Australian Government
Department of Health

Phase 1b of the Covid-19 Vaccine Strategy

Update 1 to the implementation of the COVID-19 Vaccine Strategy Privacy Impact Assessment

Agency Response

Department of Health

Australian Government
Department of Health

Copyright

Context

This document has been prepared by the Department of Health (**Health)**. It is intended to respond to the recommendations provided by Maddocks in their Phase 1b Update to the implementation of the COVID-19 Vaccine Strategy implementation Privacy Impact Assessment (PIA) Report dated 20 March 2021.

Maddocks Recommendation 1:	Continued implementation of the Original PIA report recommendations

We **recommend** that Health continue to work to implement the recommendations in the Original PIA report, as Health indicated it would do in its responses to those recommendations, during Phase 1b. We particularly highlight the importance of:

- Health continuing to adopt a 'privacy by design' approach, as Phase 1b and future Phases are rolled out (**Recommendation 1** of the Original PIA report);
- Health continuing to ensure there is open and transparent communication about how personal information will be handled in connection with the Vaccine Strategy (**Recommendation 2** of the Original PIA report);
- Health continuing to seek assurance (including from its legal advisers as appropriate) that the contractual or other administrative arrangements with Health's Partners and other third parties impose suitable privacy obligations, including in relation to the protection and security of personal information (**Recommendations 4 and 5** of the Original PIA report); and
- Vaccine Providers being appropriately trained, and provided with suitable guidance, about their privacy obligations (**Recommendations 2 and 3** of the Original PIA report).

Response

Agreed.

Phase 1b implementation of the Vaccine Strategy commenced on 22 March 2021 with a significantly larger scope than Phase 1a. Implementation of Phase 1b includes the ongoing inclusion and participation of over 3000 primary care Vaccine Providers to reach approximately 6 million eligible people across Australia. The scale of vaccine logistics including cold chain compliance for Phase 1b has been similarly expanded.

Health has committed to 'privacy by design' in all stages of the COVID-19 vaccine rollout, and has continued to work closely with Partners and key stakeholders on this, including in design, developing and testing cycles.

The publication of the Phase 1b PIA Update reflects Health's commitment to open and transparent communication about the handling of personal information in relation to the Vaccine Strategy.

As with Phase 1a, Health implemented a range of privacy protections prior to Phase 1b commencing, and will ensure these are updated as needed. Health has, among other things:

- Published Department Privacy Notices for each of the new ICT systems that has been introduced to facilitate the safe and secure delivery of COVID-19 vaccinations:
  - the Register Your Interest platform (RYI) for people in phase 2 who would like to be notified

when they are eligible to make a vaccine appointment;

- the COVID-19 Vaccine Administrative System (CVAS) which is the inventory management and COVID-19 vaccine supply system;
- the Clinician Vaccine Integrated Platform (CVIP), which Patients and Vaccine Providers can use to meet reporting obligations to the Australian Immunisation Register. Consumer Terms of Use and Vaccine Provider Terms of Use were also published; and
- the Commonwealth-procured Booking Platform (BP), which Vaccine Providers may wish to use if they do not already have an online booking solution. Separate Notices for Vaccine Providers and for Patients were published.

- Worked with HealthEngine, our Partner in developing the BP, to prepare a tailored Privacy Policy and Collection Notice that reflects agreed data collection, use and handling obligations for the BP in line with the *Privacy Act 1988*. Tailored Terms and Conditions of Use for Consumers and Terms and Conditions of Use for Vaccine Providers were also developed. These are separate from the arrangements for HealthEngine's mainstream booking solution.
- Ensured that privacy and security considerations were a priority in ICT design. Guidance and links to relevant privacy documents were embedded in the ICT systems as a 'layered' approach to facilitating user awareness of privacy protections before information is collected.
- Continued to add to and update our specific COVID-19 Vaccination Privacy landing page: www.health.gov.au/covid19-privacy.

Health has continued to consult with internal and external legal advisers in relation to agreements and contracts with Partners and third party entities involved in the rollout, including obtaining specific advice relating to privacy obligations and monitoring compliance with the contracts.

Training materials used by Vaccination Providers contains guidance on privacy and a link to the Health website. The training module on consent also covers the reporting of personal information to the Australian Immunisation Register.

