the personal information collected while conducting consultations and improve privacy outcomes compared to current processes.

## Review Methodology

Primary work on this PIA was undertaken internally by NHMRC Web Services who undertook extensive stakeholder consultation in the first stages of this PIA. Proximity Legal Services then reviewed and settled this PIA in consultation with them.

## Stakeholder identification and consultation

This project has a wide range of both internal and external stakeholders:

Stakeholders within NHMRC:

- NHMRC business areas that run consultations
- NHMRC staff who participate in internal consultations
- Web Services
- Business Services
- ITSA
- Infrastructure Project Manager
- Information Management
- Privacy officer
- Legal Services

External stakeholders include everyone who participates in consultations run by NHMRC including:

- Researchers
- Health professionals
- Administrators
- Members of the public
- Federal, State and Territory agencies
- Other interested parties

Web Services consulted with the following stakeholders:

1. NHMRC Business Services on developing a System Information Management Plan and Privacy Impact Assessment for Citizen Space.

   **Outcomes:** The development of all required NHMRC Information Data and Impact Assessments including this PIA, a Threat Risk Assessment (TRA), a System Information Management Plan (SIMP), and an Information Classification Assessment.

2. NHMRC IT Management & Strategy (ITMS) developed a TRA for Citizen Space and was consulted on the development of our System and Security SOP, and an Incident Response Plan (IRP)

   **Outcomes:** Various technical decisions to help manage security risks related to the project including:

   - A decision to ban all file uploads on consultations
   - Development of a System and Security SOP and an Admin SOP
   - Standards for password policies

3. NHMRC ITMS on project requirements and suitability of Citizen Space.

   **Outcome:** Development of a project brief outlining the requirements that need to be met in any new consultation system.

4. A pilot group was established to trial Citizen Space consisting of NHMRC staff from across the agency who are involved in developing consultations. A meeting was held with this pilot group to discuss privacy issues raised while conducting this PIA along with written questions surrounding what types of personal information are collected, when consultations are run, what this information is used for, how it is maintained, and how it is kept up to date.

   **Outcomes:**

- It was identified that a range of personally identifiable information that has historically been collected does not always have a strong practical use, e.g., *city, town, post code, country, postal address* and as such does not need to be collected in most surveys.
- Agreed on a minimal set of (non-mandatory) personally Identifiable Information (PII) that can be collected by consultations run on Citizen Space (*name*, *email address*, and *contact phone number)* without the need for a custom collection notice. Where relevant to the research at hand, other PII including sensitive information may be collected if there is a genuine business case and an adequate collection notice is provided in accordance with APP 3.
- Staff are comfortable with the personal information required to set up user accounts except for the system asking for a personal phone number. The Citizen Space vendor advised this field does not need to be filled in and the system may change to remove this requirement in future.

6. The NHMRC legal team was consulted on the need for a privacy statement, and terms of use, along with an assessment of the vendor agreement for Citizen Space.

   **Outcomes:**

- The NHMRC Legal team advised that the wording of NHMRC's existing Privacy Statement would suffice both as a Privacy Statement and as Terms of Use.

- The NHMRC Legal team gave provisional agreement with the vendor contract noting it was a standard Commonwealth Off the Shelf Contract (COTS).

