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

THE COVIDSAFE APPLICATION

Privacy Impact Assessment

24 April 2020

Contents

Part A EXECUTIVE SUMMARY

1. Introduction

1.1 The outbreak of the COVID-19 pandemic in Australia has resulted in a health emergency. This has required an unprecedented response from the Australian Government for management of the public health crisis to:

1.1.1 minimise the number of people becoming infected or sick with COVID-19;

1.1.2 minimise how sick people become and the mortality rate;

1.1.3 manage the demand on Australia's health systems; and

1.1.4 help individuals to manage their own risk and the risk to their family and community.

1.2 The Australian Government has developed a new software application, COVIDSafe (the **App**), to enhance the current contact tracing processes which are undertaken by State and Territory health officials, to identify people in Australia who may have come into contact with someone who has tested positive to COVID-19, so that appropriate advice about COVID-19 can be provided to that person.

1.3 Ensuring public trust in the operation of the App will be critical to its successful roll-out. Ensuring the App meets privacy requirements will help foster that confidence. This Privacy Impact Assessment (**PIA**) was commissioned to ensure privacy risks were being addressed throughout the development process.

1.4 In developing the App, the Australian Government has taken a "privacy by design" approach, including by taking steps to minimise the collection of personal information and to limit who will be able to access App Information. We understand that the Australian Government is also proposing to introduce legal requirements that will limit the use of information collected through the App.

1.5 We are satisfied that Australian Government has considered the range of privacy risks associated with the App and has already taken steps to mitigate some of these risks. The PIA makes a range of recommendations to ensure privacy issues continue to be addressed as the App is rolled out and App information is collected and used.

2. This PIA process

2.1 The Department of Health (**Health**) is responsible for implementation and operation of the App, in conjunction with the Digital Transformation Agency (**DTA**) and with input from representatives from the Attorney-General's Department (**AGD**), the Department of the Prime Minister and Cabinet (**PM&C**), and State and Territory agencies responsible for contact tracing.

2.2 The App will involve the collection of specific personal information about individuals who choose to download the App (**Users**). The information may be collected at different points, depending whether Users may have been exposed to another User who has tested positive to COVID-19 (a **Positive User**).

2.3 We have undertaken an urgent PIA process, to allow Health to consider the relevant information flows, determine whether the App includes appropriate privacy obligations and protections, and if not, determine what steps can urgently be taken to address, and mitigate, any identified privacy risks.

2.4 The App is intended to be released in the near future. The design and technical work needed for development of the App has occurred in parallel with our undertaking of the PIA process. We have been very pleased to see that, as various iterations of the design of the App have developed during our involvement in the PIA process, privacy risks and issues we have identified have been taken into account, and the design has been changed to further mitigate against those risks. We expect that the design of the App will continue to evolve, including to take into account the recommendations set out in this PIA report.

2.5 This PIA:

2.5.1 considers compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**);

2.5.2 sets out the information flows, which helps to highlight privacy risks and areas for improvement in terms of risk mitigation;

2.5.3 is intended to help Health manage identified privacy risks and impacts, in respect of the App;

2.5.4 may serve to inform Health and other stakeholders about the privacy elements of the App; and

2.5.5 considers the safeguards that have been, or should be, put in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure.

3. Summary of findings

3.1 In our view, the stakeholders we have engaged with have shown a genuine appreciation of the importance of addressing privacy considerations and risks involved in developing and implementing the App. The importance placed on privacy has facilitated the adoption of a "privacy by design" approach, with decisions being made to change the design of the App to mitigate against identified privacy risks during this PIA process.

3.2 Despite this, we consider that further work needs to be undertaken to address potential privacy risks in relation to the following:

3.2.1 the desirability of there being further communication to the public, with clarity about the function and purpose of the App, how the App will work, what personal information will be collected by the App, and how that information will be used;

3.2.2 the need for further assurance that personal information collected through the App will only be used for contact tracing;

3.2.3 the minimisation of risks associated with loss of control over the personal information collected through the App once the information is disclosed to State and Territory Public Health Officials and Contact Tracers;

3.2.4 the need to ensure maximum application of the "data minimisation principle", so that the minimum amount of personal information required is collected;

3.2.5 the need to ensure that consent is voluntary, and provided so that Users of the App properly understand how their personal information will be handled;

3.2.6 the need to ensure that appropriate consent is obtained from parents/guardians for Users who are children under the age of 16;

3.2.7 the need for further assurance around potential security risks;

3.2.8 further clarity about retention of personal information collected through the App after the end of the COVID-19 pandemic; and

3.2.9 the desirability of further clarity about data governance arrangements, including in ICT and other contracts or other arrangements, between entities involved in the implementation and operation of the App.

