Maddocks

Lawyers
Level 1
40 Macquarie Street
Barton ACT 2600 Australia

Telephone 61 2 6120 4800
Facsimile 61 2 6230 1479

info@maddocks.com.au
www.maddocks.com.au

Department of Health

PHASE 1B OF THE COVID-19 VACCINE STRATEGY

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

Analysis undertaken as at 20 March 2021

Contents

Part A INTRODUCTION

1. Overview

1.1 Maddocks was engaged by the Commonwealth Department of Health (**Health**) early in the process of the implementation of the COVID-19 Vaccine and Treatment Strategy and the COVID-19 Vaccine National Roll-out Strategy (together, the **Vaccine Strategy**)[1]. In February 2021, we completed a privacy impact assessment (**PIA**) in relation to Phase 1a of the implementation of the Vaccine Strategy (**Original PIA**).[2]

1.2 Consistent with **Recommendation 1** of the Original PIA (which recommended that Health continue to take a 'privacy by design' approach as the implementation of the Vaccine Strategy progresses, including for future Phases), we have now been engaged by Health to undertake an updated privacy impact assessment process (**PIA Update**), to examine the privacy impacts associated with the implementation of Phase 1b of the Vaccine Strategy.

1.3 Phase 1b involves a broader roll out of the COVID-19 vaccines to additional populations of Australia, and the implementation of some additional ICT systems and processes that have been, or are being, implemented to facilitate this. In this PIA Update, we have examined the following changes which have, or will, occur as part of Phase 1b:

1.3.1 changes to who is eligible to receive, and who is authorised to administer, the COVID-19 vaccine; and

1.3.2 several new ICT components, including:

(a) a COVID-19 Vaccine Administrative System (**CVAS**) to allow Vaccine Providers to place orders for COVID-19 vaccines and consumables;

(b) a 'Register your Interest' (**RYI**) solution, which following use of the Eligibility Checker, allows members of the public to choose to be contacted when the future Phase in which they will be eligible to make a booking to receive a vaccine will commence;

(c) a Commonwealth-Procured Booking Platform (**BP**), to facilitate members of the public being able to make online bookings to receive a vaccine where their chosen Vaccine Provider does not otherwise have an online booking system and wishes to use the Commonwealth-procured BP; and

(d) a Clinician Vaccine Integrated Platform (**CVIP**) solution (including a new software application (**CVIP App**)), to allow Vaccine Providers (and Vaccinators administering a COVID-19 vaccine) to submit required information about vaccinations to the Australian Immunisation Register (**AIR**).

1.4 This PIA Update report is intended to supplement the findings and analysis in the Original PIA report. It does not seek to reiterate or reconsider matters that were discussed in the Original PIA report. We note that, in general, the information flows and the associated privacy impacts and risks that were discussed in the Original PIA report will continue to apply during Phase 1b.

[1] The relevant documents can be found at: https://www.health.gov.au/sites/default/files/documents/2020/08/australia-s-covid-19-vaccine-and-treatment-strategy.pdf and https://www.health.gov.au/sites/default/files/documents/2021/01/australia-s-covid-19-vaccine-national-roll-out-strategy.pdf.

[2] A summary version of this PIA report, and Health's responses to the recommendations made in that report, are available at: https://www.health.gov.au/resources/publications/covid-19-vaccination-phase-1a-of-covid-19-vaccine-strategy-privacy-impact-assessment-report-and-agency-response.

2. Structure of this PIA Update report

2.1 This PIA Update report is comprised of the following sections:

2.1.1 **Part B - Executive Summary**: This section contains a summary of the privacy risks we have identified, together with a list of all recommendations we have made as a result of our analysis.

2.1.2 **Part C - Methodology:** This section details how we have undertaken the PIA Update, and includes information about the scope of the PIA Update report.

2.1.3 **Part D - Project Description - Overview:** This section contains a summary of the changes involved with Phase 1b of the Vaccine Strategy, which may have potential privacy impacts.

2.1.4 **Part E - Project Description and Privacy Analysis for Each Change:** This Part contains separate sections for each identified change. Each section sets out a detailed description of the change, and our privacy impact analysis of any potential privacy impacts or risks that we have identified as being associated with the change, including any current mitigation strategies, and any recommendations.

2.1.5 **Part F - Glossary:** This section sets out a list of some capitalised terms that we have used in this PIA Update report, and their definitions.

2.1.6 **Attachment 1 – Material reviewed:** This contains a list of relevant material we have reviewed as part of undertaking our analysis for this PIA Update report.

Part B EXECUTIVE SUMMARY

4. Summary of findings

4.1 As was the case during the planning and implementation of Phase 1a, we have been privileged to work with Health to provide advice and guidance about identified privacy risks, as the plans, processes and systems that will be used in Phase 1b have been developed in parallel with the production of this PIA Update report.

4.2 We have found that Health has continued to demonstrate an appreciation of the importance associated with the handling of personal information, and a willingness to incorporate changes to ensure compliance with the requirements of the APPs or the principles of the Privacy Act more broadly, to the maximum extent technically possible or practical.

4.3 As discussed further in this PIA Update report, we note that ongoing vigilance will be required to ensure that privacy risks (including any potential privacy risks) continue to be appropriately addressed. This will include the need to:

4.3.1 continue to implement the overarching recommendations in the Original PIA report during Phase 1b;

4.3.2 continue to monitor the appropriateness and accuracy of released communications material, including Privacy Notices for the various ICT systems, to ensure that they continue to be accurate and reflect best privacy practice (including the need to consider, and if appropriate develop, material which is tailored for specific population cohorts who will receive a COVID-19 vaccine in Phase 1b, including young or vulnerable people);

4.3.3 continue to ensure that all contractual arrangements, including with Partners and other entities involved in the delivery of the various ICT systems which handle personal information, are 'fit for purpose' and contain appropriate obligations in relation to the handling of personal information (including security obligations);

4.3.4 continue to carefully examine, and test, the security of the various ICT components, including in particular where personal information is transferred between systems or entities;

4.3.5 continue to explore further developments of the various ICT components of Phase 1b, including to assess whether additional measures could be implemented to further enhance privacy protections; and

4.3.6 continue to work with the ADHA and other stakeholders, including Services Australia, to ensure that the recommendations from the CVIP privacy assurance processes are appropriately considered and implemented.

4.4 The privacy risks have been considered throughout this PIA Update report, and the recommendations set out in paragraph 5 of this **Part B** are designed to address the identified issues and associated risks, and to further enhance privacy protections for individuals during Phase 1b of the implementation of the Vaccine Strategy.

5. Recommendations

5.1 This PIA Update makes the recommendations below. These recommendations reflect the order in which they appear in this PIA Update report, and not any order of importance or priority.

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).

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.

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 **recommend** 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.

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.

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.

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.

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.

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.

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).

Part C METHODOLOGY AND ASSUMPTIONS

6. Our methodology

6.1 This PIA Update has been conducted to ensure that any identified privacy risks can be considered and addressed, to minimise the impact upon individuals whose personal information may be collected in connection with the Vaccine Strategy.

6.2 We conducted our PIA Update broadly in accordance with the Office of the Australian Information Commissioner's Guide to undertaking privacy impact assessments, as applicable to a PIA Update process. This involved the following steps:

Stage	Description of steps
1.	**Plan for the PIA Update:** We reviewed some relevant background material provided by Health, and were provided with briefings by officers from Health. We also agreed on the scope of this PIA Update report (discussed further below in this **Part C**), the approach to undertaking a broader stakeholder consultation process, and the timeframes for the necessary activities involved in conducting this PIA Update report.
2.	**Project Description and information flows:** We prepared an initial draft Project Description, which described the changes that have been, or will be, implemented as a result of Phase 1b. This draft was refined, and then finalised, in an iterative process as further information was received from Health.
3.	**Privacy impact analysis and compliance check:** In this step we focussed on compliance of each change against the relevant Australian Privacy Principles (**APPs**), and privacy best practice. The analysis set out in this PIA Update report is consistent with the *Australian Privacy Principles Guidelines* (**APP Guidelines**) issued by the Office of the Australian Information Commissioner (**OAIC**), which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing Health's compliance with the Privacy Act. We took into account feedback from stakeholders, including valuable input from the OAIC, in considering the identified risks. In this PIA Update report, as was the case with the Original PIA report, we have not undertaken a rigorous risk assessment methodology to identify the magnitude of each of the identified risks. However, this could be done at a later stage, as required, including as part of Health's consideration and implementation of our recommendations.
4.	**Privacy management and addressing risks:** We considered potential mitigation strategies that could reduce or remove the privacy impacts and risks identified during the previous step.
5.	**Recommendations:** From the steps referred to above, we developed our recommendations, designed to remove or reduce privacy risks.
6.	**Draft report:** We prepared a draft version of this PIA Update report, which was further updated based on additional information provided and changes made to the Vaccine Strategy.
7.	**Stakeholder consultation:** Given the interest surrounding the development and implementation of the Vaccine Strategy, a draft version of this PIA Update report was provided to several stakeholders for consideration, including the OAIC, and other Australian Government agencies involved in the Vaccine Strategy. We received comments by these stakeholders on that draft version of this PIA Update report.

8.	**Refinement of draft report of Privacy management and addressing risks:** We further refined our analysis and the potential mitigation strategies following feedback from Health and other stakeholders.
9.	**Report:** We finalised this PIA Update report.

6.3 We understand that Health will review this PIA Update report, in consultation with other stakeholders as required, and separately respond to our recommendations.

6.4 A glossary of defined terms and acronyms is at **Part F** of this PIA Update report.

7. Community expectations

7.1 As with the Original PIA, in the PIA Update process, we have assessed risks based on our understanding of reasonable community expectations of privacy, including as indicated by research such as the *Australian Community Attitudes to Privacy Survey 2020* commissioned by the OAIC, which contains useful information regarding current community expectations (this was summarised in the Original PIA report).[3]

7.2 We have had the benefit of taking part in stakeholder consultations, particularly with the OAIC, which has provided useful guidance on current community expectations of privacy.

7.3 We have also taken into account public reactions to the implementation of Phase 1a, and public announcements in relation to various comments about Phase 1b, including as reported by the general media.

8. Assumptions and qualifications

8.1 This PIA Update report has been conducted from the perspective of Health, as the Commonwealth agency responsible for the implementation of the Vaccine Strategy, and not from the perspective of any other entity involved with the Vaccine Strategy (including the Australian Digital Health Agency (**ADHA**), or any State and Territory authorities).

8.2 As was the case with the Original PIA process, the implementation of the Vaccine Strategy has continued to develop during this PIA Update process (including through development of this PIA Update report). This has meant that it has been necessary to again conduct this PIA Update as a 'point in time' analysis for Phase 1b of the Vaccine Strategy, based on the factual information provided by Health as set out in **Part E [Project Description and Privacy Analysis for Each Change]** of this PIA Update report (we have not independently verified that that factual information is correct or complete, and acknowledge that it may not remain up-to-date).

8.3 This PIA Update report is limited to considering Phase 1b of the Vaccine Strategy. While this PIA Update report references our understanding of some of the matters that are likely to be covered in later stages of the Vaccine Strategy, this PIA Update report does not analyse or make recommendations into those matters. We understand that Health intends to undertake further analysis in relation to later stages of the Vaccine Strategy, after the finalisation of this PIA Update.

8.4 This PIA Update report does not analyse or examine any Information Flows, or associated privacy risks or compliance issues, for Phase 1b that are not described in **Part E [Project Description and Privacy Analysis for Each Change]** of this PIA Update report.

[3] This survey was published in September 2020.

Part D PROJECT DESCRIPTION – OVERVIEW

9. Phase 1b of the Vaccine Strategy

9.1 As discussed in the Original PIA report, as part of the Australian Government's response to the COVID-19 pandemic, Health is implementing the Vaccine Strategy, which aims to support access to, and delivery of, safe and effective COVID-19 vaccines for all persons in Australia, as soon as they are available. The Vaccine Strategy is supported by a policy released by Health, which describes the shared and separate responsibilities of the Australian, and State and Territory governments, as well as other key stakeholders, in developing and supporting the implementation of the Vaccine Strategy.

9.2 The Vaccine Strategy is being implemented in phases:

9.2.1 **Phase 1a** – this phase covers the initial rollout of a vaccine (a vaccine developed by Pfizer and also a vaccine developed by AstraZeneca) to certain high-priority populations, and the introduction of ICT systems and processes to support the COVID-19 vaccine rollout;

9.2.2 **Phase 1b** – this phase will cover the broader rollout of vaccines to additional populations, and the introduction of further ICT systems and processes (these are discussed in further detail below);

9.2.3 **Phase 2a** – this phase will cover additional populations or cohorts across Australia;

9.2.4 **Phase 2b –** this phase will cover the rest of the adult population across Australia (including individuals who were eligible in previous phases but were not vaccinated); and

9.2.5 **Phase 3** – this phase will cover children, subject to further consideration.