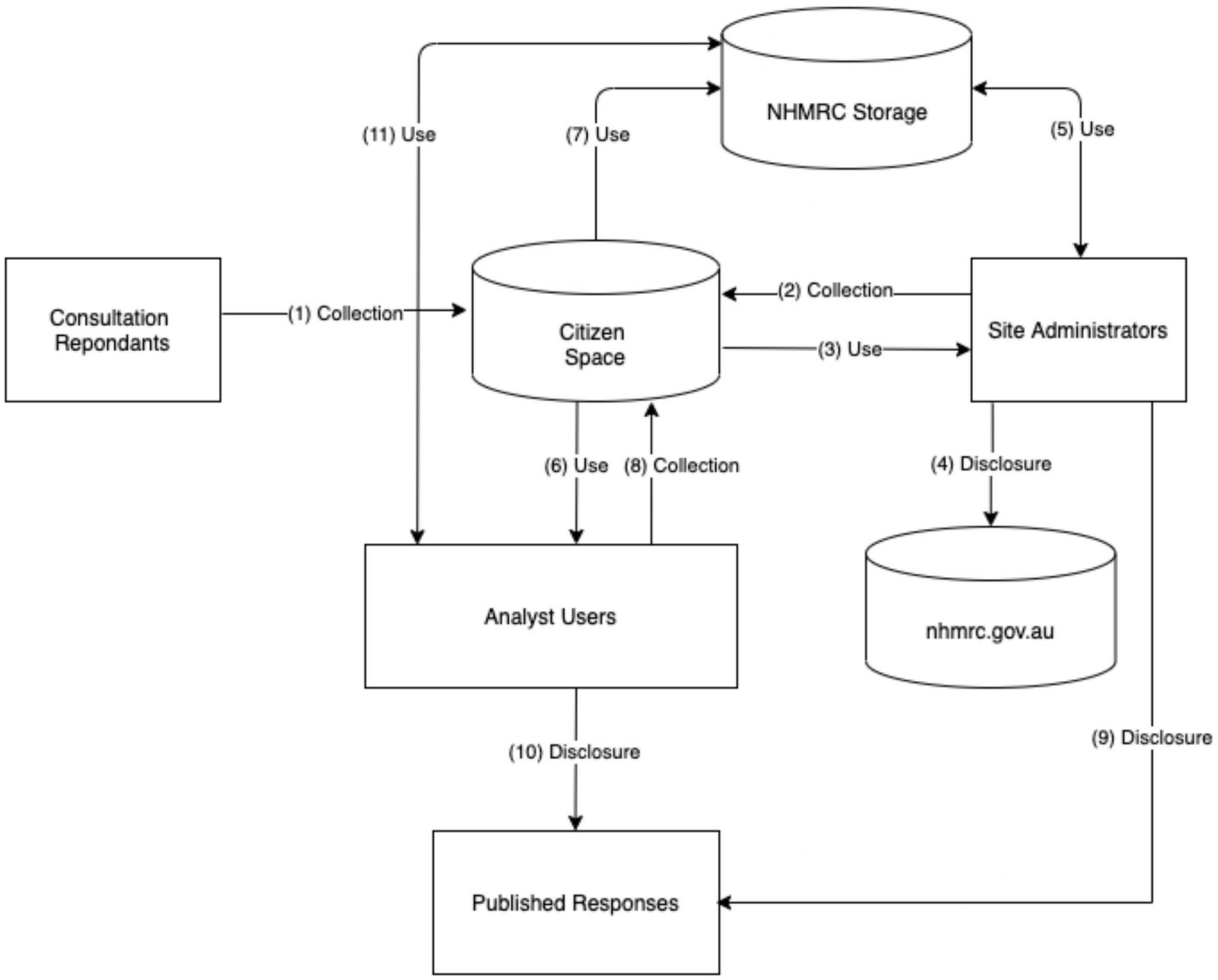
7. The NHMRC Privacy team were consulted on the development of this Privacy Impact Assessment and reviewed the final draft.

**Outcomes:**

- When finalised, this PIA will be published on NHMRC's website in accordance with s 15.1 of the *Australian Government Agencies Privacy Code*, which requires agencies to maintain a register of the PIAs they conduct and to publish that register on their website.
- Agreement that with this minimal set of data that the wording of the existing Privacy Statement would be sufficient (as at 6. Outcome 1 above), but that for where more sensitive information is being solicited that the Privacy team and Legal teams are consulted on a more comprehensive collection notice.

## Map information flows

The following diagram maps the information flows that will occur with Citizen Space. The accompanying notes below show how information will be collected, used, and disclosed, and how it will be held/stored and protected, and who will have access to it.




(1) A limited set of PII such as *name, email address, contact phone number* and in rare cases additional PII possibly including sensitive information, is collected from users as part of consultations run on Citizen Space and stored on the Citizen Space platform. Access is protected by two factor authentication and only granted to Analyst users and associated administrators.

(2), (8) Email addresses and usernames are collected from users for the purpose of creating user accounts. This information is only accessible to the users themselves and site administrators who create the accounts and assign role permissions.

(3), (6) Site administrators and Analyst users, use consultation responses to analyse data, produce reports, and redact responses before publishing. Analyst users are NHMRC staff or external contractors hired to analyse data.

(4) Reports on consultations are published on the main NHMRC website. These reports present the responses in summarised format that preserves the identity and privacy of individuals.