3.3 These risks have been considered throughout this PIA report. The recommendations set out in paragraph 4 of this **Part A** are designed to address the identified risks and further enhance privacy protections for Users, and/or further strengthen Health's compliance with the APPs.

4. Recommendations

4.1 This PIA makes the following recommendations in relation to the App:

Recommendation 1 Make PIA report and App source code publicly available

To increase public trust and confidence in the App, we **recommend** that Health consider publishing this PIA report. Health could also consider making the source code for the App publicly available, to allow for independent analysis and consideration.

Recommendation 2 Future changes to the App

We have undertaken our analysis on the basis of the development of the App as at the time of this report. As the design of the App evolves, or if there are likely to involve changes to any of the information flows discussed in this PIA report, we **recommend** that Health continue to carefully consider privacy impacts of those changes, including through a supplementary PIA process to update or supplement this report as required by the APP Code.

This will also enhance protections against the risk of "function creep", where information which is collected for one purpose starts to be used for another purpose which was not originally anticipated.

Recommendation 3 Appropriate legislative framework

We **recommend** that Health continue to consider and investigate the legislative options in relation to the collection, use, disclosure, and deletion, of personal information in connection with the App (including the appropriate restrictions to be placed on Commonwealth departments and agencies, and States and Territories (which includes the relevant health authorities, Public Health Officials, and Contact Tracers) or any other relevant entities).

This may include consulting with the AGD, OAIC and other stakeholders to determine whether it would be appropriate to consult with the States and Territories about whether the relevant State and Territory health authorities should be prescribed as organisations for the purposes of the Privacy Act.

We also **recommend** that Health continue to seek advice, including through consultation with AGD, the OAIC and the AHRC as appropriate, as to whether there are additional legislative or other measures that could be put in place to protect rights of individuals who decide not to use the App (for example, circumstances in which a particular individual does feel pressured to download the App (e.g. a supermarket insisting on customers showing that they are using the App before being permitted to enter the store; or an employer insisting that their employees demonstrate that they are using the App before being permitted to start or continue work) may constitute a breach of human rights).

We understand that work has already commenced on a legislative framework, which has been undertaken in parallel with our PIA process, with the intent of strengthening privacy protections for Users. While this framework has not been finalised as at the date of this PIA, we understand that there is an intention to make it clear that data collected through the App will only be used for purposes associated with contact tracing or administering the App. We **recommend** that this work continue, and be finalised before release of the App.

Recommendation 4 App screens displayed to the User

We **recommend** that Health ensure that the sequencing of screens displayed to the User when registering to use the App, and when they are asked for consideration to upload their Digital Handshake information, is such that the User is provided with information about the handling of their personal information before they are asked to provide consent.

We also **recommend** that Health consider whether information should be included on the App about what to do if a User feels they have been pressured into using the App (e.g. it could be included in the App Privacy Policy), unless a legislative framework is introduced to address this risk.

Recommendation 5 Clarify collection of age

We **recommend** that Health consider undertaking further consultation as required about whether it should change the proposed design of the App so that only an age range of the User is collected through the App. If there is no clear medical reason for collecting the precise age, using an age range would enhance compliance with APP 3, and have the additional benefits of being consistent with the data minimisation principle, and further reduce risks of more precise personal information being disclosed if there was to be a data breach.

Recommendation 6 Consent from Users

We **recommend** that Health ensure that the App seeks consent from Users at two different points – an initial notice which is provided to individuals before they agree to their Registration Information being uploaded to the National COVIDSafe Data Store, and a further notice which is provided before they agree to upload the Digital Handshake information on their device to the National COVIDSafe Data Store.

We **recommend** that the wording for the collection and consent notices displayed on the App be carefully considered to ensure that Users, including Child Users, will understand what they are being asked to consent to, and how their information will be collected, used, disclosed, and deleted. We developed some draft wording for these

notices, in conjunction with the Australian Government Solicitor. We **recommend** this wording be used as the basis for notices included in the App, subject to further refinement as the design of the App is finalised.

We also **recommend** that Health consider whether it is necessary to impose a time limit on the initial consent obtained in connection with the Registration Information (for example, 6 or 12 months), and ensure that the functionality of the App will require a further consent notice to be displayed to the User after this time period, which must be accepted to allow further use of the App.

Recommendation 7 App Privacy Policy

We **recommend** that Health ensure that a specific privacy policy for the App is developed and clearly available to Users of the App.

We developed some draft wording for the App Privacy Policy, in conjunction with the Australian Government Solicitor. We **recommend** this wording be used as the basis for the App Privacy Policy, subject to further refinement as the design of the App is finalised.