9.3 As part of **Recommendation 1** in the Original PIA report, we recommended that Health continue to take a 'privacy-by-design' approach as the implementation of the Vaccine Strategy progresses.

9.4 As part of Health's implementation of this recommendation, Maddocks has been engaged by Health to undertake this PIA Update process in relation to Phase 1b of the Vaccine Strategy, to examine in detail:

9.4.1 the impact of changes to the information flows for the Vaccine Strategy as identified in the Original PIA report;

9.4.2 any additional or changed analysis which is now required as a result of changes in information flows; and

9.4.3 any new privacy risks arising out of the changes, and any recommended mitigation strategies to address those risks.

9.5 Phase 1b will differ from Phase 1a in the following ways:

9.5.1 who is eligible to receive, and who is authorised to administer, the COVID-19 vaccine will be expanded; and

9.5.2 several new ICT components will be introduced, including:

(a) a 'Register your Interest' (**RYI**) solution;

(b) a COVID-19 Vaccine Administrative System (**CVAS**);

(c) a Commonwealth-procured Booking Platform (**BP**); and

(d) a Clinician Vaccine Integrated Platform (**CVIP**).

9.6 The ICT systems specified in paragraph 9.5 of this **Part D**, together with ICT systems provided by HealthDirect Australia (**HealthDirect**) – the Eligibility Checker[4], and the Vaccine Clinic Finder (which provides individuals with the ability to find a Vaccine Provider if they are eligible in accordance with the Eligibility Checker), are referred to as the COVID-19 Vaccine Information and Location Service (**VILS**).

10. Structure of Part E [Project Description and Privacy Analysis for Each Change]

10.1 We have analysed each of the changes identified in paragraph 9.5 of this **Part D** in separate sections below, including for each new ICT component. In each section, we have:

10.1.1 provided further information on the change (by way of a "Project Description" for each change);

10.1.2 considered the privacy impacts of the change, given the requirements of the Privacy Act (the APPs), including identifying any privacy risks or concerns; and

10.1.3 made recommendations that are designed to:

(a) address the risks identified as part of our considerations described in paragraph 10.1.2 of this **Part D**;

(b) further enhance privacy protections for individuals; and/or

(c) further strengthen compliance with the Privacy Act (including the APPs).

10.2 The analysis below does not address those elements of the APPs which reflect Health's broader compliance obligations, but only considers those elements that specifically relate to the changes specified in paragraph 9.5 of this **Part D**.

10.3 Details of the text of the APPs is set out in the Original PIA report, and we have not replicated this information in this PIA Update report. However, the APPs can be found here.

[4] The Eligibility Checker is available at: https://covid-vaccine.healthdirect.gov.au/eligibility, but is not part of the ICT systems examined by this PIA Update (we understand that no personal information is collected by this tool).

Part E PROJECT DESCRIPTION AND PRIVACY ANALYSIS FOR EACH CHANGE

Section A Expansion of eligibility to receive and to administer a COVID-19 vaccine

11. Project Description

11.1 As part of Phase 1b of the Vaccine Strategy, we understand that additional population groups will be eligible to make an appointment to receive the COVID-19 vaccine.[5] These include the following:

11.1.1 healthcare workers currently employed and not included in Phase 1a, including in hospitals, general practices, pharmacists, allied health, and other healthcare services in the community;

11.1.2 household contacts of quarantine and border workers;

11.1.3 critical and high risk workers currently employed, including in defence, police, fire, emergency services and meat processing industries;

11.1.4 people 70 years and over;

11.1.5 Aboriginal and Torres Strait Islander people aged 55 years and over; and

11.1.6 people with a an underlying (specified) medical condition (which means they are at an increased risk of severe disease), including people with a disability.

11.2 Health expects approximately 14.8 million doses of COVID-19 vaccines will be administered during Phase 1b.

11.3 In addition, as part of Phase 1b, the entities that may be Vaccine Providers will expand from those delivering vaccines in Phase 1a, to also include General Practitioners (**GPs**), GP-led Respiratory Clinics (**GPRCs**) and Aboriginal Community Controlled Health Services (**ACCHSs**).

11.4 We understand that due to the numbers of GPs, GPRC clinics and ACCHSs that will become Vaccine Providers from Phase 1b onwards, Health has staggered their onboarding into weekly tranches, also known as 'Vaccine Provider cohorts'. Therefore, though Phase 1b vaccinations commence on 22 March 2021, more GP, GPRC and ACCHS Vaccine Providers will come on board following that date.

[5] Further information on this is available at: https://www.health.gov.au/sites/default/files/documents/2021/03/priority-groups-for-covid-19-vaccination-program-phase-1b_1.pdf.

12. Privacy impact analysis and compliance

Increased numbers of Patients and Vaccine Providers

12.1 In Phase 1b:

12.1.1 there will be significantly greater number of Patients whose personal information, including sensitive information, will be handled; and

12.1.2 there will be a significantly increased number of Vaccine Providers:

(a) who will be handling personal information about Patients; and

(b) whose Provider Personnel may have their information handled in connection with Phase 1b.

12.2 The sheer numbers involved mean that the privacy risks identified in the Original PIA will necessarily increase, as more personal information about more individuals becomes affected. This highlights the importance of implementing the mitigation strategies we identified in the Original PIA report. We consider that implementation of the recommendations in the Original PIA report in relation to Phase 1a will greatly assist in reducing the likelihood and impact of the privacy risks during Phase 1b. Accordingly, we **recommend** that Health continue to work to implement the recommendations of the Original PIA report, as Health indicated it would do in its responses to those recommendations, during Phase 1b (**Recommendation 1**).

12.3 In particular, we highlight the importance of Health ensuring that:

12.3.1 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);

12.3.2 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

12.3.3 Vaccine Providers are appropriately trained, and provided with suitable guidance, about their privacy obligations (**Recommendations 2 and 3** of the Original PIA report).

New types of Vaccine Providers

12.4 We also note that GP practices, GPRCs and ACCHSs will now be able to be Vaccine Providers. GPs are medically trained professionals, subject to professional and regulatory obligations, and GPRCs are entities that are already subject to robust contractual obligations with the Commonwealth in relation to the COVID-19 testing of Patients and the administration of the COVID-19 vaccine (including requirements to comply with the Privacy Act). In addition, ACCHSs are incorporated Aboriginal organisations initiated by and based in local Aboriginal communities, and they deliver a holistic and culturally appropriate health service to the community. We understand that ACCHSs are existing healthcare providers, with staff members also subject to professional obligations.

12.5 As such, Health should be able to expect that these entity types will be used to dealing with the full range of individual Patients who may wish to receive a COVID-19 vaccine in Phase 1b, and also will be knowledgeable about the importance of protecting Patients' privacy.

12.6 Nevertheless, implementation of the measures recommended in the Original PIA report (as described in paragraph 12.3 above) will provide further protections to support the appropriate handling of personal information by these new types of Vaccine Providers.

12.7 In addition, during Phase 1a, there were no Vaccine Providers that operated their business as a sole trader. Given the nature of general practice, we anticipate that there will be few, if any, GPs who will be Vaccine Providers operating as sole traders. However, for any such Vaccine Providers, information that is about the Vaccine Provider or its business may be personal information about the individual who is operating the business.

12.8 In Phase 1b, it will therefore be important to ensure that Privacy Notices are drafted to take account of this fact, and we note that the Privacy Notices referenced in this PIA Update report which are directed to the personnel of Vaccine Providers do this.

New categories of Patients

12.9 In addition, we note that some of the population cohorts that will receive vaccines in Phase 1b are more likely to include individuals who are particularly vulnerable, and may need additional supports to ensure they are able to understand how their personal information will be handled (and provide consent where applicable). This includes, for example, elderly Patients and those with an underlying medical condition (including a disability), which we understand includes 16 and 17 year old individuals who meet eligibility criteria as part of this cohort.

12.10 We understand that some of these new ICT components and associated privacy notices will be displayed or provided in English only, whilst others will be translated into up to nine languages. 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 may include:

12.10.1 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

12.10.2 making interpreting services freely available.

(**Recommendation 2**)

Collection of personal information from Patients aged 16 and 17

12.11 We note that in Phase 1b there may be some Patients who are under 18 years of age, for example if they have a serious medical condition, have a disability, or work in one of the nominated industries.

12.12 Health intends that children aged 15 years or younger will only become eligible in Phase 3 (regardless of whether they meet other eligibility criteria for other Phases of the Vaccine Strategy), as the COVID-19 vaccines are not yet approved for individuals aged under 16 years. These individuals will not be permitted to use automated processes such as the Register Your Interest solution.

12.13 However, Health considered (in parallel with this PIA Update process) whether older children aged 16 or 17 years should be able to access and use the BP to obtain an appointment for vaccination in their own right, or whether another coordinated method of making a booking should be implemented for these individuals.

12.14 Stakeholders, particularly the OAIC, stressed the importance of protecting the privacy of young individuals, and noted that some individuals who are 16 or 17 are likely to have the capacity to provide valid consent, but others may not have that capacity and would therefore require a parent or guardian to provide that consent on their behalf.

12.15 As the numbers of individuals in this age bracket may not be very large for Phase 1b (there will be greater numbers of Patients under 18 during the implementation of Phase 2), we understand that Health has decided that any Patients who are under 18 will not be able to use automated processes such as the BP to make an appointment, and is currently developing a tailored pathway for these Patients instead.

12.16 As part of developing this tailored pathway, we suggest that Health should consider, as soon as possible but certainly in time for the implementation of Phase 2a:

12.16.1 developing tailored communication and explanatory materials for this age bracket, to ensure that older children who are Patients are able to understand and communicate valid consent[6]; and

12.16.2 implementing alternative processes that are specifically designed for Patients under the age of 18, such as tailored booking services which will provide an opportunity to assess capacity and to provide targeted information (see **Recommendation 2**).

[6] Health may wish to consider other tailored communications or approaches that have, or are being, considered or developed for older children (such as for the My Health Records system).

Section B Introduction of the COVID-19 Vaccine Administrative System (CVAS)

13. Project Description

13.1 The COVID-19 Vaccine Administrative System (**CVAS**) is a digital vaccine ordering and inventory management system, based on Health's existing Vaccine Administrative System (**VAS**).[7] We understand that the CVAS:

13.1.1 will increase the scale and speed of the logistics involved with the roll-out of the COVID-19 vaccines;

13.1.2 is the central mechanism for onboarding entities to become Vaccine Providers as part of the COVID-19 vaccine rollout (and we understand that only Vaccine Providers that have been onboarded to CVAS will be able to receive supplies of the COVID-19 vaccines (unless they became Vaccine Providers as part of Phase 1a of the Vaccine Strategy, i.e. hospital hubs or jurisdictional sites)); and

13.1.3 will serve as a checkpoint for Vaccine Providers to identify, when they register their vaccination site, if they do not have an existing online booking platform and if they wish to use the BP (see further discussion of the BP in **Section D**).

13.2 The CVAS will be used by Vaccine Providers, but not by Patients or any other members of the public.

Before onboarding of Vaccine Provider

13.3 To onboard Vaccine Providers to the CVAS, we understand that the following has occurred:

13.3.1 As part of the expression of interest (**EOI**) process[8] to engage GPs as Vaccine Providers for Phase 1b of the Vaccine Strategy, Vaccine Providers were requested to provide certain information to Health (for consideration by Health and Primary Health Networks (**PHNs**)), including:

(a) the name of the legal entity, and the trading/business name;

(b) the ACN/ABN (as applicable);

(c) the registered address or address of principal place of business;

(d) the shipping address (if different to the registered address or address of principal place of business);

(e) the name, position title, and contact details (such as email address and telephone number) of a contact person or persons (we understand these personnel have been nominated as the primary contacts and potentially, secondary contacts for the delivery of vaccines and related products to the Vaccine Provider) (**Delivery Contact**)[9];

[7] The VAS is Health's existing system for procuring and distributing vaccines to States and Territories, and facilitating management of supply chains for all vaccines procured by the Commonwealth under the National Immunisation Program (**NIP**) including forecast, order, delivery and financial management as well as reporting national vaccine procurement and distribution to State and Territory health departments.
[8] We have only considered this process to the extent that the EOI Information flows into the CVAS and other systems discussed in this PIA Update.
[9] This contact is referred to as the 'Distribution Contact' in the CVAS Privacy Notice.

(f) the name and email address of a 'Notice Representative' (**Notice Contact**) (which we understand will be the contact for general notices to the Vaccine Provider); and

(g) the number of full-time equivalent GPs available at that site.

(together, **EOI Information**).