Maddocks Recommendation 2:	Tailored communication products and processes

We **recommend** that Health consider implementing, as soon as possible, additional measures designed to ensure that all Australians receiving vaccines or otherwise involved in Phase 1b are able to fully understand how their personal information will be handled. This is particularly important given that Phase 1b will involve greater numbers of Patients who may be vulnerable and need additional support to ensure they are able to understand how their personal information will be handled (and provide consent where applicable). This may include:

- including functionality so that information on all of the new ICT components and in the associated privacy notices can be displayed or provided in other languages; and/or
- making interpreting services freely available.

In particular, Health may wish to, in addition to the measures recommended in **Recommendation 6**, commence developing tailored communication and explanatory materials, and/or alternative processes, for children who are aged 15 years or older, to ensure that these older children who are Patients are able to understand and communicate valid consent. Health may also wish to implement alternative processes that are specifically designed for such younger Patients, such as tailored booking services that would provide an opportunity to assess the individual's capacity to provide consent and to deliver targeted information

Response	Agreed. Health is ensuring that information is widely accessible for a range of audiences. Online privacy documents have been drafted to be understood by the vast majority of people who speak English. Translations into the 9 languages other than English that are most frequently spoken in Australia[1] have also been undertaken for the Eligibility Checker and RYI platforms, as well as the associated Privacy Notice. Health is in the process of having other platforms and notices translated, such as the BP workflow and associated privacy documents. Health has also engaged with the Culturally, Ethnically and Linguistically Diverse COVID-19 Health Advisory Group in relation to the rollout. In relation to young people aged 16 or 17 years, who meet eligibility criteria for Phase 1b, Health is preparing a tailored pathway for young people of these ages to make bookings and receive vaccinations. The RYI is restricted to people aged 18 years and older in Phase 2 at this stage to reflect the expected

[1] These include Arabic, Greek, Italian, Korean, Punjabi, Simplified Chinese, Traditional Chinese, Turkish, and Vietnamese.

	continuation of a tailored pathway for people aged 16 and 17 years in Phase 2. COVID-19 vaccines are not yet approved for people aged 15 years or under (Phase 3) and therefore use of the ICT systems excludes this phase. Health will consider the most appropriate pathway for Phase 3 as needed.

Maddocks Recommendation 3:	**Review and update Privacy Notices for the CVAS, the CVIP, the RYI and the BP**

We **recommend** that the Privacy Notice for the CVAS be reviewed and updated to:

- reflect preferred terminology now used in respect of the Vaccine Strategy, for consistency with other publicly available information (e.g. 'Delivery Contacts' rather than 'Distribution Contacts');
- reflect the additional Delivery Contacts who will now provide personal information when using the CVAS (these could potentially be referred to as 'Users' which is a term currently used in the drafting but not defined);
- reflect the role of PHNs in facilitating the onboarding of Vaccine Providers to the CVAS (including the use of the Notice Contact's email address to facilitate this onboarding);
- ensure the role of the Data Partner in handling personal information is clear; and
- specify with greater certainty whether any, and if so what, personal information will be disclosed to States and Territory governments (the Privacy Notice specifies that Health 'may disclose provider (site) information to other entities, such as State or Territory governments, for the purposes of facilitating or monitoring the vaccine rollout'). If no personal information will be disclosed to States and Territories, then the Privacy Notice should expressly state this.

In addition, we **recommend** that the Privacy Notice for the CVIP also be reviewed and updated so that:

- it adequately informs users how and where their information will be stored. In particular, we think it is important that users are aware that their information will be temporarily stored using cloud infrastructure made available by a third party (Salesforce) before it is provided to the AIR;
- separate notices for Patients, and for Vaccine Providers and their personnel (i.e., Vaccinators) are developed; and
- it appropriately reflects the personal information being collected and stored on the CVIP platform (including when information will be deleted), and all proposed uses and disclosures of that personal information.

We also r**ecommend** that the Privacy Notice for the RYI solution:

- be updated to reflect Health's current understanding that only de-identified information would be provided to States and Territories, and how those entities would be permitted to use that information; and

- could perhaps be updated to make it clear that the individual may provide a pseudonym or 'fake name', to enhance compliance with APP 2 (although we do not consider this to be critical).

In relation to the BP, we **recommend** that Health consider:

- the most appropriate way to communicate to Patients accurate and complete information about how their personal information will be handled by Health and by HealthEngine in connection with the BP, taking into account the need to provide Patients with useful and consistent information whilst considering the risks of Patients experiencing 'information overload'; and

- some minor adjustments to the HealthEngine BP Privacy Policy to better reflect the method of collection described in this PIA Update report and consistency with the contractual mechanisms for deletion in the HealthEngine Contract.