The App Privacy Policy could also be displayed on Health's website.

Recommendation 8 Form on the App to request access and correction of information

We **recommend** that Health consider whether processes could, unless access and correction is otherwise covered by a legislative framework for the App, be adopted to make it easier for Users to make requests to access and/or correct their personal information held in the National COVIDSafe Data Store (e.g. an e-form accessible from the App).

Recommendation 9 Communication materials for the public and potential Users

We **recommend** that Health develop and publish a range of communication materials so that the general public, and potential Users, are provided with as broad a range of information about the App and the National COVIDSafe Data Store as possible. Such information could include:

- answers to frequently asked questions;
- summary information about this PIA report;
- information about the voluntary nature of the App, and that no-one should pressure an individual to download or use the App; and
- information about any legislative framework which is put in place to govern the operation of the App.

This would assist in building community understanding and acceptance for the App, particularly if such material explains why the App has been developed, its function and purposes, how it works (including where information will be stored), what it collects, what information will be used by States and Territories, how the information can be deleted or will be retained, and the App's security features. It will also be important to emphasise the voluntary nature of the App, with the consent requirements, and the User's ability to not proceed at any stage or to delete the App.

Recommendation 10 Further assurances by Health about access to and use of the Registration Information in the National COVIDSafe Data Store

To further alleviate potential community concerns associated with the use of the App, we **recommend** that (unless a suitable legislative framework is put in place) Health consider taking additional steps to alleviate concerns that the Registration Information will be used in ways other than those contemplated in this PIA report. This could include taking steps, including:

- to ensure that it will not be possible to generate Unique ID Reports which use the Registration Information of Users to identify individual Users who are using the App (and/or individual Users who have downloaded but are not using the App);
- to ensure that it will not be possible, either for the Australian Government or State and Territory governments (through their Public Health Officials or Contact Tracers), to access Registration Information of a User before they have tested positive for COVID-19, or have been identified as a Contact User for someone who has tested positive; and
- making public commitments that Registration Information will not be used in these ways (e.g. as part of a publishing a frequently asked questions document on its website when implementing **Recommendation 9**), and the voluntary nature of the App, and about the security protections that have been put in place in relation to the App and the National COVIDSafe Data Store (without providing information that would pose an additional security risk).

Recommendation 11 Development of training and/or scripts

We **recommend** that Health consider developing training and/or scripts for Public Health Officials and Contact Tracers in connection with the App.

Such a script could include guidance about:

- how to ask Positive Users to use their mobile phone number in the App to send them an SMS message to upload their data, which clearly asks for permission to enter their mobile phone number into the National COVIDSafe Data Store in order to generate and send the SMS message to the Positive User; and
- how Public Health Officials and Contact Tracers should deal with Child Users, including those who need to be contacted as a result of an upload of Digital Handshakes from a Positive User (e.g. to ensure they speak to the Child User's parent/guardian, before proceeding further with the contact tracing procedures).

Further, training could include providing:

- guidance to Contact Tracers of the limitations of the quality of the information in the National COVIDSafe Data Store when undertaking contact tracing procedures; and

- appropriate security training (including privacy briefings) before Public Health Officials and Contact Tracers are granted access to the National COVIDSafe Data Store.

Recommendation 12 Contractual or other arrangements with State and Territory public health authorities

Whilst Health will not have effective control over the information once it has been disclosed to Contact Tracers, we **recommend** that Health ensure that it has contractual or other administrative arrangements in place with the State and Territory public health authorities responsible for contact tracing.

These arrangements should contain terms and conditions for access to, and use and disclosure of information obtained from, the National COVIDSafe Data Store, including to require that State and Territory public health authorities:

- only access, use and disclose personal information for the purposes contemplated in this PIA;

- ensure that agreed processes (including any developed "scripts") are used by Public Health Officials and Contact Tracers when contacting Positive Users and Contact Users; and

- ensure appropriate security arrangements are in place for any personal information obtained from the National COVIDSafe Data Store which is held by the Public Health Officials or Contact Tracers, that such information is deleted, de-identified or not further used after the time of the decommissioning of the National COVIDSafe Data Store, and that it may not be transferred, stored or accessed from outside of Australia.

Such obligations would need to be consistent with any legislative framework that is put in place in respect of the App.

Further, we **recommend** that each time a Contact Tracer accesses the National COVIDSafe Data Store, they be required to agree to terms and conditions of use, which clearly set out the limited ways in which Contact Tracers are permitted to use, access and disclose information stored on the National COVIDSafe Data Store.

Ideally, State and Territory public health authorities should also be required to comply with the Privacy Act as if they were an APP entity. Such arrangements would assist in providing Users with additional privacy protections, including to ensure that all Users are afforded the same protections across all jurisdictions.