13.3.2 We understand that there was also a request for information process to determine suitable GPRCs and ACCHSs that will also be Vaccine Providers. The GPRCs are already providing COVID-19 testing services under a contractual arrangement with Health, and Health worked closely with the National Aboriginal Community Controlled Health Organisation (NACCHO) to conduct the request for information process with ACCHSs. We have assumed that Health collected, or already held, information equivalent to the information described for GPs in paragraph 13.3.1 above. In this PIA, this previously collected information about GPRCs and ACCHSs is also 'EOI Information'.

13.3.3 We understand that Health, in conjunction with PHNs,[10] has determined which Vaccine Providers are eligible to administer COVID-19 vaccines for Phase 1b, and through the relevant PHN, an email was sent to the Vaccine Provider's email address provided as part of the EOI Information with onboarding documents for the CVAS that included the Vaccine Provider's 'Cohort Registration Code', and a unique URL to access the CVAS.

13.3.4 Once the Vaccine Provider's cohort is ready to be onboarded to the CVAS, Health will send another email to the Vaccine Provider with the Vaccine Provider's specific 'Site Registration Code'.

13.3.5 Key information from the EOI process, such as site capacity for vaccine storage and site details (e.g. site address) were pre-loaded into the CVAS ahead of Vaccine Providers being onboarded to the CVAS.

13.3.6 In addition, to prepare for onboarding Vaccine Providers to the CVAS, the relevant identifier for the Vaccine Provider (as specified below) was pre-loaded into the CVAS from the EDW:

(a) for Vaccine Providers that are not GP clinics[11], this is – their AIR provider number; and

(b) for Vaccine Providers that are GP clinics, this is a unique identifier (**Site Identifier**) generated by Health's EDW, which is created by combining the GP clinic's Practice Incentives Program (**PIP**) number with their PIP Location ID[12].

13.3.7 We understand that when a Vaccine Provider creates an account in CVAS, they are required to confirm their site shipping address, which is used to match the relevant identifier for the Vaccine Provider (i.e. either the AIR provider number of the Site Identifier) to the Vaccine Provider.

Vaccine Provider registers account in CVAS

13.4 To onboard and use the CVAS, Vaccine Providers will need to register an account to use the CVAS to place orders for a vaccine, as follows:

[10] We note that the EOI form clearly indicated that EOI Information would be held and used by both Health and PHNs.
[11] We note that these entities are already Vaccine Providers under Phase 1a.
[12] We understand that the Site Identifier generated by combining a Vaccine Provider's PIP number and PIP Location ID is a site-specific identifier and cannot be used to identify a relevant Vaccine Provider, even if the Vaccine Provider is a sole trader (e.g. a sole practitioner).

13.4.1 Vaccine Providers will register an account for their site (the CVAS operates on there being an account for each site at which a vaccine can be administered, as opposed to needing an account for each Vaccine Provider or Vaccinator), and will be onboarded onto the CVAS.

13.4.2 Vaccine Providers are able to register an account for their site in the CVAS by using the unique URL and inputting both the 'Site Registration Code' and the 'Cohort Registration Code). The Vaccine Provider will then need to review and confirm some EOI Information (such as their site address and details of their Delivery Contacts). At this point, they may update the details of their Delivery Contacts (such as their names and contact details). We understand this information may be used by the Delivery Partners upon delivering vaccines to the Vaccine Provider.

13.4.3 At this stage, Vaccine Providers will be asked whether they have an existing online booking platform, and if they enter yes, they will be requested to specify the booking platform.

13.4.4 For completeness, we understand that in the future, Vaccine Providers will be requested to enter their specific booking platform URL if they have an existing online booking platform.[13]

13.4.5 We also understand that in the future, to register their account, Vaccine Providers will then be asked to provide public facing contact details and information for inclusion in the Vaccine Clinic Finder (see further discussion of this system in paragraph 17.8 of **Section D**). We understand that this information may include information about the clinic (such as the clinic's classification, name and contact details), and the clinic's opening hours.[14]

After Vaccine Provider has been onboarded to, and uses, the CVAS

13.5 We understand that Vaccine Providers will be prompted to complete a 'Site Readiness Checklist and Declaration' when they log in to the CVAS for the first time. They will be required to confirm site information (including the clinic name, site address, and organisation responsible for the site) and to enter the name and role or title of the signatory to the declaration.

13.6 We understand that when using the CVAS, Vaccine Providers may enter identifying information as follows:

13.6.1 When creating a new order, the name and position of the Vaccine Provider's Delivery Contact who will take receipt of the order may be entered.

13.6.2 When confirming the Vaccine Provider's acceptance of a vaccine delivery, Vaccine Providers must provide:

(a) the name of the delivery person (if known) and the delivery company (i.e. the Logistics and Distribution Partner); and

(b) the name, position and phone number of the Delivery Contact who will take receipt of the order.

13.6.3 When reporting a wastage incident that involves 5 or more vials at one time, Vaccine Providers must provide the name, position and phone number of the person submitting the report.

[13] As this has not occurred as at the date of analysis of this PIA Update report, we have not considered this as part of this PIA Update process.
[14] As this has not occurred as at the date of analysis of this PIA Update report, we have not considered this as part of this PIA Update process.

13.6.4 When reporting weekly stock levels and usage and wastage, Vaccine Providers must provide the name, position and phone number of the person submitting the report.

General information related to the CVAS

13.7 A link to a Privacy Notice (a document titled *Privacy notice for COVID-19 vaccination providers using our ordering and inventory management system*) is displayed to users when entering information for a Vaccine Provider. We understand that the relevant Delivery Contact's information (together with details of the vaccines ordered) is extracted by Accenture (as the Data Partner, under the Data Partner Contract) from the CVAS, which is temporarily stored on an Accenture personnel's laptop. We understand that Accenture then sends this information via email to Health, which in turn sends via an encrypted email this information to the Logistics and Distribution Partners (Linfox and DHL), who have the required decryption key.

13.8 We understand that Accenture (as the Data Partner) extracts this information in two separate processes, one related to deliveries by DHL and one related to deliveries by Linfox, and we also understand that the Accenture personnel deletes this information from their laptop after 1-2 days (it is retained for this period in case there are any questions about the order for vaccines during that time).

13.9 We also understand that this is intended to be a temporary measure only and that, in the future, Health intends on implementing system-to-system integration, that will allow for order information to be directly transferred from the CVAS to the Logistics and Distribution Partners' systems (so this information will not need to be sent via email).

13.10 The CVAS uses a solution built by the Data Partner under its Partner Contract, hosted on cloud services provided by Salesforce.

13.11 We understand that:

13.11.1 the CVAS will receive information from the EDW as discussed above (but information will not flow from the CVAS to the EDW); and

13.11.2 some information in the CVAS is transferred to the Vaccine Data Solution (**VDS**). We understand that currently extracts of vaccine orders are transferred from the CVAS to the VDS (which include AIR provider numbers and Site Identifiers, and details relating to the order), however Health does not intend that any personal information about individuals such as contact names or contact details will be transferred.

14. Privacy impact analysis and compliance

14.1 The introduction of the CVAS will mean that:

14.1.1 Health will **use** personal information already collected about Vaccine Providers and their Provider Personnel (including through the EOI processes for GPs and ACCHSs, and the existing contractual relationships with GPRCs) to:

(a) create and populate an account for the Vaccine Provider in CVAS;

(b) determine the relevant AIR provider number, or establish a random Site Identifier, for the Vaccine Provider (including using the Vaccine Provider's PIP number and PIP Location ID);

(c) otherwise contact the Notice Contact to administer the CVAS, or the Delivery Contacts if needed in connection with the implementation of the Vaccine Strategy; and

(d) operate the CVAS (by allowing Vaccine Providers to order COVID-19 vaccines);

14.1.2 Health may **collect** additional personal information in the CVAS:

(a) if the Notice Contact enters further personal information into the CVAS (e.g. about a new Delivery Contact);

(b) when a Vaccine Provider Personnel signs the 'Site Readiness Checklist and Declaration';

(c) when a new order is placed, which will include collection of:

(i) information about the Delivery Contact; and

(ii) information about the relevant Logistics and Distribution Partner's personnel;

(d) if a Vaccine Provider Personnel submits a wastage incident report; and

(e) when a Vaccine Provider Personnel submits stock levels and usage and wastage reports;

14.1.3 Health will **disclose** personal information about Delivery Contacts to the Data Partner and to Logistics and Distribution Partners;

14.1.4 PHNs may **use** personal information about Notice Contacts to send onboarding information and access codes to the Notice Contact (if the Notice Contact's email address, as opposed to the Vaccine Provider's general email address, will be used), to allow them to finish setting up a CVAS account for the Vaccine Provider; and

14.1.5 Health may **disclose** additional personal information to its Data Partner, if the Data Partner accesses that information in the course of providing ICT services (e.g. support services).

14.2 We understand that, at this stage, no personal information will be transferred from the CVAS to the VDS. If personal information will in future be transferred to the VDS, we **recommend** (in accordance with **Recommendation 1** of the Original PIA report) that Health consider the privacy impacts of that development, and whether any additional mitigation strategies are required, before those changes are implemented (**Recommendation 1**).

Transparency regarding the handling of personal information

14.3 The CVAS only collects and uses limited information that is personal information about individuals, such as name and work contact details, and does not collect or use any sensitive information (as defined in the Privacy Act). However, we still consider it important that those individuals whose personal information is collected in the CVAS (including individuals who are Notice Contacts and Delivery Contacts for a Vaccine Provider, and any Vaccine Providers who are operating as sole traders) are made aware that their personal information is being collected, and how their personal information will be handled.

14.4 In addition, when completing the EOI process, Vaccine Providers were required to declare the following:

> *Do you also acknowledge that the data from this expression of interest will be held by the Department of Health and the Primary Health Network for the purpose of informing the COVID-19 vaccination program roll-out. It may be provided to 3rd parties (such as vaccine delivery partners) as relevant. Your data will not be used beyond this purpose without your knowledge.*

14.5 Although it does not specifically reference use of the information in connection with the CVAS (or any ordering system more generally), this wording may have assisted in making Vaccine Providers generally aware that Health may further use and disclose the information provided in connection with Phase 1b.

14.6 We consider that it is a privacy-enhancing feature (consistent with Health's obligations under APP 1 and 5) that the CVAS has been designed to display a link to the Privacy Notice to individuals who are using the CVAS, which clearly explains how personal information is collected, used, stored and disclosed in connection with the operation of the CVAS. We understand that a link to the Privacy Notice is also available on the privacy page for the Vaccine Strategy on the Health website.

14.7 In our view, the Privacy Notice clearly explains how personal information will be collected, used, stored, and disclosed in relation to the CVAS.

14.8 We do acknowledge that the condensed timing of the roll out for Phase 1b meant that the Privacy Notice needed to be drafted while details of the relevant ICT systems were being fully developed. We **recommend** that the Privacy Notice be reviewed and updated to:

14.8.1 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');

14.8.2 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);

14.8.3 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);

14.8.4 ensure the role of the Data Partner in handling personal information is clear (including its role in transferring information (which includes information in relation to Delivery Contact) from the CVAS to the Logistics and Distribution Partners); and

14.8.5 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.

(**Recommendation 3**)

14.9 We note that the Privacy Notice does not expressly explain to individuals what the consequence will be if their personal information is not collected by the CVAS (i.e. initially, the Vaccine Provider will not be able to complete the account establishment process and commence ordering vaccines, or to place their order after establishment). However, we suggest that this should be obvious to the user (as they will technically be unable to complete the onboarding process or place the order without completing all relevant fields).

14.10 In addition, the Privacy Notice does specify that if an individual needs to access or correct their personal information in the CVAS, the individual can access the CVAS to make amendments, or can call the Vaccine Operations Centre (**VOC**) if they require further assistance. However, technically APP 5.2(h) requires that the individual be informed that the APP privacy policy contains information about how the individual can access or correct their information. Again, we note that Health's privacy policy is clearly referenced in the Privacy Notice, but the drafting could perhaps be updated to reflect this.

14.11 Finally, we suggest that Health could consider updating its Privacy Notice to name Accenture Pty Ltd (**Accenture**) as the contracted ICT service provider responsible for managing and operating the CVAS, and Salesforce as the relevant cloud service provider for the CVAS platform. We consider this would further increase transparency regarding the CVAS and therefore enhance Health's compliance with APP 1.

14.12 While we do not consider any of these matters to be essential (noting that APP 5 only requires Health to notify or make individuals aware of such APP 5.2 matters as is reasonable in the circumstances), if Health decides to implement **Recommendation 3**, it may also wish to take the opportunity to consider adding wording to address these additional matters.

Collection of additional personal information

14.13 Additional personal information (not sensitive information) will be collected by Health at the time, or after, a CVAS account is established by the Vaccine Provider (e.g. new or changed information about a Delivery Contact or Notice Contact, and new information about Vaccine Provider Personnel (such as the individual submitting various reports)). This collection must comply with APP 3, in that it must be reasonably necessary for, or directly related to, Health's functions or activities in order to comply with APP 3.1. We are satisfied that collection of up-to-date contact details in order to ensure effective ordering and delivery processes of vaccines is reasonably necessary for implementation of the Vaccine Strategy, which is part of Health's functions and activities.