(5), (11) Site Administrators and NHMRC Analyst users store data related to consultations they are working on in protected areas inside the NHMRC network. The response data exported on NHMRC infrastructure will be stored as government records by NHMRC as required.

(7) Backups of Citizen Space data are made on the completion of consultations and stored in a protected area inside the NHMRC network for the purposes of disaster recovery and records management.

(9), (10) Redacted consultations are published. These may include PII such as name and title of respondents in cases where they have specifically consented to the information being published. The original versions of all responses are kept in the system as separate entries in the database and cannot be modified by anyone including site administrators.

The responses (with any accompanying personal information) will be collected directly by NHMRC through Citizen Space, without any third-party intervention.

## Summary of outcomes from consultation processes

- Redaction of consultations before publishing avoids inappropriate disclosure of private information.
- Analyst users/ (which are always either NHMRC staff or external contractors) will be restricted to accessing only data related to consultations they are assigned to.
- The provision of a Privacy Policy to consultation respondents outlining how any personal information they provide is managed.
- Business areas will gain a greater awareness of the issues surrounding the collection of personal information when conducting consultations. This awareness will be built and maintained through training, the System and Security SOP, the Admin SOP, and the consultation work undertaken in the development of this PIA.
- Providing personal information on consultations is generally optional and if provided respondents can choose whether this information is to be published or not.

**This PIA has identified a few negative privacy impacts which have been addressed (see Part 2 below):**

1. Data is stored with a third-party provider and NHMRC is dependent on the security of their systems to protect user data
2. Consultation respondents could provide unsolicited PII or sensitive information.
3. There may be a temptation for business areas to use information collected for a purpose other than the purpose for which it was provided.

## Recommendations

Because of the comprehensive consultation and review process undertaken by Web Services, the recommendations are activities that NHMRC will undertake on an ongoing basis as surveys are developed:

1. Because of the potential for unexpected privacy issues to arise in the form of any survey, we recommend that the collection notice developed for each survey be reviewed by the Privacy Officer before the survey is published.
2. Advise respondents that personal information provided in a survey response *may be stored* on a third-party service provider (which will be subject to privacy obligations under its contract).
3. If a survey seeks sensitive information from a respondent, it will specifically advise this in the collection notice and give respondents the option of not providing it.
4. Expand the APP4 note (regarding collection of unsolicited personal information) to cover both public and targeted consultation processes.

# Part 2: Analysis of Compliance with the APPs

## APP 1 — Open and transparent management of personal information

*APP entities must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.*

**Analysis**

The NHMRC has a Privacy Management Plan, the most recent version of which is dated 1 July 2021-22, which was developed using the guidance in the OAIC Privacy Management Framework.

The NHMRC's Privacy function sits within the Governance, Regulation and Secretariat Support Section in the Research Quality and Priorities Branch. It is responsible for ensuring that the agency complies with the *Privacy Act 1988*, by:

- ensuring the provision of privacy management training to staff
- assisting business areas to understand the practical application of the *Privacy Act 1988*
- coordinating a register of PIAs
- having responsibility for the Privacy Policy, the NHMRC Response plan for data breaches involving personal information and Privacy Management Plan
- assisting business areas to respond to privacy breaches, and
- managing the NHMRC's relationship with OAIC.

With the implementation of the OAIC's Australian Government Agencies Privacy Code on 1 July 2018, there was some re-arrangement of privacy functions, primarily as a result of the required appointment by the NHMRC of a Privacy Officer (APS) and a Privacy Champion (SES), the latter of whom is the Senior Responsible Person with prescribed responsibility for these functions.

We are satisfied that NHMRC has taken reasonable steps to implement practices, procedures, and systems to ensure this project's compliance with the APPs before adoption. These have included:

- Completing a Threat Risk Assessment of the project and adapting system configuration, policy and procedures based on the outcomes.
- Completing and publishing this PIA and using the analysis process to inform our policy, procedures, and training.
- The development of a System and Security SOP and Admin SOP designed to ensure compliance with the APPs
- Developing a system comprised of multiple layers of checks to ensure APPs are complied with. Compliance is ensured by a combination of system configuration, policy and procedures to ensure compliance, and an approval process for all consultations to ensure the policy and procedures are being complied with.

NHMRC's Privacy Policy sets out how an individual can contact the privacy officer to complain that the NHMRC may have breached any of the APPs with options to contact us via telephone, email, or written mail.