Recommendation 13 Notify Users they can register with a pseudonym

We **recommend** that Health clearly and expressly notifies Users, before registering for use of the App, that they may, when providing their Registration Information, use a pseudonym (for example, a note under the name field could be included to clarify that the User can give a "fake name"). Further, we **recommend** that Health, in its notices provided to Users when seeking consent, and/or in the App Privacy Policy, should indicate that Users may use a pseudonym.

Recommendation 14 Security arrangements

We **recommend** that Health, if it has not already done so, seek independent assurance from security experts (including as appropriate, the Australian Signals Directorate and the Australian Cybersecurity Centre), to provide additional testing and assurance that the security arrangements for the App and the National COVIDSafe Data Store, and the use of information in it, are appropriate. We also **recommend** that this assurance be made publicly available (without providing any information that would pose an additional security risk).

Further, we **recommend** that Health undertake appropriate planning, and ensure that appropriate arrangements are in place, so that steps can be taken immediately to minimise the effect of any data breach, and an efficient and effective investigation process is undertaken as soon as possible. We note that this may involve ensuring that appropriate contractual (or administrative) provisions are included in the AWS Contract, the memorandum of understanding (**MOU**) arrangements with DTA and the contractual or other arrangements with the State and Territory agencies.

We also **recommend** that Health consider whether:

- Bluetooth technology is the most appropriate available technology to use for the App; and
- there are additional technological solutions or strategies that could be used to avoid the need to advise Users to have the App unlocked on their device.

Recommendation 15 Application of the *Archives Act 1983* (Cth)

Unless it will be otherwise dealt with by a legislative framework, we **recommend** that Health promptly, and before the finalisation of the App Privacy Policy and the notices that will be provided to Users when seeking consent (see **Recommendation 6** and **Recommendation 7**), seek advice (including consultation with the National Archives of Australia as appropriate):

- as to whether the personal information in the National COVIDSafe Data Store will be subject to the Archives Act;
- if so, whether the records will be able to be deleted or de-identified after the personal information in the National COVIDSafe Data Store is no longer required (for example, it may be necessary to determine whether a records disposal authority should be obtained in advance of the release of the App, or

other legislative action taken, to enable deletion or de-identification of the personal information as required); and

- whether retention of the records is required by any other law or legal requirement (e.g. if a complaint or legal action was brought by a User after de-commissioning of the National COVIDSafe Data Store).

Recommendation 16 Confirmation of arrangements with AWS

We **recommend** that Health take steps to investigate and confirm the arrangements in relation to the role of AWS. This could be through Health undertaking a review of the AWS Contract, or ensuring that relevant provisions are included in appropriate arrangements between DTA and Health (such as an MOU or other suitable administrative arrangements)

We **recommend** that Health investigate the nature of the services being undertaken by AWS (i.e. limited to infrastructure support services and not data analysis services) and that the AWS Contract contains:

- detailed functional and non-functional requirements for the App and the National COVIDSafe Data Store infrastructure;
- detailed security requirements about the storage of information in the App and on the National COVIDSafe Data Store infrastructure, including encryption requirements, and obligations on AWS in relation to security, confidentiality and privacy requirements;
- detailed support requirements, which limit access to the National COVIDSafe Data Store to AWS' authorised support personnel who need that access for the purposes of providing the contracted support;
- in accordance with provisions which are commonly found in contracts for provision of cloud-based infrastructure, requirements under which:
    - AWS is not responsible for the management of data content stored in the National COVIDSafe Data Store;
    - the Commonwealth of Australia (acting through DTA) is given the necessary rights and powers to control access to, change, or retrieve, the information in the National COVIDSafe Data Store, so as to reflect that the Commonwealth and not AWS has effective control of the information, and how it is handled by AWS; and
    - AWS will allow the Commonwealth to remove data content stored in the National COVIDSafe Data Store after the end of the AWS Contract, after which time it will be deleted if not removed;
- detailed subcontractor requirements, such that AWS is required to ensure that any obligations imposed upon AWS are also imposed upon any of AWS' subcontractors and/or its service providers;
- detailed access to information requirements, so that if a User is entitled to request access to, or correction of, their personal information and Health needs to ask DTA to obtain the information (through AWS) from the National COVIDSafe Data Store, AWS must provide the required information to DTA (which will, if **Recommendation 17** is implemented, be required to be provided to Health); and

- detailed requirements, so that no information from the National COVIDSafe Data Store is:
    - taken outside Australia, or accessed from or stored outside of Australia, without the prior written consent of Health; or
    - transferred outside of the National COVIDSafe Data Store (e.g. to other parts of the AWS' infrastructure environment).