14.14 In addition, some of the additional personal information that is entered into CVAS may be collected from someone other than the individual. APP 3.6 does allow collection from someone other than the individual concerned where it is unreasonable or impractical to collect it from the individual (APP 3.6(b)). In the circumstances of a national roll-out, and given the nature of the personal information collected, we are satisfied that it would be impractical and unreasonable to require Health to collect the information directly from each Notice Contact or Delivery Contact which is nominated by a Vaccine Provider.

14.15 We also note that as part of the CVAS, Health will collect personal information (but not sensitive information) about Logistics and Distribution Partner personnel. We understand that this will be limited to the name of the delivery person, if this is known by the relevant Vaccine Provider Personnel inputting information related to acceptance of a vaccine delivery. We understand that this information will assist with Health's accountability responsibilities and audit processes in case there are any issues related to a delivery.

14.16 Given it is not mandatory for Vaccine Provider Personnel to ask for this information and accordingly report it into the CVAS, it raises the question of data minimisation and whether this information is required by Health (given that it is reasonable to assume that the Logistics and Distribution Partners will also have their own systems to record which of its personnel delivered certain vaccines. Accordingly, we suggest that Health consider whether this information is required in the CVAS, and if it determines it is not reasonably necessary to its functions and activities, remove this data field from the CVAS system.

Access to personal information by ICT service providers

14.17 It is apparent that the personal information stored in the CVAS can be accessed by the Data Partner, or other third party service providers.

14.18 We note that the Privacy Notice specifies that:

> *'Our ICT service providers responsible for managing and operating the CVAS may also have access to information stored in the CVAS for system maintenance and upgrades, but they must meet our strict requirements for privacy, confidentiality and security'.*

14.19 We understand that Accenture, as the contracted Data Partner, is responsible for providing ICT support services in respect of the CVAS. Accordingly, we **recommend** that Health ensure (through seeking assurance from its legal adviser, as appropriate) that the robust general privacy and security obligations in its contractual arrangements with Accenture, as applicable to the specific services involved in the implementation and operation of the CVAS, continue to remain suitable (**Recommendation 4**). We note that this is consistent with **Recommendation 4** of the Original PIA report.

14.20 In addition, it is possible that personal information may also be accessed by Salesforce as the cloud services provider of the CVAS platform (for example, to provide ICT support services). We note that these companies have a degree of foreign ownership and there may be some community concern that foreign laws may require such companies to disclose personal information to a foreign government. For example, the *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**) is an American law that allows US federal law enforcement agencies to compel certain companies, including cloud service providers, to produce data stored on servers they own, irrespective of whether the data is stored in the USA and even if the data is owned by, and stored on behalf of a customer. We consider that there is only a low risk that a US enforcement agency would seek, via a US court order, to gain access to personal data in the CVAS (noting the limited amount of personal information held).

14.21 Again, we suggest that having robust contractual arrangements in place with Salesforce which impose suitable privacy and data security obligations, and which enable Health to maintain effective control of data stored on the CVAS platform, and communicating this via the Privacy Notice, will assist in alleviating potential concerns about the involvement of these companies (**Recommendation 4**).

Security of personal information in the CVAS

14.22 It is important that when collecting and storing personal information in the CVAS (including when EOI Information is transferred into the CVAS), Health can demonstrate that it has taken all reasonable steps to protect the personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. This will assist Health to comply with its obligations under APP 11 in relation to the security of personal information.

14.23 We have not been able to determine all of the mechanisms that will be used to protect personal information (e.g. how EOI Information will be uploaded into the CVAS).

14.24 Again, we stress the importance of Health ensuring that its contractual arrangements with the Data Partner responsible for designing, building, and operating the CVAS solution contain appropriate obligations, so that the solution will be appropriately secure and protected against unauthorised access (**Recommendation 4**).

Disclosure of personal information in the CVAS to the Logistics and Distribution Partner

14.25 As discussed in paragraphs above, we understand that personal information will be extracted from the CVAS about Delivery Contacts by Accenture (and this information will be stored on an Accenture personnel's laptop), which will then disclose (via email) this information to Health, which will then disclose (via email) this information to the Logistics and Distribution Partners.

14.26 In our view, this handling of personal information seems likely to involve an enhanced risk of errors occurring (given the manual extraction process), as well as representing an additional point of access to personal information when stored on the laptop (the portability of laptops means they may be more easily misplaced or stolen). We are concerned there may be an increased potential for loss or unauthorised access to the personal information that is extracted from the CVAS.

14.27 We therefore **recommend** that, prior to disclosing any personal information in the CVAS to the Logistics and Distribution Partners, Health ensure that:

14.27.1 it has taken all reasonable steps to ensure that the mechanisms for transferring information to the Logistics and Distribution Partners are secure, so that the personal information is 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). In particular, we **recommend** that the temporary arrangements that have been established be re-examined as soon as possible, to reduce the enhanced potential for loss or unauthorised access (**Recommendation 5**); and

14.27.2 it is satisfied that its contractual arrangements with the Logistics and Distribution Partners contain appropriate obligations to require the Partners to protect personal information (this will also assist Health to comply with its obligations under APP 11) (**Recommendation 4**).

Transfer of information to the VDS

14.28 We understand that the CVAS and VDS will not be integrated as such, but that some information will nevertheless be transferred from the CVAS to the VDS (where it will be used for analysis and reporting purposes, as described in the Original PIA). The Privacy Notice states that the information to be transferred to the VDS will not include any personal information.

14.29 If personal information will in future be transferred to the VDS, we **recommend** (in accordance with **Recommendation 1** of the Original PIA) that Health consider the privacy impacts of that development, and whether any additional mitigation strategies are required, *before* those changes are implemented (**Recommendation 1**).

14.30 We particularly note that, if in future any personal information will be transferred to the VDS from the CVAS, the contractual arrangements with all third party providers who will or may have access to that personal information, will need to be drafted appropriately to cater for such potential access.

Section C Introduction of the 'Register your Interest' (RYI) solution

15. Project Description

15.1 The relevant systems for the RYI solution have been developed by Accenture as the contracted Data Partner. The RYI solution involves individuals entering their personal information (including sensitive information) into a new webpage so that they can be notified when they become eligible to make an appointment to receive a COVID-19 vaccine, based on the information they have provided.

15.2 To register their interest, members of the public first need to complete the 'Eligibility Checker', which is a tool on a website run by HealthDirect Australia (**HealthDirect**), a national, government-owned, not-for-profit organisation.

15.3 The Eligibility Checker on the HealthDirect website requires the individual to input their age and State or Territory, and answer questions about whether they are employed in a particular type of work, whether they are a resident of an aged care or disability care facility, whether they have one or more particular underlying medical conditions including a disability, and their Indigenous status. The Eligibility Checker can be completed by the individual concerned, or by another person acting on their behalf.

15.4 As some of this information may include information about their health, disability, or ethnic origins, this may include information which, if the individual can be identified, will be sensitive information.

15.5 After completing the Eligibility Checker and receiving advice about the implementation Phase in which they will be eligible to receive a vaccine, the individual may, if they are eligible for a vaccination in Phase 2a or Phase 2b[15] of the Vaccine Strategy only, be invited to proceed to the RYI solution to register their interest and be notified when Phase 2a has commenced.

15.6 A link is displayed to the completing individual in order to transfer them to the RYI solution. Before the link is the following text:

> *If you would like to register for a notification, we will need to collect your eligibility responses and contact details. If you submit information on behalf of someone else, you must be their parent/legal guardian or have their permission to do so.*

15.7 We understand that no information entered into the Eligibility Checker is collected unless and until the individual proceeds to the RYI solution by clicking on the link displayed.[16]

15.8 Individuals who click on the link to proceed will be taken from the Eligibility Checker to a new webpage where they will be asked to input their:

15.8.1 first and last name[17];

15.8.2 State or Territory;

15.8.3 postcode; and

[15] For clarity, if the Eligibility Checker determines that an individual will only be eligible in Phase 3, an option to register their interest will not be displayed.
[16] We agree with submissions provided by the OAIC that, if the Eligibility Checker were to collect (i.e. include identified personal information in a record) and store personal information even if the individual did not choose to proceed to the RYI solution, they should be informed about this before being asked to enter details into the Eligibility Checker. However, we understand that this is not the case, including because the individual completing the Eligibility Checker cannot be identified unless and until they submit their details into the RYI solution.
[17] We understand that individuals are able to use a pseudonym when using the Eligibility Checker, but are not notified they are able to do so.

15.8.4 mobile phone number and/or email address.

15.9 If the individual selects to continue to the RYI solution, the individual's previous responses to the Eligibility Checker questions will also be collected by the RYI solution and displayed to the individual (if a drop down icon is selected).

15.10 The webpage contains the statement:

> *If you submit information on behalf of someone else, you must be their parent/legal guardian or have their permission to do so.*

15.11 It also notes:

> *We will keep your eligibility responses and contact details so we can notify you when it is your turn to book a vaccine. For more information on how we handle your personal details see the Privacy Notice for Register Your Interest.*

15.12 The Privacy Notice explains that personal information is being collected in order for the individual to be notified when they become eligible to make an appointment to receive the COVID-19 vaccine.

15.13 The collected information will be stored in a secure cloud services platform provided by AWS, under a contractual arrangement with Health (the **RYI platform**). Accenture, as the contracted Data Partner, will have access to the personal information held on the RYI platform, to provide support services (i.e. system maintenance and upgrade purposes) in accordance with contractual arrangements.

15.14 Health intends to engage a provider to provide notification services to Health (**Notification Provider**). The role of the Notification Provider will involve sending the notifications to individuals who have provided their contact details using the RYI solution:

15.14.1 when they become eligible to make an appointment to receive a COVID-19 vaccine; or

15.14.2 in other situations where it may be important to notify individuals about the availability of COVID-19 vaccines, such as if excess doses of the vaccine are available in or near the individual's postcode and Health decides it would be beneficial to contact the individual and advise them to make an appointment to receive the vaccine (such as to avoid wastage of the vaccine doses).

15.15 We understand that Health is considering how personal information will be handled by the Notification Provider and how to ensure that only information required for the notification will be provided by Health to the Notification Provider. We also understand that Health intends for this information to be disclosed either via a secure link (such as an upload) or via a secure API, and that the information is to be deleted by the Notification Provider at an agreed later date. Health will then retain the only copy of the RYI personal information.

15.16 When Phase 2a commences, the Notification Provider will use its existing IT solutions and the information received from Health to send a notification to the contact details provided by individuals. If required by Health, the Notification Provider will send additional notifications to individuals who have provided a particular postcode.

15.17 Once an individual is notified that they have become eligible to make an appointment, they will need to either go through the Eligibility Checker again, or go directly to the National Health Services Directory (also run by HealthDirect), to make an appointment with their chosen Vaccine Provider (i.e. no information from the RYI solution will be transferred to or populated in any appointment booking system, including the BP).

15.18 We understand that, if States or Territories request information from Health, Health may disclose aggregate information collected by the RYI solution to States and Territories. We understand that disclosure of aggregate information to States and Territories may include, for example, information about the number of people registered in that jurisdiction who

identify as Aboriginal and/or Torres Strait Islander, and information relating to the ages of people who registered in that jurisdiction. However, Health does not intend to disclose personal information, and intends to provide de-identified aggregate data only. Health should undertake assurance activities to ensure that any aggregated information is properly de-identified, including so that there is a very low risk of re-identification.[18] In addition, the provision of aggregate reports to the relevant State or Territory should only be for the purpose of supporting the effective implementation of the Vaccine Strategy (e.g. because it is required in order to manage interest in vaccinations against known stock levels).

15.19 In future, we understand that it is contemplated that the RYI solution may transfer some personal information to the EDW, or potentially transfer some information collected by the RYI solution into other systems, however we understand that no personal information in the RYI solution will be shared with the VDS. Before any information is transferred to the EDW, Health intends to update the Privacy Notice, and may take other steps as reasonable to notify relevant individuals.

15.20 For completeness, we note that the website used for the RYI solution collects cookies (small files stored on an individual's device) created both by Health and third parties. These cookies allow Health to recognise an individual web user as they browse Health's website. The cookie identifies the individual's browser or device, and not the individual personally. We understand that no personal information is stored within cookies used by Health's website. The information collected includes:

15.20.1 the individual's server and IP address;

15.20.2 the name of the top level domain (for example, .gov, .com, .edu, .au);

15.20.3 the type of browser used;

15.20.4 the date and time the website was accessed;

15.20.5 how the individual interacted with Health's website; and

15.20.6 the previous website the individual visited.

15.21 We understand that Health uses the above information to understand how its websites are being used, in order to improve these websites and provide users with a better experience.