**APP Privacy Policy**

NHMRC has an up-to-date privacy policy that is freely available at https://www.nhmrc.gov.au/privacy. We are satisfied it covers all the matters listed in APP 1.4

In particular, with respect to the conduct of surveys, we noted the policy addressed this practice with the following references, which we found satisfactory in their current form.

Under the heading 'Collection of your personal information', there is an acknowledgement that personal information **may** be collected if an individual participates in a NHMRC targeted or public consultation or survey.

We note the policy also advises that NHMRC may also collect personal information from publicly available sources to enable it to *(inter alia)* contact stakeholders who may wish to participate in targeted or public consultation processes.

NHMRC's Privacy Policy will require the following changes:

- In the section headed 'Receipt of Unsolicited Personal Information', fourth line, replace 'submissions to public consultations' with 'submissions to public or targeted consultations or surveys'.
- In the section headed 'Submissions to NHMRC targeted or public consultations'**:** Insert words at the beginning to the effect 'Providing personal information in any consultation or survey response is usually optional'.
- In the section headed '**Disclosure of personal information to overseas recipients'**, add the following sub-section (or something similar):

  ***Disclosure of Personal Information in public or targeted consultations or surveys***
  *NHMRC undertakes public or targeted consultations and surveys in order to perform its functions. If an expert or consultant engaged to analyse or consider any survey or consultation data is based overseas, NHMRC will ordinarily adopt one of the following approaches:*

  *redact any personal information that may be contained in the response before forwarding the data overseas; or*

  *advise in the collection notice attached to the survey or consultation that any personal information provided in the response will only be forwarded overseas if the respondent expressly gives consent to the information being forwarded overseas.*

- In the section headed '**Submissions to NHMRC targeted or public consultations':** Insert words at the beginning to the effect 'Providing personal information in any consultation or survey response is generally optional'.

**Procedures and systems in place for handling privacy inquiries and complaints**

Procedures to make a privacy complaint to NHMRC are our outlined in its Privacy Policy under the 'Making a privacy complaint if you believe that NHMRC has breached the Australian Privacy Principles' Relevant section reproduced below:

> *If you wish to complain that the NHMRC has breached one of the Australian Privacy Principles you can contact the NHMRC's Privacy Officer on (02) 6217 9000, by email to nhmrc.privacy@nhmrc.gov.au , or by writing to the following address:*
>
> *Privacy Officer NHMRC*
>
> *GPO Box 1421*
>
> *CANBERRA ACT 2601*
>
> *Your privacy complaint should be in writing and set out as much detail as possible and include any supporting documentation. You may make a privacy complaint anonymously, or by using a pseudonym. However, you should realise that if you wish to communicate with the NHMRC in this way, our ability to fully investigate and deal with the complaint may be restricted.*

## APP 2 — Anonymity and pseudonymity

*Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.*

**Analysis**

In most cases in consultations or surveys run on Citizen Space individuals will have the option of not identifying themselves or of using a pseudonym.

In exceptional cases where there is a strong practical reason for needing to identify individual respondents then a collection notice will be placed on the survey to identify why this personal information needs to be collected, how it will be used, and that provision of this information is voluntary, but that NHMRC may not be able to process the submission if this information is not included.

## APP 3 — Collection of solicited personal information

*Any personal information collected (other than sensitive information) must be reasonably necessary for (or if your entity is an agency, reasonably necessary for, or directly related to) one or more of the entity s functions or activities.*

*An APP entity must not collect sensitive information about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies.*

*Personal information can only be collected by lawful and fair means.*

*Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.*

**Analysis**

NHMRC's role in providing health advice includes a long-standing policy of public consultation which is mandated in the legislation as set out in the *National Health and Medical Research Council Act 1992* (NHMRC Act) and the National Health and Medical Research Council Regulation 1996 (NHMRC Regulation) (NHMRC 1992; NHMRC 2016).

*NATIONAL HEALTH AND MEDICAL RESEARCH COUNCIL ACT 1992 [NHMRC Act] - SECT 3*
***Object of the Act etc.***
*(1) The object of this Act is to make provision for a national body to pursue activities designed:*
*(a) to raise the standard of individual and public health throughout Australia; and*
*(b) to foster the development of consistent health standards between the various States and Territories; and*
*(c) to foster medical research and training and public health research and training throughout Australia; and*
*(d) to foster consideration of ethical issues relating to health.*
*(2) It is the intention of the Parliament that, to the extent that it is practicable to do so, the NHMRC should adopt a policy of public consultation in relation to individual and public health matters being considered by it from time to time*

Although a major part of NHMRC's role is met by its support through funding of third-party medical research, it also has a role in advising government and disseminating evidence-based health advice on a range of issues – often in the form of guidelines.