Recommendation 17 Ensure ICT contracts and arrangements are properly documented, and contain appropriate contractual or other protections

Our analysis has been conducted on the basis that both Health and DTA intend that DTA will provide the infrastructure on which the collected information will be stored as a service provider to Health, and that Health will be the data custodian of the collected information. Accordingly, we **recommend** that appropriate MOU or other arrangements are documented between DTA and Health which, amongst other things:

- establish Health as the data custodian of the information collected using the App;
- clarify that the relevant infrastructure will be provided as a service by DTA to Health;
- confirm that the AWS Contract contains the matters specified in **Recommendation 16**;
- clarify DTA's role in providing the relevant infrastructure (through its contractor AWS) as a service by DTA to Health[1];
- provide Health with the rights of access to and control of the stored information on the DTA infrastructure;
- place appropriate limits on DTA's access to and use of the stored information;
- impose appropriate security requirements;
- sets out the processes for Health to request, and receive, information from DTA (and AWS) if a User requests access to, or correction of, their personal information held in the National COVIDSafe Data Store; and
- ensure the DTA's subcontractors are required to comply with the above requirements.

We also **recommend** that Health ensure that all contractual arrangements with relevant ICT and other service providers, who may have access to collected personal information in order to provide services under that contract, include suitable privacy requirements, and appropriate security clauses that require protection of the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

[1] An alternative might be for Health to administer the AWS Contract on behalf of the Commonwealth instead of DTA (with appropriate arrangements made for payments to AWS under the Contract), but given DTA's integral role in developing and supporting the App and National COVIDSafe Data Store, this may not be practical.

Recommendation 18 Number of Digital Handshakes

We **recommend** that:

- Health investigate whether it is technologically possible to only record Digital Handshakes if they meet risk parameters, set on the basis of medical advice about the risks of exposure to COVID-19 (i.e. so that the minimum amount of information required for contact tracing is collected from Users); or
- if this is not possible, whether it is technologically possible to only upload Digital Handshakes if they meet those risk parameters; or
- if this is not possible, whether it is technologically possible for the National COVIDSafe Data Store to, once Digital Handshakes are uploaded, automatically delete (or de-identify if deletion is not possible) any Digital Handshakes that do not meet those risk parameters; or
- if this is not possible, access to the Digital Handshakes stored in the National COVIDSafe Data Store be limited to those Digital Handshakes which meet those risk parameters.

Recommendation 19 Consent process for Child Users

We **recommend** that Health further consider the processes in the App if a User is a Child User. For example, Health should consider whether there could be a more robust process to ensure that informed consent is obtained from an adult responsible for the Child User. For example, a "verified consent" process would assist in strengthening the likelihood that an adult responsible for the Child User has provided their consent. The Child User could also be presented with an option to click if they do not have their parent/guardian's consent, which results in a message to then uninstall the App.

Part B METHODOLOGY AND ASSUMPTIONS

5. Our methodology

5.1 This PIA has been conducted in an extremely compressed timeframe, to ensure that any identified privacy risks can be considered and addressed so as to minimise the impact upon Users who may submit their personal information using the App.

5.2 To the extent possible in the required timeframe, this PIA has been developed in accordance with the *Privacy Impact Assessment Guide* (**PIA Guide**) issued by the Office of the Australian Information Commissioner (**OAIC**). We have adapted our usual methodology in order to conduct this PIA in the required timeframe, as follows:

Stage	Description of steps
1.	**Plan for the PIA:** We have reviewed some relevant background material provided by Health, and were provided with briefings by officers from Health, DTA, AGD and PM&C. We discussed the policy intent behind the collection of personal information through the App, and clarified our understanding of the technical and other arrangements for the App. We discussed and agreed the scope and truncated timeframes for carrying out this PIA.
2.	**Stakeholder consultation:** Given the general public interest surrounding the development and implementation of the App, we recognise that widespread community consultation would have been desirable for this PIA process. However, the truncated timeframes have meant that it has simply not been possible for us to conduct stakeholder workshops with the many individuals or groups that might be impacted by the issues raised by this PIA. However, when undertaking our analysis and forming our views about risks, we have taken into account: • issues raised with Health and other stakeholders by the OAIC, including through consultation meetings with representatives from the OAIC; • issues raised with Health and other stakeholders by the Australian Human Rights Commission (**AHRC**); • published material, including media reports in relation to the development of the App and about contact tracing applications internationally (including the material in **Attachment 2**); and • our research about reasonable community expectations of privacy. For example, the *Australian Community Attitudes to Privacy Survey 2017* commissioned by the OAIC contains useful information regarding current community expectations, including about the level of trust in government agencies' handling of personal information. We have also had the benefit of some early findings from OAIC's update of this research, including how community expectations have changed since the outbreak of the COVID-19 pandemic in Australia, as noted in this PIA report.
3.	**Privacy impact analysis and compliance check:** In this step we focussed on compliance against each APP and privacy best practice. The analysis set out in this PIA is consistent with the *Australian Privacy Principles Guidelines* (**APP Guidelines**) issued by the 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. In this PIA, given the compressed timeframe, 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 report.
7.	**Further stakeholder engagement:** We received recommendations and comments by Health, the OAIC, DTA, the Department of the Prime Minister and Cabinet, and the Attorney-General's Department on draft versions of this PIA report. We again recognise that further time to conduct additional consultation processes about the draft PIA report and its recommendations would have been desirable. In particular, we appreciate offers by the OAIC and the AHRC to facilitate further consultation processes and engagement, including with State and Territory privacy authorities, to obtain timely and comprehensive advice in relation to deployment of the App, but note that timeframes have not permitted facilitation of such further engagement.
8.	**Privacy management and addressing risks:** We further refined the potential mitigation strategies that could reduce or remove the privacy impacts and risks identified during the privacy impact analysis step.
9.	**Recommendations:** From the steps referred to above, we refined our recommendations, designed to remove or reduce privacy risks.
10.	**Report:** We finalised this PIA report.

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

5.4 A glossary of defined terms and acronyms is at **Part E** of this PIA report.

6. Assumptions and qualifications

6.1 This PIA has been conducted from the perspective of Health, as the Commonwealth agency responsible for the implementation and operation of the App and the National COVIDSafe Data Store, and not from the perspective of any other agency or other entity.

6.2 In undertaking our PIA, we have assumed that all Users will be natural persons, and therefore will not be APP entities.

6.3 We have based our analysis in this PIA on the factual information in **Part C** of this PIA report, which has been confirmed by Health and DTA as correct. However, we are not ICT technical experts, and have not independently verified the accuracy and completeness of the information in **Part C**. In particular, we have not yet been provided with final versions of the content or order of screens (although we have made recommendations that will assist with these matters).

6.4 We have not in this PIA considered:

6.4.1 the ability of Public Health Officials to collect personal information about Positive Users, or their ability to use that personal information (including to contact the Positive User), or to disclose that information to Health, as custodian of the National COVIDSafe Data Store; and

6.4.2 the use by Contact Tracers of personal information after it is obtained from the National COVIDSafe Data Store (although we have in this PIA considered several strategies which could be used to enhance privacy protections for Users).

6.5 We are aware of the importance of the need for privacy protections to be built into every aspect of the system, including information flows and processes involving the States and Territories that are outside the scope of this PIA. We note that the use of the App may have

privacy impacts associated with State and Territory compliance with applicable privacy laws, such as those associated with increased volume of tracing information or changes to practices to accommodate this new data source. Despite these information flows and privacy risks being out of scope, we believe a number of our recommendations may assist in mitigating some of the associated potential risks.

6.6 Given the timeframes available for the conduct of this PIA, we have also not considered any personal information about Public Health Officials or Contact Tracers which may be collected by Health (e.g. information required to grant or maintain access to the National COVIDSafe Data Store), or the creation of user accounts for, or audit logs in relation to, access to the National COVIDSafe Data Store. We can do so at a later stage, if required.

"Point in time" analysis of the App

6.7 We have undertaken our analysis on the basis of the development of the App as at the time of this PIA report. As the design of the App evolves, or if there are likely to involve changes to any of the information flows discussed in this PIA report, we **recommend** that Health continue to carefully consider privacy impacts of those changes, including through a supplementary PIA process to update or supplement this PIA report as required by the APP Code. This will also enhance protections against the risk of "function creep", where information which is collected for one purpose starts to be used for another purpose which was not originally anticipated (**Recommendation 2**).

6.8 We note that these risks associated with "function creep" could also be potentially limited through a legislative framework, if one were to be introduced (**Recommendation 3**).

Part C PROJECT DESCRIPTION AND INFORMATION FLOWS

7. Why is the App being developed?

7.1 As part of the nationally coordinated government response to the COVID-19 pandemic, each State and Territory has already implemented procedures designed to reduce the further spread of COVID-19 in Australia. These procedures include contact tracing processes, where if an individual has tested positive to COVID-19, officials from relevant State and Territory health agencies contact that individual to investigate, and if possible, identify other individuals who may have been in contact with the affected individual, and may therefore have been exposed to COVID-19.