16. Privacy impact analysis and compliance

16.1 The introduction of the RYI solution will mean that:

16.1.1 Health will **collect** information entered into the Eligibility Checker when the individual navigates to the RYI solution website;

16.1.2 Health will **collect** the name and contact details entered by the individual into the RYI solution;

16.1.3 Health will **use** the collected information by storing it in the RYI platform;

16.1.4 Health will **disclose** the collected information to the Notification Provider (and there will be a corresponding **collection** by the Notification Provider); and

16.1.5 the Notification Provider will **use** the collected information to send a notification to the relevant individual;

[18] Health should ensure its de-identification processes are consistent with OAIC guidance on *De-identification and the Privacy Act*, and the *De-identification Decision-Making Framework* (produced jointly by OAIC and CSIRO's Data61.

16.1.6 Health may **use** the collected information to de-identify it, and **disclose** the de-identified aggregate information to States and Territories.

16.2 In the above, we have analysed the entity that is collecting, using and disclosing the relevant information as Health, rather than Accenture as the Data Partner, or AWS as the cloud services provider of the RYI platform. This is because we understand that it is clearly intended that Health, rather than the other entities, will have effective control over the stored personal information. As discussed in detail in relation to the CVAS and CVIP systems (see **Section B** and **Section E**), it will be important that the contractual relationships with the Data Partner and with AWS reflect this intention.

16.3 Health is procuring a cloud services platform from AWS. We understand that Health will be holding all information it collects (including personal and sensitive information) on the platform[19]. Therefore, we suggest Health takes steps to ensure that the relevant contractual arrangements with AWS contain appropriate privacy and security obligations (including in relation to storage in Australia and limitations on access from overseas etc) (see **Recommendation 4**).

Making individuals aware of collection of information

16.4 Because sensitive information will be collected, APP 3.3 requires that consent be obtained from the relevant individual (noting that no exception in APP 3.4 seems likely to apply).

16.5 We consider that various privacy-enhancing features have been built into the design of the RYI solution to ensure that consent from the relevant individual is provided, and that it is appropriately informed and specific. For example:

16.5.1 individuals are told that their personal information will be collected if they proceed to the RYI solution, before they are taken to the RYI solution;

16.5.2 the placement of the reference to the collection of personal information in the RYI solution, and the clear link to the Privacy Notice, is displayed reasonably prominently (taking into account the design of the page and consistently with typical user expectations about where they might expect to find privacy information), and before personal information is submitted;

16.5.3 the Privacy Notice contains clear explanations about what personal information is collected, why it is collected, and how it will be used, stored, and disclosed, including that their personal information:

(a) will be collected and used by both Health and the Notification Provider, to contact them when they are eligible to make an appointment (and if applicable, that this may include during situations when there are excess doses available in area in or close to the postcode they have nominated); and

(b) may be accessed by Health's Data Partner (Accenture) or other ICT service providers, but that they are bound by strict privacy, confidentiality and security obligations; and

16.5.4 the information displayed on both the Eligibility Checker and RYI solution webpages clearly indicates that there is no compulsion to register details (assisting to ensure that the consent obtained is voluntary).

16.6 These features will assist in ensuring that consent, which can be implied from the actions of the individual in submitting their information, is properly informed.

[19] See also the discussion in paragraph 14.20 in relation to potential community concerns about foreign laws, such as the US CLOUD Act, which may require companies with foreign ownership to disclose data to foreign governments, which may also apply in relation to AWS' involvement.

16.7 We also note that features have been included to accommodate the situation where someone other than the relevant individual inputs information on their behalf. To assist with compliance with APP 3.6 (which provides that information must be collected from the individual concerned, unless there is consent, or authorisation by law, or it is unreasonable or impracticable to do so), the website clearly references the need for the individual concerned to have given their permission for their details to be provided.

16.8 We note that if an age under 18 is entered into the Eligibility Checker, no option to proceed to the RYI solution will be displayed (which we consider to be an appropriate feature).

16.9 There may be potential to further improve the RYI solution at a later stage. For example the website could include 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*') (**Recommendation 6**).

Data minimisation principle

16.10 The minimum amount of information that is reasonably necessary to notify the individual that they are eligible to make an appointment should be collected.

16.11 We consider that collection of either or both of a phone number and email address of the individual is reasonably necessary to ensure that they can be effectively notified, and that this falls within Health's functions and activities.

16.12 We note that Health also collects the individual's postcode and State/Territory. The Privacy Notice explains that this information is reasonably required in order to ensure that individuals can be notified if excess doses of vaccine become available in their area. On this basis, we consider this to be reasonably necessary for Health's functions and activities of ensuring that valuable COVID-19 vaccines are not unnecessarily wasted. We do not think that mere collection of a postcode is sufficiently granular to represent collection of specific location information that is likely to be an unreasonable intrusion into the individual's privacy.

16.13 We note that the OAIC suggested that the RYI webpage could include a 'pop-up' message beside each field that needs to be completed, which explains why the collection of the information is reasonably necessary. While we agree that this (or inclusion of other explanatory wording on the website) would be a privacy-enhancing feature, we do acknowledge the need to balance the benefits against the risk of 'information overload' for users and the costs of implementation (**Recommendation 6**). We do note that the explanations are included in the Privacy Notice.

16.14 However, we do note that the Privacy Notice indicates that:

> *We may also use and disclose your details to enable your State or Territory to send you important messages about the COVID-19 vaccine.*

16.15 This appears to be inconsistent with the intention that personal information would be de-identified before being provided to a State or Territory (see paragraph 15.18 above). Accordingly, we **recommend** that the Privacy Notice for the RYI solution be updated to accurately reflect the potential disclosure to, and use by, a State or Territory body of such personal information (**Recommendation 3**).

16.16 We also note that Health has acknowledged that submission of an individual's true name is not necessary in order for Health, and the Notification Provider, to ensure that the individual receives a notification. While there is no verification or other checking of the name entered (which is consistent with APP 2), we suggest that the Privacy Notice could perhaps make this clearer (**Recommendation 3**), but note that this may need to be balanced against Health's expectation that the requirement for a true name discourages deliberate entry of incorrect information to obstruct or defeat the RYI solution's purposes.

Engagement of the Notification Provider

16.17 As at the date of analysis of this PIA Update, Health has not announced the entity selected to be the Notification Provider. Given the role of the Notification Provider in the Vaccine Strategy (i.e. contacting individuals to notify them of their eligibility status), the Notification Provider will need to collect and hold personal information. We understand that it is intended that the Notification Provider will do so in its own right.[20]

16.18 We **recommend** that Health ensure that:

16.18.1 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

16.18.2 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 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 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.

(**Recommendation 7**)

Security and quality of information

16.19 Health should be satisfied that the personal information will be securely transmitted by the Notification Provider to the intended recipients, and that the quality of the information will not be degraded during transmissions (**Recommendation 5**).

Updating information or withdrawing consent

16.20 We note that it is currently not possible for an individual to update or change the personal information they have submitted to the RYI solution, for example, if they have incorrectly inputted their details or their circumstances change (i.e. the individual turns 70), or if the individual updates their contact information. Instead, the Privacy Notice explains that an individual is required to re-register their interest (by again using the Eligibility Checker and including the correct information in this and the RYI solution).

16.21 In addition, the individual submitting information into the RYI solution cannot later decide that they no longer wish to receive a notification.

16.22 This is problematic because:

16.22.1 it is incongruous with the 'data minimisation principle', as it may mean that multiple copies of some personal (and sensitive) information may be collected and held where this is not reasonably necessary for the RYI solution's functions;

16.22.2 we see the potential for individuals to be confused if they receive an alert indicating that they are eligible for the vaccine which is based on incorrect information; and

16.22.3 in any consent model, it is important that individuals have the ability to withdraw their consent if they change their mind.

[20] While the Notification Provider will use message templates designed by Health, it will necessarily need to hold the contact details of individuals in order to populate and send the completed message templates.

16.23 Accordingly, we **recommend** that:

16.23.1 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

16.23.2 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.

(**Recommendation 6**)

Deletion of information

16.24 Given the likelihood that the personal information that will be supplied by interested individuals will only be useful while the individual is waiting to receive the vaccine, Health should only retain personal information records for a short period. We understand that Health intends that information relating to an individual will be deleted once that individual has been notified of their eligibility. Health is currently engaging with its records management team to determine the appropriate process to delete data in accordance with its usual administrative practices, and in a manner consistent with its obligations under the Archives Act.

16.25 Health should also include, in its contractual or other arrangements with the Notification Provider, a requirement for the Notification Provider to delete personal information within a specified period after the person has been contacted (i.e. four weeks after the individual has been contacted, their personal information should be deleted).

Section D Introduction of the Commonwealth-procured Booking Platform (BP)

17. Project Description

17.1 We understand that many Vaccine Providers have their own existing online booking systems to allow Patients to make appointments to receive a vaccine. In addition, some Vaccine Providers prefer to use their existing telephone booking services to allow Patients to make such appointments.

17.2 However, as part of the process to onboard Vaccine Providers to the CVAS (as discussed in **Section B**), Vaccine Providers who do not have an existing online booking solution are able to indicate whether they wish to use the Commonwealth-procured BP, to allow Patients to make online appointments with them to receive a COVID-19 vaccine.

17.3 Following a procurement process during which Health considered a number of potential arrangements, Health has entered into a contract with HealthEngine Pty Ltd (**HealthEngine**), to develop and run the BP.

17.4 If a Vaccine Provider chooses to use the BP, the Vaccine Provider will be required to notify Health, in order for Health to arrange for HealthEngine to onboard the Vaccine Provider.

17.5 The Vaccine Provider will then be onboarded to the BP, and required to accept HealthEngine's End User Terms and Conditions and sign HealthEngine's End User Services Form (together, the **End User Agreement**), which have both been tailored for the BP (and differ from HealthEngine's standard terms of use). As part of entering into the End User Agreement, the Vaccine Provider will be required to provide HealthEngine with the following information:

17.5.1 the legal name of the Vaccine Provider entity, and other entity-related information (such as the Vaccine Provider's ABN);

17.5.2 the address of the Vaccine Provider's site; and

17.5.3 the full name, phone number, and email address of a primary contact for the Vaccine Provider (**Primary Contact**).

17.6 If a Vaccine Provider would like Patients to be able to make available appointments with specific individual health professionals (i.e., Vaccinators) in the BP, the Vaccine Provider's Primary Contact will need to provide the names of those Vaccinators to HealthEngine. We understand that the Vaccine Provider will then be able to make and manage times for appointments with those Vaccinators in the BP.

17.7 We understand that before a Patient makes an appointment using the BP, they must first complete the 'Eligibility Checker' to determine that they are eligible to book an appointment to receive a COVID-19 vaccine. If the Eligibility Checker determines that the Patient is eligible, they will be invited to search for their preferred Vaccine Provider via the Vaccine Clinic Finder (which is run by HealthDirect and based on the existing National Health Services Directory model[21]) in order to make an appointment to receive a COVID-19 vaccine.

17.8 The Patient will then be directed to the Vaccine Clinic Finder and, after entering their postcode or suburb name, the Patient will be asked to select their preferred Vaccine Provider from a list.

[21] The Vaccine Clinic Finder is not part of the ICT systems examined by this PIA Update (we understand that no personal information is collected by this tool).

17.9 The Patient will then be asked to select their preferred Vaccine Provider by clicking on a link to make a booking with that Vaccine Provider. We understand that one of the following may then occur:

17.9.1 if the selected Vaccine Provider has chosen to use their own existing online booking system (including the mainstream HealthEngine solution), the Patient will be taken to that booking system;

17.9.2 if the selected Vaccine Provider has chosen to use the BP, the Patient will be taken to the BP; or

17.9.3 if the selected Vaccine Provider does not have an online booking system in place (and has not opted to use the BP), there will be no link available to make an online booking and only a phone number will be displayed. The Patient may then call the Vaccine Provider using the number specified.[22]

17.10 We understand that if a Vaccine Provider uses the BP, Patients will be presented with a co-branded booking solution, indicating that they are using an Australian Government and HealthEngine booking platform.

17.11 If the Patient is directed to the BP, the Patient will be asked:

17.11.1 to select whether the appointment is for themselves, or for someone else;

17.11.2 to select whether they are an existing patient of the Vaccine Provider, or they are a new patient;

17.11.3 to select the relevant appointment timeslots to receive each dose of the vaccine (as relevant);

17.11.4 to either:

(a) log in with their HealthEngine account, using their email address; or

(b) if the Patient does not have an account, to create an account with HealthEngine by entering the following information:

(i) their full name;

(ii) their preferred name;

(iii) their email address;

(iv) their mobile phone number;

(v) their address; and

(vi) their date of birth;

17.11.5 to enter relevant information about their Medicare card (including the card number, the identifier on the card, and the card's expiry date), if they did not choose to do so when creating their HealthEngine account (we understand that if a Patient's Medicare information is entered at this stage as opposed to when they created their HealthEngine account, this information will not be stored as part of their account and they will need to re-enter it each time they make a COVID-19 vaccination appointment);

[22] We understand that in some circumstances, the Vaccine Provider may be part of a jurisdictional health network. Depending on whether that health network has opted to use the BP for the COVID-19 vaccine roll out, or is using an existing or alternative online booking platform, the Patient will be directed to the relevant booking platform.