In this respect, section 3(2) of the NHMRC Act specifically imposes on the NHMRC the expectation that in doing so it would adopt a practice of public consultation in relation to individual and public health matters.

Accordingly, information collected through the use of surveys - and in particular in the future via Citizen Space - is a necessary part of the NHMRC meeting its statutory role.

The NHMRC Act is technology neutral in relation to the form of the IT systems that NHMRC should adopt to undertake consultations.

Most of the information collected by NHMRC from the responses it receives will be in the form of opinion, recommendations, or data.

Typically, however, each survey will request a respondent to provide:

- Name
- Email Address
- Phone number

These pieces of personal information will only be requested in order that NHMRC can follow up on any issues that arise from reviewing the survey response.

A more problematic issue is the question of collecting sensitive information such as gender and race.

These kinds of sensitive information can be collected in a survey, provided the reasons for collecting are explained, the individual has a discretion whether to provide the information, and any extended use of the information ('secondary') is closely related to the original purpose of its collection ('primary purpose').

There must, however, be a solid reason to justify requesting the information.

For example, NHMRC may, from time to time, conduct a survey where statistical results may be important. In these cases, the agency may request that respondents also advise of their gender/sexual orientation, race, state of health, etc. In those rare instances, the collection notice attached to the survey will need to advise this and explain the purpose of collecting the personal/sensitive information. The collection notice will also need to confirm that provision of this information will be voluntary.

Consistent with all previous consultations undertaken by NHMRC under earlier or current consultation platforms, information collected on NHMRC's Citizen Space website will only ever be collected voluntarily from respondents.

The responses (with any accompanying personal information) will be collected directly by NHMRC through Citizen Space, without any third-party intervention.

## APP 4 — Dealing with unsolicited personal information

*If an agency receives unsolicited information, it must decide whether it could have collected it under APP 3.*

**Analysis**

Unsolicited personal information is personal information received when there were no active steps taken by the agency (in this case the NHMRC) to seek or collect the information.

The NHMRC Privacy Policy states:

*In regard to submissions received during public consultation, NHMRC reserves the right to redact unsolicited personal information from submissions or to not publish submissions containing unsolicited personal information*

In compliance with this policy, before any consultation response is published a redaction process with be carried out to ensure that unsolicited personal information is not published.

## APP 5 — Notification of the collection of personal information

*An agency that collects personal information about an individual must (at or before the time it collects the information or, if not practicable, as soon as practicable) take such steps as are reasonable in the circumstances to ensure the individual is aware (e.g., by giving them notice) of the following:*

- *agency identity;*
- *details of any law that requires or authorises the collection;*
- *the purposes of collection;*
- *consequences if the information is not collected;*
- *the entities that the agency usually discloses that kind of personal information to;*
- *information about the agency's privacy policy;*
- *whether the agency is likely to disclose the information to overseas recipients [including the names of those countries if practicable].*

*This must be done before or when it collects the information or, if that is not practicable, as soon as possible after collection.*

**Analysis**

Individuals using Citizen Space will be notified of NHMRC's Privacy Policy (https://www.nhmrc.gov.au/privacy) described above whenever personal information is being collected as part of the survey package.

In addition, the NHMRC Privacy Policy and website outline these matters.

Importantly, Citizen Space will not be used to collect or store personal information from any other sources.

## APP 6 — Use or disclosure of personal information

*6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the **primary purpose**), the entity must not use or disclose the information for another purpose (the **secondary purpose**) unless:*

*(a) the individual has consented to the use or disclosure of the information; or*

*(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.*

*6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:*

*(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:*

*(i) if the information is sensitive information--directly related to the primary purpose; or*

*(ii) if the information is not sensitive information--related to the primary purpose; or*

*(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or*

**Analysis**

Information collected by Citizen Space will be used for the sole purpose of running consultations and surveys. This will be outlined in the Admin SOP and included in training given to users of the system.