7.2 The current contact tracing processes require State and Territory officials to rely on the affected individual's memory. The individual is asked to recall their movements, and details about who they may have been in contact with, during the previous 21 days. The officials then contact any individuals who have been identified by the affected individual to offer advice and assistance, and to take steps required to reduce the risk of further spread of COVID-19. For example, depending on the situation, the officials may recommend or require monitoring of COVID-19 symptoms, COVID-19 testing, and/or the imposition of self-isolation requirements.

7.3 To complement the existing contact tracing processes, the Australian Government is developing the App, with the intention of facilitating faster and more accurate tracing of contacts of an individual who has contracted COVID-19. This is to assist in slowing the spread of COVID-19 in Australia. In this way, the Australian Government hopes that the App will save the lives of more people in Australia.

7.4 The technical development of the App is being led by DTA, on behalf of the Australian Government. Amazon Web Services (**AWS**), under a contract with DTA, will assist in developing the App, and will supply the infrastructure and associated support services for the National COVIDSafe Data Store. DTA will make the infrastructure and support services for the National COVIDSafe Data Store available as a service to Health.

8. How will the App work?

8.1 This section reflects our understanding of the current design of the App. We expect that the design of the App will continue to evolve before it is released to the public, including to take into account the recommendations set out in this PIA report.

8.2 We have identified the following 7 steps associated with the use of the App:

Step 1: User downloads the App

8.3 The User will download the App from a relevant application store, and install the App on their mobile phone or other device.

8.4 When the User opens the App for the first time, information will be displayed to the User about the App, including about how personal information will be collected, stored, used and disclosed in connection with the App (**Registration Notice**). If the User wishes to proceed with using the App, they will need to agree to the terms in the Registration Notice.

8.5 If the User agrees to the terms in the Registration Notice, they will be asked to input the following information:

8.5.1 their full name;

8.5.2 their mobile phone number;

8.5.3 their postcode; and

8.5.4 their age.

8.6 The User will be asked to input their full name, their postcode and their age into the App.

8.7 If a User indicates that they are under 16 years of age (**Child User**), the Child User will see an additional screen on the App. This additional screen will require the Child User to confirm that their parent/guardian has consented to Health collecting the Child User's information. Once the Child User confirms they have received their parent/guardian's consent, the registration process will continue in the same manner as for other Users who are not Child Users (as below).[2] If the Child User does not provide this confirmation, they cannot continue with the registration process.

8.8 The User will be asked to then input their mobile phone number into the App. The User's mobile phone number will then be sent to the National COVIDSafe Data Store to be verified, and a one-time six-digit PIN will be sent via SMS text message to the User's device. After correctly entering the PIN into the App, the information entered by the User as specified in paragraph 8.5 (**Registration Information**) will be sent to the National COVIDSafe Data Store from the App. The Registration Information will, at this stage, be stored in an encrypted form in the National COVIDSafe Data Store. The National COVIDSafe Data Store will generate a temporary unique identifier for the User's mobile phone number (**Unique ID**), which is stored in the App (as discussed further in paragraph 8.17).

8.9 The User will not be able to access or change their Registration Information using the App. If they wish to do so, they will have to uninstall the App, re-install the App, and begin the registration process again.

8.10 After the User provides their Registration Information, the User will be prompted to enable their device's Bluetooth. They will also be advised that for the App to work, Bluetooth technology will need to be enabled on the User's device. If the User does not enable Bluetooth, the App will run, but will not collect any Digital Handshakes.

8.11 The App will indicate that it is running through a Bluetooth shield pulsing and wording appearing on the screen of the device. If the User turns off Bluetooth at any time after installing the App, the App will automatically prompt the User to keep Bluetooth on (e.g. a message similar to *"Turned off Bluetooth by mistake? Help stop the spread of COVID-19 by keeping your phone's Bluetooth on until the outbreak is over"*).

8.12 After entering the Registration Information and enabling Bluetooth, the App will be able to be used by the User.

8.13 At any time after downloading and installing the App, the User may uninstall the App from their device. If the User uninstalls the App:

8.13.1 the User will have to, if they wish to use the App again, re-install the App and begin the registration process again, including re-inputting their Registration Information; and

8.13.2 their Registration Information in the National COVIDSafe Data Store will not be automatically deleted. The User may request Health to delete their Registration Information from the National COVIDSafe Data Store.

[2] In this PIA report, any references to 'Users', 'Positive Users', or 'Contact Users', includes 'Child Users', unless specified otherwise.

Step 2: Push notifications and Unique ID

8.14 After the User provides their Registration Information, the User will be prompted to enable push notifications for the App. The App will generate a daily push notification to Users to remind them to use the App when they are out and about. If the User does not enable push notifications, or the User's device is in 'do not disturb' mode, the App will continue to run.