17.11.6 to verify their mobile phone number using a verification code that is generated by the BP and sent to their phone; and

17.11.7 to verify their email address using the verification URL that is generated by the BP and sent to their email address.

17.12 All information collected by the BP will be stored on HealthEngine's cloud environment (which uses infrastructure located in Australia).

17.13 Once the booking is made, the relevant Vaccine Provider will be able to access the information entered by the Patient into the BP.

17.14 The Patient will be sent a (via email or text) a communication confirming the appointment(s) they have booked.

17.15 After receiving a dose of the vaccine, the Patient will receive (via email or text) further post-appointment communications from HealthEngine (which is sent automatically after the time of the appointment has passed), directing the Patient to a web message in their HealthEngine account, asking the Patient to book a second appointment, and providing general information on, and ways to seek further assistance if they experience any, adverse effects.

17.16 In the relevant communication (either via text or email) the Patient will be asked to call the National Coronavirus Helpline, use HealthDirect's COVID-19 Vaccine Side Effects Symptom Checker (**Symptom Checker**), or call their GP, to discuss any concerns about adverse effects.

17.17 We understand that the 'Symptom Checker' would require an individual to input the following information:

17.17.1 their gender and age; and

17.17.2 their responses to various questions relating to whether they experienced any allergic reactions (based on any symptoms experienced).

17.18 At this stage, we understand that the Symptom Checker would then use the information inputted to generate and display relevant advice to the individual (e.g. advice that the adverse event should be reported to their Vaccine Provider, to the TGA, to their State or Territory health authority, or to the NPS MedicineWise Adverse Medicine Events hotline). In addition, at no stage will the individual be asked to provide any identifying information including their name, phone number or email.

17.19 Accordingly, we understand that no personal information, as defined in the Privacy Act (including any information relating to adverse events) will be generated by or uploaded to the Symptom Checker, or uploaded from the Symptom Checker site to any system (including the BP). Accordingly, we have not further considered this Symptom Checker as part of this PIA Update process.

17.20 We understand that at this stage, it is proposed that the BP will send de-identified information on bookings made using the BP to Health, but details of how this will occur are still being determined (we understand that this de-identified information will either be sent to the EDW (which will then send this information to the VDS), or this de-identified information will be sent to the VDS directly.

17.21 We also understand that HealthEngine will disclose some information from the BP to Health so that Health can monitor service capacity by reference to other information such as stock levels.

17.22 For completeness, we note that the BP websites used by Patients and Vaccine Providers uses cookies (small files stored on an individual's device) to recognise an individual web user as they use the BP. The cookie identifies the individual's browser or device, and not the individual personally. We understand that no personal information is stored within cookies used by the BP. The information collected includes:

17.22.1 the individual's server and IP address;

17.22.2 the name of the top level domain (for example, .gov, .com, .edu, .au);

17.22.3 the type of browser used;

17.22.4 the date and time the website was accessed;

17.22.5 how the individual interacted with the BP; and

17.22.6 the previous website the individual visited.

17.23 We understand that HealthEngine uses the above information to understand how the BP is being used, in order to improve the BP and provide users with a better experience. We understand that HealthEngine may provide this information in the form of usage reports to Health.

17.24 In relation to information provided to Patients, we understand the following:

17.24.1 a Patient will be provided with versions of the HealthEngine Collection Notice[23] and Privacy Policy that have been tailored for the BP (**HealthEngine BP Privacy Policy**[24]), before the Patient creates a HealthEngine account (as described in paragraph 17.11.4(b) above), or before they make an appointment using the BP. The Collection Notice and HealthEngine BP Privacy Policy are different to HealthEngine's standard privacy policy and collection notice);

17.24.2 a link to Health's Privacy Notice will be displayed to users when entering information into the BP for a Vaccine Provider[25]; and

17.24.3 a link to a different form of Health Privacy Notice will be displayed to Patients when making a booking using the BP.

Potential future developments

17.25 In the future, we understand that the BP may receive some personal information about Vaccine Providers (including Provider Personnel and Vaccinators) from the CVAS, however further details are not clear at this stage.

18. Privacy impact analysis and compliance

18.1 The introduction of the BP will mean that:

18.1.1 HealthEngine will **collect** information (including personal information) about Vaccine Providers and their personnel (including Vaccinators) when the Vaccine Provider establishes and operates their account within the BP;

18.1.2 Health Engine will **collect** information (including personal information, and potentially including sensitive information) about Patients, when the Patient:

[23] This Collection Notice is available at: https://healthengine.com.au/legal/commonwealth/collection.php?cid=par:hea:cbp::cbp::::mar21.
[24] This Privacy Policy is available at: https://healthengine.com.au/legal/commonwealth/privacy.php?cid=par:hea:cbp::cbp::::mar21.
[25] This Privacy Notice is available at: https://www.health.gov.au/privacy-notice-covid-19-vaccine-booking-platform.

(a) creates their account; and

(b) makes a booking using the BP;

18.1.3 HealthEngine will **use** the personal information of the Patient to generate verification codes and URLs to allow the Patient to verify their contact details, and undertake that verification process;

18.1.4 HealthEngine may **disclose** information about the Vaccine Provider (and their Vaccinators, if provided by the Vaccine Provider) to the Patient when it displays information about available booking times;

18.1.5 HealthEngine will **disclose** the Patient's information to the Vaccine Provider, when Vaccine Providers access information about their bookings;

18.1.6 HealthEngine will **use** Patient information to send confirmation, reminder, and post-appointment emails or texts to the Patient; and

18.1.7 HealthEngine may **disclose** Vaccine Provider information to Health, if:

(a) it is necessary for Health to confirm that the Vaccine Provider is eligible to use the BP; or

(b) Health needs that information to monitor service capacity by reference to other information such as stock levels of the vaccine.

18.2 We have undertaken our analysis above based on our understanding that Health's intention is that any information inputted into the BP (by Patients or by users on behalf of Vaccine Providers) will be collected by HealthEngine in its own right.

18.3 We suggest that this analysis appears to be consistent with Health's contract with HealthEngine (**HealthEngine Contract**). We note that this provides that HealthEngine must only collect personal information to the extent required to perform its contractual obligations, and must not commit any act, omission or engage in any practice that is contrary to the Privacy Act. This is an important privacy protection for Patients and Vaccine Providers.

Making individuals aware of the handling of their personal information

18.4 We note the importance of individuals who use the BP being made aware of how their personal information will be handled, including by HealthEngine. We consider that Health should continue implementing **Recommendation 2** of the Original PIA report to ensure that it has developed a broad public communication strategy which includes information about how personal information (including sensitive information) will be handled and how the privacy of Patients and other individuals will be protected (**Recommendation 1**).

Vaccine Providers (and their personnel)

18.5 The End User Terms and Conditions require a user to agree to their personal information (including health information) being handled in accordance with the HealthEngine BP Privacy Policy and Health's Privacy Policy. In addition, a link to Health's Privacy Notice for Vaccine Providers using the BP, which explains how *Health* will handle personal information, will be displayed to users when entering information in the BP for a Vaccine Provider.

18.6 It will be important that this information is provided to the Vaccine Provider's Primary Contact before the Primary Contact gives their consent for their information to be provided by the Vaccine Provider to HealthEngine. Accordingly, we **recommend** that Health explore whether the BP has this functionality and, in addition, consider issuing Vaccine Providers with guidance on how to ensure that its nominated personnel (such as its Primary Contact) provide their consent to their information being collected, used and disclosed by HealthEngine (**Recommendation 8**).

Patients

18.7 When Patients use the BP, HealthEngine will collect various types of personal information from Patients (as described above in paragraph 17.11). Accordingly, given the sensitive nature of this information, it is important that Health ensure Patients are adequately informed before they provide this information to HealthEngine.

18.8 As described above in paragraph 17.24, Patients and Vaccine Provider personnel will receive a variety of notices and information relating to the handling of their personal information in connection with the BP.

18.9 We have briefly reviewed the HealthEngine BP Privacy Policy and Collection Notice for the BP, and Health's Privacy Notice for the BP, and consider they are broadly consistent with the information in this PIA Update report. Nevertheless, we suggest that Health consider the below point.

18.10 The HealthEngine BP Privacy Policy states that HealthEngine may collect an individual's personal information in various ways, including via telephone and email. We are not aware of any information collected from Patients via telephone or email that is not already collected when the Patient creates their BP account or books an appointment. If this is incorrect, we suggest Health request HealthEngine to update the notice accordingly. We note that if personal information is collected via telephone and email, this collection would not be afforded the security protections afforded by the BP.

18.11 In addition, we **recommend** that Health ensure, through its HealthEngine Contract, that HealthEngine is required to provide Patients, with all the relevant information about how their personal information will be handled, ***before*** they either:

18.11.1 log into their HealthEngine account; or

18.11.2 create a HealthEngine account,

in order to book an appointment to receive the COVID-19 vaccine.

18.12 This will assist in ensuring that before Patients provide HealthEngine with any personal information in connection with the Vaccine Strategy, Patients are sufficiently informed about how their personal information will be handled before deciding to provide HealthEngine with this information.

18.13 We also **recommend** that Health confirm that any personnel of the Vaccine Provider are directed to, or can easily view, both the HealthEngine BP Privacy Policy and Health's Privacy Notice each time they use the BP (**Recommendation 8**).

18.14 We note that it may be confusing for Patients and users of the BP to receive up to three different links/notices related to how their personal information will be handled. This raises the risk of "information overload" for individuals, and may lead to individuals being less informed before providing their consent and their personal information to HealthEngine. In addition, given some of these notices are published by Health, and others by HealthEngine, there is a risk of inconsistency in the information, which may lead to confusion for individuals.

18.15 Accordingly, we **recommend** that Health consider the most appropriate way to communicate to Patients information about how their personal information will be handled by Health and HealthEngine in connection with the BP, taking into account the need to provide Patients with useful and consistent information whilst considering the risks of experiencing 'information overload'. For example, it may better to prepare one agreed privacy collection notice with HealthEngine, which could incorporate information currently in Health's Privacy Notice. We also **recommend** that Health review its Privacy Notices against:

18.15.1 HealthEngine's Privacy Policy and Collection Statement; and

18.15.2 the information (and information flows) described above in paragraph 17

to ensure that any information provided to individuals is consistent and accurate (**Recommendation 3**).

Collection of personal information

Data minimisation principle

18.16 Best practice requires consideration of the "data minimisation principle", under which an APP entity should minimise the amount of personal information collected to the extent possible, and limit collection to only that information which is necessary for the purposes for which it is collected.

18.17 Accordingly, it is important that HealthEngine only collects personal information that is reasonably necessary to make a booking, and individuals should not be asked to provide additional information that could be collected by the Vaccine Provider at the point that the individual attends the booked appointment.

18.18 We understand that Health is satisfied that each data field collected by HealthEngine is reasonably necessary to be collected in order to make an appointment for a Patient.

18.19 We note that as described above in paragraph 17.11.5, a Patient will need to enter information about their Medicare card when they create their HealthEngine account, or if they did not choose to do so, when they make their appointment. We understand that this information will be again collected from a Patient when they attend their appointment to receive the COVID-19 vaccine.

18.20 Given this, it is important to consider whether it would be preferable for this Medicare information to only be collected at the point when a Patient attends their appointment, as opposed through the BP as well. We understand that Health has considered this issue and has weighed the privacy risks associated with this collection by the BP against the public utility of facilitating a smooth and efficient process for Patients when they attend their appointment. We understand that by the BP collecting Medicare information, it assists in speeding up the administration processes for Vaccine Providers when Patients attend their appointments, and given the volume of Patients that will be attending these Vaccine Providers, Health has decided that the public benefits outweigh the potential privacy risks.

18.21 We have considered whether it would be appropriate for Patients to be able to use the BP without making an account, for example by making a booking for an appointment as a 'guest user'. This would have the benefit of HealthEngine collecting less personal information if Patients were not required to create HealthEngine accounts. However, we consider that the benefits for Patients in making an account (including allowing Patients to amend their personal details such as contact information, or change or cancel their appointments, as well as the ease of booking another appointment to receive the second dose of the vaccine) are likely to outweigh the potential benefits offered by a 'guest user' option. We again note the importance of ensuring that Patients can easily understand how the personal information they are providing will be handled.

Use or disclosure of personal information

18.22 It is also necessary to consider the potential privacy risk that HealthEngine could use or disclose personal information that was collected through the BP for a primary purpose for collection, but also for another permitted purpose (a secondary purpose). The information collected through the BP has been collected for the primary purpose of facilitating the booking of an appointment to receive a COVID-19 vaccine.