The system will not by default contain any disclosure about additional uses of personal information as NHMRC's default policy as outlined in the Admin SOP will be to not allow it. If a business area wishes to create a consultation that will collect personal information that will be used for uses beyond the primary purpose set out in the survey/consultation material, they will be required to provide notice of this in the collection notice in a form that has been approved by NHMRC's privacy team as outlined in the Admin SOP.

As part of running consultations in the system NHMRC may hire consultants to analyse results. In those cases, appropriate contractual measures will be put into place to ensure confidentiality and privacy obligations are met, and the fact that data will be provided to external consultants for analysis will be advised in the collection notice attached to the relevant survey.

*With respect to the provision of personal information to consultants or committee members based overseas, see APP8.*

## APP 7 — Direct marketing

*This APP restricts an agency from using or disclosing personal information for direct marketing purposes.*

**Analysis**

No personal information collected from consultations run on NHMRC's Citizen Space are to be used for marketing purposes. This is outlined in the Admin SOP.

## APP 8 — Cross-border disclosure of personal information

*Before an agency discloses personal information to an overseas recipient, the agency must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach APPs 2-13 in relation to the information.*

**Analysis**

If an expert or consultant engaged to analyse survey data is based overseas, NHMRC will adopt one of the following approaches:

- redact any personal information that may be contained in the survey response before forwarding the data overseas.
- advise in a collection notice attached to the survey that any personal information provided in the response will only be forwarded overseas if the respondent specifically gives their consent to their personal information being forwarded overseas.

## APP 9 — Adoption, use or disclosure of government related identifiers

*This APP prevents private sector organisations from using government related identifiers, such as TFNs or Medicare numbers.*

**Analysis**
This project will not adopt, use or disclose any government related identifiers. This is outlined in the Admin SOP.

## APP 10 — Quality of personal information

*10.1 An agency must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date, and complete.*

*10.2 An agency must take reasonable steps to ensure that the personal information that it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.*

**Analysis**
The information collected while running consultations on the system is provided on a voluntary basis and as such NHMRC cannot control the information that is provided. It is reasonable for NHMRC to take the prima facie view that any personal information provided by a survey respondent is correct and that it would not be expected to verify the accuracy of the information unless there was a clear need to do so.

## APP 11 — Security of personal information

*An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.*

**Analysis**
The OAIC's *Guide to Securing Personal Information* sets out the reasonable steps the OAIC expects entities to take to protect personal information.

The NHMRC Privacy Policy notes that, under the PGPA Act, NHMRC is required to implement the Australian Government Protective Security Policy Framework (PSPF). The PSPF is recognised as providing the appropriate level of controls for the Australian Government to protect its people, information, and assets. All personal information held by NHMRC is stored in accordance with the PSPF and managed in accordance with the *Archives Act 1983*. Further, the policy also states that NHMRC complies with the Australian Signals Directorate Information Security Manual, 'and with relevant Government security standards when storing any information.'

The Privacy Policy also provides information and contact details for the NHMRC's Agency Security Advisor if an individual desires further information on the way NHMRC manages security risks in relation to personal information that it holds.

Typically, in an information collection system like Citizen Space, which can hold information from a number of surveys at the same time the particular privacy security issues that arise relate to levels of access to the system and levels of training provided to those having access to the system.

**System access**

Note: NHMRC has redacted certain security related information in this section in order to limit the potential for malicious activity.

- Personal information of administrators and analysts

Email addresses and usernames are collected from users of the system for the purpose of creating user accounts. This information is only accessible to the users themselves.

**Storage of information on NHMRC's systems**

NHMRC staff who have Citizen Space accounts store working copies of data related to consultations they are working on in protected areas inside the NHMRC network. These working copies are disposed of at the conclusion of the consultation or completion of related reports. At this point a final copy of the data is stored in a restricted part of the NHMRC network for the purpose of data recovery and records management.

**Storage of survey results on a third-party service**

Survey results collected by the system will be stored on a third-party service provider. Contracts entered into with the third-party service providers include provisions for compliance with the *Privacy Act 1988*.

**Staff training**

All staff that are using Citizen Space to run consultation will receive one-on-one training with Web Services or a member of the Citizen Space working group to ensure appropriate collection, handling and security of personal information when using the system.