Response	Agreed. Health has updated the CVIP Privacy Notice to align with the PIA Update recommendations and will consider whether further updates should be made. Health is in the process of updating the Privacy Notices for the CVAS and the RYI platforms. In relation to the RYI Privacy Notice, Health has considered and decided against specifying that an individual may use a 'fake name' or pseudonym in its privacy material as the requirement to complete the First and Last Name fields can also act as a quality assurance mechanism against 'vandal' responses. Health does not, however, prevent a pseudonym or 'fake name' from being used if the consumer chooses. This is set out in Health's Privacy Policy which is linked in the RYI Privacy Notice. Health had implemented a range of privacy protections for the Commonwealth-procured Booking Platform ahead of its launch, including a tailored Privacy Policy and Collection Notice that reflects agreed data collection, use and handling obligations for the BP in line with the *Privacy Act 1988*. Tailored Terms and Conditions of Use for Consumers and Terms and Conditions of Use for Vaccine Providers were also developed. These are separate from the arrangements for HealthEngine's mainstream booking solution. Health has considered whether changes should be made to the privacy documents surrounding the BP, taking into account feedback from the PIA process, including engagement with the OAIC. In order to prevent 'information' overload, a 'snapshot' Privacy Summary is available to consumers in the BP confirming key information in relation to their privacy. Health will continue to take a 'privacy by design' approach and will continue to engage with relevant stakeholders to implement any additional privacy protections that may be needed as the rollout progresses.

Maddocks Recommendation 4:	Contractual arrangements with third party entities

We **recommend** that Health ensure (including through seeking assurance from its legal adviser, as appropriate) that the robust general privacy and security obligations in its contractual arrangements with the Data Partner, and with other third parties involved in accessing or otherwise handling personal information in Phase 1b, continue to remain suitable.

We also **recommend** that Health consider supplementing already robust privacy and security protections in the HealthEngine Contract, by making amendments as necessary or appropriate to clarify:

- that HealthEngine must hold any information collected in connection with the BP separately from any other information it collects as part of its BAU practices (such as through the usual online booking services it provides to other health professionals); and
- whether or not the contractual obligations (including the protections in relation to privacy and security) sufficiently apply to information collected by HealthEngine in connection with the BP; and
- the points at which HealthEngine is required to delete or destroy information collected through the BP (or return it to Health).

We also note that it will be important for Health to ensure that it has appropriate monitoring and auditing processes in place, to ensure HealthEngine complies with its strong privacy and security obligations under the HealthEngine Contract.

Response	Agree in principle. Health has robust contractual privacy clauses with its Partners, including in its contract with HealthEngine for the BP. Health has ensured that the BP has been designed and functions as a stand-alone system, without interoperability with HealthEngine's mainstream platform. Health owns the data from the BP, including personal information, and has ensured it will only be used for the purpose of facilitating COVID-19 vaccinations. Data from the BP is protected by the Privacy Act and strict privacy provisions in Health's contract with their cloud service provider. Health will, consistent with the contract, request the data be returned and/or deleted from HealthEngine's holdings. Privacy materials developed for the BP reflect these arrangements and Health considers that additional contractual revisions (beyond formal amendments contemplated under the current terms of the contract) are not warranted. The OAIC provided comments for Health to consider in relation to arrangements for the BP. Following this PIA, Health will engage with appropriate stakeholders and the OAIC on the further steps that will be put into place at the time of the decommissioning of the BP. Health's contract managers will ensure that appropriate auditing and monitoring processes are in place for compliance against the contract.

	Contracts with the Data Partner and HealthEngine also require the provision of Data Protection Plans. Health is currently reviewing the plans received to date. As in Phase 1a, Health will continue to engage with relevant stakeholders, as appropriate, in relation to contractual arrangements with Partners and third party entities involved in the COVID-19 vaccine rollout.

Maddocks Recommendation 5:	**Transmission of personal information between ICT systems and entities participating in Phase 1b**

We **recommend** that Health take steps to ensure, including by undertaking appropriate testing, that when personal information is transferred between ICT systems or components, or otherwise between different entities participating in Phase 1b:

- the information is appropriately protected from misuse, interference and loss, and from unauthorised access, modification or disclosure (this will assist Health to comply with its obligations under APP 11); and
- the quality of information transferred is not reduced during the transmission, (for example through unintentional changes or omissions) (this will assist Health to comply with its obligations under APP 10).