18.23 We have reviewed the HealthEngine Contract and note that HealthEngine must only use and disclose any personal information for the purposes of providing its contracted services to Health. This means that no personal information can be used and disclosed for a secondary purpose, unless required or permitted under the HealthEngine Contract or the Privacy Act. We also consider that Health has implemented a privacy-enhancing measure by containing in the HealthEngine Contract an express limitation on HealthEngine using any collected personal information for the purposes of direct marketing (as defined in the Privacy Act).

Segregation of data

18.24 Given that HealthEngine will be providing the BP in addition to its usual online booking services, there is a risk that information from the BP (**BP information**) may be mixed with other information collected as part of its business as usual (**BAU**) functions. As BP information is afforded the protections agreed in the HealthEngine Contract, to preserve these protections it will be important that BP information be able to be held and handled separately from HealthEngine's BAU information.

18.25 Accordingly, we **recommend** that Health ensure that the HealthEngine Contract requires HealthEngine to:

18.25.1 hold any information collected in connection with the BP separately from any information it collects as part of its BAU practices (such as through the usual online booking services it provides)[26]; and

18.25.2 not use the BP information for any other purpose beyond the provision of the BP.

18.26 This siloed approach will assist in ensuring that this information is not used for another purpose other than HealthEngine providing its services to Health, as specified in the HealthEngine Contract (**Recommendation 4**).

18.27 We **recommend** that Health ensure that it has an effective monitoring and compliance regime in relation to the handling of personal information by HealthEngine (e.g. through appropriate auditing processes of HealthEngine's data management and handling practices against its obligations in the HealthEngine Contract), which is appropriately communicated to HealthEngine (**Recommendation 4**).

Security and quality of information

18.28 As discussed in the Original PIA report, in circumstances where Patients will be concerned about their health and well-being, we consider it is reasonable for Health to assume that the personal information they enter into the BP (in order to make an appointment to receive the COVID-19 vaccination) will be accurate, up-to-date, and complete.

18.29 We also consider that any information that is provided about the Vaccine Provider's Primary Contact will either be provided by:

18.29.1 the individual themselves – in which case it is reasonable for Health to assume this information will be accurate, up-to-date, and complete; or

18.29.2 by the Vaccine Provider- we consider it will be in the Vaccine Provider's interest to provide accurate, up-to-date and complete information about its personnel, including to ensure that the Primary Contact can successfully use the BP to manage its bookings, so again consider it is reasonable for Health to assume that this information will be accurate, up-to-date and complete.

18.30 We assume that in accordance with its BAU practices, HealthEngine will provide Patients with the opportunity to amend and update their personal information linked to their account online, to ensure that their information is accurate, up to date and complete.

[26] This does not necessarily mean that a different ICT platform must be used, as the separation could be achieved by appropriate sequestering within the platform.

18.31 We understand that the BP will not integrate with other external systems (such as any Vaccine Provider systems). We have reviewed the HealthEngine Contract and note that it requires HealthEngine to maintain reasonable safeguards against loss, unauthorised access, use or disclosure and other misuse of personal information, but note that a number of the relevant clauses only apply if the information concerned falls within the definition of 'buyer data'. Accordingly, we **recommend** that Health clarify whether or not the information collected by HealthEngine in connection with the BP is included in the definition of 'buyer data' (noting that a number of important contractual obligations and protections are only triggered if this is the case) (**Recommendation 4**).

18.32 We understand that Health has engaged security experts to assist in evaluating the security of the BP, including by conducting penetration testing of the BP.

18.33 We also note that the HealthEngine Contract prevents any personal information obtained by HealthEngine in connection with this contract from transferring, storing, or allowing any person to access this information from outside of Australia. We consider this important to protect any personal information collected through the BP, and ensure compliance with the requirements of APP 8.

Retention and deletion of information

18.34 We suggest that there could be further clarity about HealthEngine's obligations in relation to the deletion of information.

18.35 We note that the HealthEngine BP Privacy Policy provides:

> *"We will only retain your personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or for legal purposes. To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements."*

18.36 However, in the following paragraph it states:

> *"Where HealthEngine has collected personal and sensitive information through the Commonwealth booking platform on behalf of the Department of Health, HealthEngine will return, retain or destroy that personal information in accordance with the CBP Agreement.*"

18.37 These paragraphs do not seem consistent with one another. Accordingly suggest that Health consider requesting HealthEngine to delete the first paragraph (as any return, retention or deletion should be done in accordance with the protections and processes built into the HealthEngine Contract).

(**Recommendation 3**)

18.38 The Health Privacy Notice states:

> *Once the Booking Platform is no longer needed, we will require Health Engine to destroy or return the data to us.*

18.39 This is consistent with stakeholder views (including the OAIC) that Health should ensure the HealthEngine Contract does not permit HealthEngine to retain any information about Patients after the termination or expiry of the HealthEngine Contract (including any information that has been de-identified or anonymised, and for any record-keeping purposes). This is especially important given that HealthEngine already holds a substantial amount of health information about Australians, and there is a risk it could conduct data matching activities that could potentially lead to the re-identification of that information.

18.40 We note that any return of personal information to Health would represent a collection of that information by Health, and Health would need to consider at that time whether such a collection was reasonably necessary for its functions and activities and otherwise in compliance with APP 3.

18.41 We do **recommend** that Health consider whether the HealthEngine Contract is sufficiently clear about the points at which HealthEngine is required to delete or destroy information collected through the BP. For example, Health may wish to consider whether information about a Patient should be deleted from HealthEngine's systems (including deleting their HealthEngine account, if that account was only created to book an appointment to receive the COVID-19 vaccine), once the Patient has attended their appointment (or second appointment) to receive the COVID-19 vaccine (**Recommendation 4**).

18.42 We note that deletion of information will, of course, be subject to any Archive Act requirements.

18.43 Finally, if Patients created a HealthEngine account only to book an appointment to receive the COVID-19 vaccine, we **recommend** that Patients are made clearly aware of how they can request for their HealthEngine account to be deleted, and are reminded of this option after they have attended both appointments to receive the relevant COVID-19 vaccine.

18.44 The HealthEngine BP Privacy Policy provides that:

> *"If we do agree to your request for the deletion of your personal information, we will delete your data but will generally assume that you would prefer us to keep a note of your name on a register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data is collected in unconnected circumstances. If you would prefer us not to do this, you are free to notify us accordingly."*

18.45 We suggest that if a Patient requests HealthEngine to delete their data, this request should be fulfilled by HealthEngine and accordingly all of their data should be deleted, including their name. We do not consider it necessary to retain a Patient's name on a 'do not call register', because presumably HealthEngine would also need to retain their phone number to ensure they are not contacted (which we understand is not also being retained).]

Future developments, such as transfer of information to the VDS

18.46 We understand that any information that may be transferred from the BP to the EDW, and then to the VDS, will not contain any personal information. If any future integration with other systems is planned, as contemplated by **Recommendation 1**, we **recommend** that Health carefully consider the privacy implications of any such developments before they are implemented, and ensure that any additional privacy impacts and risks are appropriately mitigated.

Section E Introduction of the Clinician Vaccine Integrated Platform (CVIP)

19. Project Description

19.1 Health is responsible for the implementation of this component, but is working in very close conjunction with the ADHA, as well as Services Australia.

19.2 A new digital application (**CVIP App**) has been developed by Accenture as the Data Partner as part of the CVIP solution, which is intended to streamline the uploading of vaccination data into the AIR. Use of the CVIP App will be optional for Vaccine Providers, but not required (Vaccine Providers who already have their own systems that they use to transmit information to the AIR can continue to use those systems).

19.3 We are aware that the ADHA has been responsible for arranging for independent privacy assurance processes in relation to the CVIP to be undertaken, and these processes have occurred in parallel with this PIA Update process. We have had the benefit of reviewing some draft deliverables developed as part of these processes. Those drafts contemplated that ADHA would have primary responsibility for the procurement of the CVIP platform and implementation of the CVIP App. However, we understand that these privacy assurance processes now reflect Health's greater role in the process.

19.4 In summary, we understand from those privacy assurance processes, that:

19.4.1 Vaccine Providers must register to use the CVIP App, including by inputting details, including personal information, relating to their Vaccinators (i.e. the individual personnel of the Vaccine Provider who will administer the vaccine to the Patient). This information will include their PRODA identification details (PRODA is a system managed by Services Australia), which will be used by Vaccine Providers and their personnel to log into the CVIP App. We understand that a Collection Notice (which meets the requirements of APP 5) will be provided to Vaccine Providers when they register to use the CVIP App. We understand this Collection Notice will either be provided through a registration form, or will be provided verbally if the Vaccine Provider registers via telephone.

19.4.2 All information entered into the CVIP App will be stored in a Salesforce cloud services platform (**CVIP platform**), with the relevant infrastructure located in Australia, under a contractual arrangement between Salesforce and Health.

19.4.3 Patients (when they attend their appointment with a Vaccine Provider) will be able to access a webform using the Vaccine Provider's unique QR code (publicly displayed or otherwise provided by the Vaccine Provider)[27], to enter some personal information before they receive their vaccination (e.g. name, date of birth, contact details, gender, and Medicare number). We understand that at this stage, Patients will be provided with a Collection Notice developed for the CVIP (this is available on Health's website, see https://www.health.gov.au/using-our-websites/privacy/collection-notice-for-the-clinician-vaccine-integrated-platform-cvip). All information entered is stored in the CVIP platform.

19.4.4 Once the Patient has completed this process, the Patient will be provided with a unique QR code that can be used by the Vaccinator to quickly access the Patient's information. The Vaccinator is able to do this by using the CVIP web version or CVIP App to scan or enter the Patient's unique QR code to find the Patient in the AIR and view the Patient's details. Through the CVIP, the Vaccinator will also be able to view the Patient's immunisation history available in the AIR.

[27] In future, it is possible that Patients may be able to download and use the CVIP App (or a version of it), rather than a webform to enter their details.

19.4.5 Alternatively, if the Patient does not wish to use the process specified in paragraphs 19.4.3 and 19.4.4, the Patient can provide their details directly to the Vaccinator during their consultation. The Vaccinator can then use these details to search for the Patient in the AIR using the CVIP App. The Vaccinator will then view the Patient's AIR record if a match is found, or create a new AIR record if the Patient cannot be found. This enables the Vaccinator to enter details for persons who are not eligible for Medicare and do not have a Medicare card.

19.4.6 The Vaccinator will then administer the vaccine, and input details of this vaccine into the CVIP App, together with their personal details that they are required to submit to the AIR.

19.4.7 The training provided by Health to Vaccinators includes guidance on providing appropriate notification to Patients about the mandatory reporting of their information to the AIR.

19.4.8 All information entered into the CVIP App will be stored in the CVIP platform. Most of this information will be transferred to the AIR in batches, and then deleted after it has been uploaded to the AIR. We understand that some information about Vaccinators will not be uploaded to the AIR, and this information will not be deleted (see further discussion in paragraph 20.14 below).

19.4.9 ADHA technical support staff for the CVIP will be able to access personal information stored in the CVIP platform when providing ICT support, such as resolving any technical issues relating to the upload of any information to the AIR. This could include errors relating to Patient records being rejected from being included in the AIR. We understand that in circumstances where the ADHA requires assistance from Health to resolve the issue (such as rejection of a record), the ADHA may need to disclose information on any technical issues with Health (but we understand this would not involve disclosure of any personal information to Health).

19.5 Both Patient and Provider Terms and Conditions for CVIP have been developed by Health (in close consultation with the ADHA) and are available on the Health website:

19.5.1 Consumer Terms and Conditions: https://www.health.gov.au/resources/publications/clinician-vaccine-integrated-platform-self-registration-form-terms-and-conditions-for-consumers; and

19.5.2 Provider Terms and Conditions: https://www.health.gov.au/resources/publications/clinician-vaccine-integrated-platform-self-registration-form-terms-and-conditions-for-providers.

20. Summary of independent privacy assurance processes

20.1 We consider that the commissioning and undertaking of independent privacy assurance processes in relation into the CVIP, at a relatively early stage of its development, demonstrates the commitment of the participating Commonwealth agencies to adopt a 'privacy by design' approach to the development and implementation of the CVIP, including the CVIP App.

20.2 In accordance with our instructions, we duplicated the work that has already been separately undertaken as part of the ADHA's privacy assurance processes and which appear to be a very thorough and comprehensive analysis of the privacy impacts associated with the CVIP, including the CVIP App. However, we strongly **recommend** that Health continue to work with the ADHA to implement the findings and recommendations of the CVIP privacy assurance processes (**Recommendation 9**), taking into account any future design updates to the CVIP App.