**Use of Personal Information for Other (sometimes Unrelated) Surveys**

NHMRC recognises the risk of business areas wanting to use personal information collected as part of consultations for other future purposes. The agency has a strict policy as outlined in its Admin SOP that personal information collected via Citizen Space is to be used only for the purpose of conducting the consultation that it was sourced for, unless:

- the survey contains a collection notice that specifically advises that the information may be sourced and used for future research, or
- the respondent would reasonably expect the NHMRC to source and use the information for the purpose of future research, and;
    - if the information is sensitive information, it is directly related to the purpose/aims of the original survey or
    - if it is not sensitive, it is related to the purpose/aims of the original survey.

**Security measures**
A full Threat Risk Assessment (TRA) has been carried out on Citizen Space. The TRA describes the technical controls that will be implemented. A System and Security SOP will also be developed in conjunction with ITSA to outline policy and processes for maintaining the security hygiene of the system.

The Threat Risk Assessment for Citizen Space along with the System and Security SOP will be developed in-line with the Australian Government Information Security Manual and the Protective Security Policy framework. We regard these as sufficient for a system like Citizen Space.

The following security measures have been or are planned to be undertaken because of recommendations arising from the Threat Risk Assessment:

> Note: NHMRC has redacted certain security related information in this section in order to limit the potential for malicious activity.

The Admin SOP will outline that no results are to be physically printed from consultations run on the system.

ITSA has conducted a due diligence review, and we are satisfied with the results of the review - that Personal information held on Citizen Space will be adequately protected by third party providers.

The Security Assessment conducted by the NHMRC ITSA has established that the Citizen Space platform (subject to the implementation of additional mitigations listed in the assessment) provides adequate protection of personal information.

**Responding to data breaches**
Any data breaches will be responded to by NHMRC's Incident Response Team in accordance with NHMRC's IT Incident Response plan. This plan will be amended to include procedures specific to Citizen Space for each type of incident as outlined in *Part 3: Summary of risks and recommendations* of this document.

In cases where there has been a breach of personal or sensitive information, privacy commissioner reporting requirements will be complied with in accordance with the '*NHMRC Response Plan for data breaches involving personal or sensitive information'* available for download at https://www.nhmrc.gov.au/privacy.

## APP 12 — Access to personal information

*An APP entity that holds personal information about an individual must give the individual access to that information on request unless an exception applies.*

As outlined in the privacy statement on NHMRC's website an individual can ask to access or correct their personal information by contacting NHMRC's Privacy Officer by email at nhmrc.privacy@nhmrc.gov.au or by writing to the following address:

Privacy Officer NHMRC
GPO Box 1421
CANBERRA ACT 2601

## APP 13 — Correction of personal information

*An agency must take reasonable steps to correct a record of personal information if it is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading ('unreliable').*

The privacy statement on NHMRC's website informs individuals how they can correct their personal information stored by NHMRC along with the processes that are in place to respond to such requests, as outlined below:

> *If you ask, NHMRC must give you access to your personal information unless there is a law that allows or requires NHMRC to refuse access. If your personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the NHMRC will take reasonable steps to correct your personal information within 30 days of receiving and verifying your request.*
>
> *You will be asked to verify your identity before NHMRC will give you access to your information or corrects it. If you are uncertain about how to set out your request, or the supporting material required, the Privacy Contact Officer may be able to assist you.*
>
> *If a correction is made and NHMRC has disclosed the incorrect information to certain third parties, you can ask NHMRC to tell them about the correction.*
>
> *If NHMRC refuses to give you access to, or correct, your personal information, you will be notified in writing of the reasons.*
>
> *You also have the right under the FOI Act to request access to documents that NHMRC holds and ask for information that NHMRC holds about you to be changed or annotated if it is incomplete, incorrect, out-of-date or misleading. For further information see Freedom of information requests to NHMRC (https://www.nhmrc.gov.au/about-us/freedom-information*

Expert Advisor, Proximity legal services, 14th July 2022

# Part 3: Respond and review

## Responding to recommendations

| # | Action | Response |
|---|---|---|
| 1 | Update Threat Risk Assessment to take account of information outlined in this PIA | Complete |
| 2 | Ensure System and Security SOP is consistent with statements made in this PIA | Complete |
| 3 | Ensure the Admin SOP is consistent with statements made in this PIA | Accepted |
| 4 | Develop a Training SOP consistent with this PIA | Accepted |
| 5 | Ensure Privacy Statements include changes outlined in the recommendations in this PIA. | Accepted |
| 6 | Update NHMRC's Incident Response Plan to include a procedure specific to Citizen Space for each type of incident | Accepted |