In particular, we **recommend** that the temporary arrangements established for the transfer of information (which includes personal information) from the CVAS to the Logistics and Distribution Partners be re-examined as soon as possible, to reduce the enhanced potential for loss or unauthorised access.

Response	Agreed. Health has undertaken the design of digital and ICT systems working in a federated environment, and so acknowledges that there are transition points when individuals move out of the Health-developed and managed systems into those managed by other entities, such as jurisdictions or commercial organisations. As part of implementing 'privacy by design', Health aims to transfer only required personal or sensitive information under the 'data minimisation' principle and in compliance with the Privacy Act. Nevertheless, in developing ICT solutions, contractual obligations with Health's Partners in the COVID-19 vaccine rollout oblige them, in turn, to ensure that personal information is appropriately protected from unauthorised access, use or disclosure and other misuse. Robust processes are in place for carrying out testing and quality assurance of systems developed to identify security vulnerabilities and ensure appropriate security arrangements are in place. In implementation of the new ICT systems developed for Phase 1b, Health has completed various processes and engaged relevant expertise through the Chief Information Security Officer, including resources from the Australian Cyber Security Centre (ACSC), a security assessor certified through the ACSC Information Security Registered Assessors Program (IRAP) and independent assurance services to ensure that the systems meet the requirements of the Protective Security Policy Framework. There are various artefacts developed

	including Security Plans, Threat Assessments, Data Protection Plans, Incident Response Plans, Penetration Test Reports and a Final Security Report. Health notes the particular recommendation in relation to the CVAS. Further system design for a secure automated transfer of information from the CVAS to the Logistics and Distribution Partners' delivery dispatch systems has already commenced, with the intent of replacing temporary arrangements and mitigating associated risks as soon as possible.

Maddocks Recommendation 6:	**Consider further development of wording on the RYI solution webpage**

We **recommend** that Health consider whether there is potential to further improve the RYI solution at a future time. For example, Health could consider including on the RYI solution webpage:

- a mechanism or place for a person submitting information on behalf of another person to confirm that they have authority to provide consent on behalf of the relevant individual (e.g. by requiring individuals to confirm words to the effect of *'I acknowledge that I am the legal guardian of, or have consent to provide the information of, the individual identified in the information I have supplied'*); and/or
- a 'pop-up' message beside each field that needs to be completed, which explains why the collection of the information is reasonably necessary.

We do acknowledge the need for Health to balance the privacy benefits of such developments against the costs of implementation and the risk of 'information overload' for users.

In addition, we **recommend** that:

- individuals are provided with a mechanism to update or correct their information, and to 'opt-out' of receiving a notification if they choose (for example, it may be that the phone line and email address for Health privacy enquiries, as set out in the Privacy Notice, could be used); and
- once those mechanisms are put in place, the Privacy Notice for the RYI solution (and also the wording on the RYI solution webpage) be updated to reflect those mechanisms.

Response	We agree in principle with this recommendation. With respect to children, at present, an individual can only be registered via the RYI platform if they are 18 years or older. For those who enter an age under 18 years in the precursor system, the Eligibility Checker, an option to then Register Your Interest will not appear. Health is also conscious that the user experience of the RYI platform should not be onerous. Instead of an additional verification mechanism, Health has provided guidance on its RYI webpage that submissions on behalf of someone else should only be done by a legal guardian or with the person's consent.

	In relation to pop-up messages, Health agrees that it is important for all persons using the RYI platform to understand why the requested information fields are published. However, Health notes that an individual should be able to reasonably infer the rationale behind the fields requested, such as names and contact details. The questions in the Eligibility Checker (which we only collect if the individual goes on to RYI) include relevant information for phase eligibility to receive a vaccine. Health has focused on collecting key information only to ensure that notifications can be sent to the right people at the right time. As the RYI platform is intended for a point in time notification, Health is not considering options to correct or amend information. However, Health is implementing an 'opt-out' mechanism for potential recipients of notifications for RYI and is updating the Privacy Notice accordingly.

Maddocks Recommendation 7:	**Arrangements with the Notification Provider for the RYI solution**

We **recommend** that Health ensure that:

- it selects, or has selected, an appropriate entity to be the Notification Provider, who should be subject to the obligations of an 'agency' under the Privacy Act (either in its own right or through imposition of appropriate contractual obligations), and who has appropriate security mechanisms in place to protect the collected personal information; and
- the contractual or other documented arrangements between Health and the Notification Provider contain appropriate obligations in relation to the handling of personal information. The contractual or other arrangements should include requirements for the Notification Provider to act as if it is an 'agency' for the purposes of the Privacy Act (if it is not an APP entity), and must comply with obligations under the Privacy Act. For example, the arrangements could require the Notification Provider to use particular (strong) security arrangements, confirm that the use and disclosure of the information will only be for the purpose provided, confirm that access will be on a need-to-know basis, and require early notification of any actual or suspected data breach.