20.3 In our view, implementation of the findings and recommendations from the independent CVIP privacy assurance processes (as set out in the draft material developed as part of these processes that we have reviewed) would effectively address the following identified privacy risks:

Making individuals aware of handling of information

20.4 It will be important that both the Patient, and the Vaccinator, are made aware of how their personal information will be handled. That is, there should be a mechanism for the relevant user to be made aware of how their personal information will be handled, before they submit that information to the CVIP platform. We note that these matters were considered, and addressed by a number of recommendations developed, by the privacy assurance processes conducted by the ADHA.

20.5 In addition to these recommendations, we also **recommend** that Health:

20.5.1 review and, if necessary, update the CVIP Privacy Notice on its website to ensure 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, using AWS infrastructure) before it is provided to the AIR; and

20.5.2 develop separate notices for Patients, and for Vaccine Providers and their personnel (i.e. Vaccinators)

(**Recommendation 3**).

Collection of personal information

20.6 We note that the draft deliverables from the independent CVIP privacy assurance processes conducted by the ADHA (that we have had the benefit of reviewing) focus on the ADHA's functions and activities, which was appropriate given the understanding at that time that the ADHA would procure the CVIP platform. We have considered compliance with APP 3 from Health's perspective, rather than the ADHA's perspective, noting the need for collections to be reasonably necessary for *Health's* functions and activities in order to comply with APP 3.

20.7 In our view, we consider that there is a sufficient nexus between Health's role in the implementation of the COVID-19 roll out, and its responsibility for administration of the AIR Act (which requires Vaccinators to provide certain information to the AIR by law[28]), to conclude that APP 3.1 is satisfied.

20.8 We note that in the findings from the privacy assurance processes conducted by the ADHA, the collection of information by and from the AIR was found to be authorised by s22(2) of the AIR Act, which authorises the collection, use or disclosure of information, where this is done for the purposes of the AIR. The privacy assurance processes considered that the collection of a Patient's details and immunisation history using the CVIP App can be characterised as being 'for the purposes of' the AIR, on the basis that this will enable Vaccine Providers to:

20.8.1 check the Patient's vaccination status; and

20.8.2 (if the vaccine is administered) provide vaccination details for inclusion in the AIR, in accordance with the Vaccine Provider's mandatory reporting obligations.

[28] A separate PIA was conducted for Health in relation to those changes, see: https://www.health.gov.au/using-our-websites/privacy/privacy-impact-assessment-register.

20.9 We agree with this, as long as Health can be satisfied that it has effective control over the personal information stored in the CVIP platform, and that there is no separate collection of information by Accenture or Salesforce. This will depend upon an analysis of the relevant contractual arrangements, and whether they meet the guidance issued by the OAIC about the limited circumstances in which providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure (consistent with **Recommendation 4**).[29]

20.10 In addition, we support the findings and recommendations from the privacy assurance activities conducted by the ADHA which conclude that the CVIP App should only collect the minimum amount of information necessary for the purposes of transferring it to the AIR. That is, it should not ask the user to enter any data fields that are not required to be uploaded to the AIR (**Recommendation 9**).

Security of information

20.11 Given the sensitivity of the information stored in the CVIP platform, Health will need to be satisfied that there are strong security protections for that platform.[30] We agree with the analysis and recommendations developed through the CVIP privacy assurance processes and note that Health should be satisfied that the contractual arrangements with Accenture as the Data Partner, and with Salesforce, contains appropriate security obligations (**Recommendation 4**).

Deletion of information from the CVIP platform

20.12 We note that it is intended that personal information relating to vaccinations will be stored in the CVIP platform only temporarily (i.e. until it is uploaded to the AIR). We note that relevant obligations to this effect will need to be included in the relevant contractual relationships (e.g. the Partner Contract with Accenture).

20.13 In addition, we understand that Health and the AHDA are working with the National Archives of Australia to ensure that such temporarily stored information can be deleted in accordance with the Archives Act after it has been uploaded to the AIR and verified by Services Australia.

20.14 In relation to collection of Vaccinator information, we understand that the CVIP platform will collect and store some information about Vaccinators that will not be uploaded to the AIR. This information will not be deleted. Vaccinators should be made aware of this, and of any proposed uses and disclosures of the retained information (see **Recommendation 3**).

Future developments, such as the transfer of responsibility for the CVIP App to the ADHA or integration with the VDS

20.15 We note that it does not appear that any personal information will be provided to Health. However, if this changes in the future, Health should ensure it has robust data governance in place before any personal information is disclosed to Health.

20.16 We understand that at some future point, responsibility for operation of the relevant cloud services platform (including the relevant contractual arrangements) may be transferred from Health to the ADHA.

[29] See APP Guidelines, Chapter B, paragraph B.63–B.68.
[30] See also the discussion of this issue in relation to the CVAS in **Section B** of this **Part E**, including issues of community perception in relation to cloud services provided by foreign owned companies.

20.17 In addition, we understand that although there are no current plans to integrate or otherwise transfer information stored in the CVIP platform to other ICT systems or components referenced in this PIA Update report (e.g. the VDS), this may be considered in the future.

20.18 As contemplated by **Recommendation 1**, we **recommend** that Health carefully consider the privacy implications of any such developments before they are implemented (including undertaking any updated or supplementary PIA processes, as required by the APP Code), and ensure that any additional privacy impacts and risks are appropriately mitigated (noting that there are no references to the possible transfer of information to the ADHA or Health, or other systems, in the CVIP Privacy Notice, so individuals will have not been given any notice of these possibilities).

Part F GLOSSARY

Definitions	
ADHA	means the Australian Digital Health Agency.
AIR	means the Australian Immunisation Register.
AIR Act	means *Australian Immunisation Register Act 2015* (Cth).
APP, or Australian Privacy Principle	has the meaning given to it in the Privacy Act.
Archives Act	means the *Archives Act 1983* (Cth).
BP	means the Commonwealth-procured Booking Platform, through which individuals are able to make online bookings to receive a COVID-19 vaccine with a Vaccine Provider (where that Vaccine Provider does not otherwise have an online booking system and wishes to use the BP).
Collection Notice	means a notice provided to individuals before their personal information (including sensitive information) is collected, which provides them with information on how their Vaccine Strategy Information will be handled in connection with the Vaccine Strategy (including any subsequent uses and disclosures of that information).
COVID-19	means the coronavirus disease caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).
CVAS	means the COVID-19 Vaccine Administrative System, which is Health's system for procuring, ordering and distributing vaccines to States and Territories, facilitating the management of supply chains for all vaccines procured by the Commonwealth.
CVIP	means the solution, including the CVIP App, which has been designed in order to assist Vaccine Providers/Vaccinators to transmit and input relevant Vaccine Strategy Information into the AIR.
CVIP App	means the mobile application developed by the Data Partner as part of the CVIP solution..
Data Partner	means the provider contracted by Health who will design, develop and implement the VDS.
EDW	means the Health's Enterprise Data Warehouse, which is a platform that supports Health's storage of health data in a secure environment.
GP	means a general practitioner.
GPRC	means a GP-Led Respiratory Clinic.
Health	means the Commonwealth Department of Health.
Information Flow	means a flow of personal information as described in this Stakeholder Consultation Document.

Logistics and Distribution Partner	means the provider contracted by Health who will co-design, establish and operate a logistics and distribution network for COVID-19 vaccines, and who is responsible for the distribution of the COVID-19 vaccines in connection with Phase 1a of the Vaccine Strategy.
My Health Record	means the online summary of a Patient's key health information.
Notification Provider	means a provider engaged by Health to send notifications to individuals who have provided their contact details using the RYI solution, including when the individual becomes eligible to make an appointment to receive a COVID-19 vaccine.
OAIC	means the Office of the Australian Information Commissioner.
organisation	has the same meaning given by section 6C of the Privacy Act.
Partners	collectively means the Data Partner, Strategy Partner, Logistics and Distribution Partner, Vaccine Administrator, and Training Partner, as engaged by Health under a Partner Contract.
Partner Contract	means the contractual arrangements between Health and a Partner.
Patient	means an individual wishing to receive a vaccine for COVID-19.
Patient Information	means information collected about a Patient, which may include personal information (including sensitive information).
personal information	has the meaning given in section 6 of the Privacy Act.
PIA	means the privacy impact assessment that will be informed by this Stakeholder Consultation Document.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Notice	Means a Collection Notice and/or Privacy Policy for one or more specific components of the Vaccine Strategy.
Privacy Policy	means a privacy policy, developed in accordance with the Privacy Act (including the requirements of APP 1).
Provider Personnel	means the Vaccine Provider's personnel.
RYI or **RYI solution**	means the 'Register your Interest' solution, which allows members of the public to choose to be contacted when the future Phase in which they will be eligible to make a booking to receive a vaccine will commence.
sensitive information	has the same meaning given by section 6 of the Privacy Act.
TGA	means the Therapeutic Goods Association.
Vaccinator	means a Provider Personnel who will administer a COVID-19 vaccine to a Patient.
Vaccinator Information	means information collected about the Vaccinator who administers the relevant vaccine, which may include personal information.

Vaccine Administrator	means the provider contracted by Health who will provide vaccine administration services, on an 'as required' basis, to supplement delivery of the vaccines by other entities, including to particular priority and other vulnerable or hard to reach populations or communities, or in other circumstances where an additional workforce is required. The Vaccine Administrator may be a Vaccine Provider for particular locations.
Vaccine Provider	means the entity responsible for operating the site at which the COVID-19 vaccines will be administered to Patients. The Vaccine Administrator may be a Vaccine Provider.
Vaccine Strategy	means the COVID-19 Vaccine and Treatment Strategy and the COVID-19 Vaccine National Roll-out Strategy, currently being implemented as part of the Australian Government's response to the COVID-19 pandemic.
Vaccine Strategy Information	means any Patient Information, Vaccinator Information, other Provider Personnel Information, and Distribution Partner Personnel Information collected under the Vaccine Strategy.
VDS	means the data solution developed by the Data Partner to enable the tracking and reporting of COVID-19 vaccines across the vaccination delivery chain, over the life of the national COVID-19 vaccination program.
VILS	means the COVID-19 Vaccine Information and Location Service, which includes ICT systems that are being developed, implemented and/or used as part of the Vaccine Strategy.

Attachment 1 Material reviewed

1. Aboriginal and Torres Strait Islander Implementation Plan Consultation – received 2 February 2021
2. Aged Care Implementation Plan Consultation – received 2 February 2021
3. Australian Capital Territory COVID-19 Vaccine Implementation Plan – received 2 February 2021
4. CALD Communities Implementation Plan Consultation – received 2 February 2021
5. COVID Vaccine data flow – 1A Pfizer, 1A AstraZeneca, 1B AstraZeneca, Consumables – received 12 March 2021
6. COVID Vaccine Information and Booking System – received 5 March 2021
7. COVID Vaccine Information and Booking System (CVIBS): Overview for CIOs – 5 March 2021
8. COVID-19 Vaccine Management Systems and Data Flows – received 10 March 2021
9. COVID-19 Vaccine Management Systems and Data Flows NSW – received 5 March 2021
10. COVID-19 Vaccine Roll-out Phase 1B Eligibility Declaration Information and Form – Option 2 (Non-Statutory Declaration) – received 16 February 2021
11. CVIBS Booking Platform – Further CBP Comms, version 0.1 – received 19 March 2021
12. Digital Sourcing Contract – Hosted Software (executed by HealthEngine)
13. Disability Sector Implementation Plan Consultation – received 2 February 2021
14. HealthEngine End User Services Form for National Booking Platform, version 0.4 – received 17 March 2021
15. HealthEngine End User Terms and Conditions – received 17 March 2021
16. National Booking System Minimum Viable Product – Initial Release – received 5 March 2021
17. National Health Services Directory – Data Sharing Arrangements with Australian Government Department of Health: Coronavirus Vaccine Clinics 2021 – received 5 March 2021
18. New South Wales COVID-19 Vaccine Implementation Plan – received 2 February 2021
19. Northern Territory COVID-19 Vaccine Implementation Plan – received 2 February 2021
20. Phase 1B COVID-19 vaccine roll-out – General Practice EOI process: Frequently asked questions version 2 – received 2 February 2021
21. Queensland COVID-19 Vaccine Implementation Plan – received 2 February 2021
22. Register your Interest information flow and contractual arrangements – 3 March 2021
23. Several OAIC responses to the Department of Health on preliminary phase 1b PIA update documentation
24. South Australia COVID-19 Vaccine Implementation Plan – received 2 February 2021
25. Tasmania COVID-19 Vaccine Implementation Plan – received 2 February 2021

26. Vaccine order management – Release 1 + Release 2: Experience walkthrough – received 23 March 2021

27. Various draft and final Privacy Notices for new ICT components being introduced as part of Phase 1b of the Vaccine Strategy.

28. Victoria COVID-19 Vaccine Implementation Plan – received 2 February 2021

29. Western Australia COVID-19 Vaccine Implementation Plan – received 2 February 2021