Response	Agreed. Health has sought input from relevant stakeholders in relation to selecting the most appropriate Notification Provider. This process has included considering the Department's privacy and security requirements, as well as privacy considerations and the advice sought from the OAIC for RYI. Health has carefully considered the above recommendations in relation to the selection of 'Notify', an online notifications service developed by the Digital Transformation Agency (DTA). Government entities are able to use notify to securely send messages via email or mobile number to users. Existing privacy protections for Notify are outlined in their privacy statement.

	While the DTA is presently Health's only contracted partner and delivery channel for notifications, if Health needs to contract another Notification provider, Health will engage a Notification provider with equally strong privacy and data security protections, and if necessary engage relevant stakeholders in that process.

Maddocks Recommendation 8:	**Consider further development of information provided to individuals in relation to the BP**

We **recommend** that Health consider whether there is potential to further improve the BP solution at a later stage. For example, Health could consider:

- ensuring the BP displays the Collection Notice and Health's Privacy Notice for Vaccine Providers to users accessing the BP on behalf of a Vaccine Provider, before any personal information is required to be provided;
- issuing Vaccine Providers with guidance on how to ensure that their nominated personnel (such as their Primary Contact) provide their consent to their information being collected, used and disclosed by HealthEngine; and
- ensuring that the BP displays to Patients all of the relevant information about how their personal information will be handled, before they either log into or create a HealthEngine account, in order to book an appointment to receive the COVID-19 vaccine.

Response	Agreed. In relation to Vaccine Providers, a link to the Department's COVID-19 privacy page is provided in the Services Form that providers are required to sign before signing up to the BP. In relation to Patients, HealthEngine's Privacy Policy and Collection Notice are linked before a patient's personal information is collected – that is, just before a patient clicks 'continue' to submit their information. HealthEngine's Privacy Policy also references Health's Privacy Notices.

Maddocks Recommendation 9:	**Implementation of recommendations from the separate CVIP privacy assurance process**

We **recommend** that Health continue to work with the ADHA to ensure the CVIP has strong privacy protections in its design and supporting contracts, as recommended through ADHA's privacy assurance processes (conducted in parallel with this PIA Update process), including:

- additional clarity of information in the relevant privacy documents provided to Patients and Vaccine Providers using the CVIP (consistent with **Recommendation 3**);
- engagement with the OAIC on privacy considerations and publication of the outcome of the privacy assurance processes for the CVIP App (consistent with **Recommendation 2** of the Original PIA report);
- robust contractual obligations for the security of information with third parties (consistent with **Recommendation 4**);

- implementation of the principle of 'data minimisation' so that the CVIP App only collects the minimum amount of information necessary for the purposes of transferring it to the AIR; and

- progressing additional privacy assurance processes, particularly if the responsibility for administration of the CVIP App is transferred from Health to another Commonwealth entity, such as the ADHA (consistent with **Recommendation 1** of the Original PIA report).

Response	Agreed. The CVIP Privacy Notice has separate sections for providers and consumers to ensure clarity and relevance of information for each group. The Privacy Notice is displayed at the 'check yourself in' page at the start of the process the page includes links to the CVIP Privacy policy and Terms of Use. Further updates are under consideration in line with Recommendation 3. Health will continue to implement 'privacy by design,' including progressing additional assurance processes in the event that the responsibility for CVIP transfers to another Commonwealth entity. Any changes will also be reflected in the published privacy documents. Health has engaged with the OAIC ahead of the publication of the Phase 1b COVID-19 Vaccine Strategy PIA Update, and will continue to do so in relation to any further privacy assurance processes for the CVIP. Health's internal and external legal advisers are also engaged in ensuring that the contractual arrangements underpinning the CVIP meet robust privacy and security requirements. Health can confirm that the principle of 'data minimisation' continues to be implemented in the design and ongoing management of the CVIP and associated business processes. Information collected during the course of a vaccination appointment is intended for the purpose of meeting reporting obligations to the Australian Immunisation Register. If there are further system developments, Health will consult with the appropriate stakeholders to ensure ongoing privacy protections.