8.15 These push notifications are built into the design of the App and are triggered on the User's device itself, noting that push notifications are sent at regular intervals throughout the day. The push notifications are not controlled by, and do not require the transfer of any data from, or to, any external server.

8.16 The App will contain screens that allow the User to check whether or not Bluetooth is enabled for their device.

8.17 We understand that the National COVIDSafe Data Store will automatically generate new Unique IDs for each User every two hours and send these new Unique IDs to the User's App.

8.18 The App will only accept the new Unique IDs if it is open and running. If the App successfully accepts the new Unique ID, an automatic message will be generated and sent back to the National COVIDSafe Data Store. This message will only effectively indicate a "yes (new Unique ID successfully delivered)" response to the National COVIDSafe Data Store. If the App is not open and running, it will not be able to accept a new Unique ID. It will continue to store the previous Unique ID and use this when the App is opened, until a new Unique ID is generated and accepted.

8.19 The National COVIDSafe Data Store will regularly compile and store reports (**Unique ID Reports**), based on whether the new Unique ID for a User has been accepted by the App, which will give a measure of what proportion of Users who have downloaded the App have it open and running. These Unique ID Reports will not include any information about which Users have the App open and running, or where any Users are located.

8.20 The Unique ID Reports will be sent to Health, in its role as data custodian of the National COVIDSafe Data Store. Health will use the information in the Unique ID Reports to gauge the extent to which the App is being properly used across all of Australia and to determine whether further communication to the public is necessary (for example, if usage rates are very low, even though download rates are high, Health may decide to implement additional communication strategies about how to use the App).

Step 3: Creation of "Digital Handshakes"

8.21 After the registration process is complete, if the User's App is open and running on the User's device, the App will use the enabled Bluetooth technology to continually seek out Bluetooth signals from other Apps that are open and running on the devices of other Users. When a Bluetooth signal of a User's device detects the Bluetooth signal of another User's device, each User's App will create an encrypted file (a **Digital Handshake**) and store this on the User's device.

8.22 Each User will then be a "**Contact User**" of the other User.

8.23 Digital Handshakes operate most effectively when the User's device has the screen unlocked. If the screen is locked, not all contact with other Users will create a Digital Handshake, even if the Users are within the defined proximity for the defined time period.

8.24 A Digital Handshake will only include the following information (stored in an encrypted form on the User's device):

8.24.1 that there was contact between the User and the Contact User;

8.24.2 the Contact User's Unique ID;

8.24.3 the Bluetooth signal strength during the Digital Handshake; and

8.24.4 the date and time of the Digital Handshake.

8.25 A separate Digital Handshake is created every minute.

8.26 Importantly, no geolocation data of either the Contact User or the User will be included in a Digital Handshake. A Digital Handshake will not record where the contact between the Contact User and the User took place, or for how long the contact took place.

8.27 The Digital Handshake will be stored as encrypted information on the User's device, and for as long as it is stored on the User's device, it cannot be accessed by the User, any Contact User, or any Public Health Officials or Contact Tracers.

8.28 Each Digital Handshake will be automatically deleted from a User's device, 21 days after that Digital Handshake was created.

8.29 For clarity, the App will only create Digital Handshakes after the User has started using the App (there can be no creation of Digital Handshakes in relation to any retrospective contact with another person before the User has started using the App).

8.30 If the User uninstalls the App from their device, all Digital Handshakes stored on the User's device will be permanently deleted. However, any Digital Handshakes which are stored on a Contact User's device will not be deleted (they will remain on the Contact User's device for the usual 21 day period). Further, any Digital Handshakes that have already been uploaded to the National COVIDSafe Data Store (as described in paragraph 8.37 in **Step 4** below) will not be deleted. However, as specified above in paragraph 8.13.2, the User may request for their Registration Information and Digital Handshakes to be deleted from the National COVIDSafe Data Store.

Step 4: User tests as positive for COVID-19

8.31 At any point after downloading the App, the User may undertake a test to determine if they have contracted COVID-19. As part of taking such a test, the User will be required to provide information about themselves (this could be provided to, for example, their medical practitioner, a respiratory clinic, and/or a pathology laboratory). If the User tests positive, this information is provided to, and collected by, the relevant State or Territory Public Health Officials.[3]

8.32 In accordance with the current contact tracing processes, the relevant Public Health Officials will use the information they have been provided in order to contact the affected User (who will be a **Positive User**).[4]

8.33 After the App has been released by the Australian Government, the Public Health Official will ask the Positive User whether they have been using the App. If the Positive User indicates that they have not been using the App, the Public Health Official will refer the Positive User to the Contact Tracer to continue with the currently implemented contact tracing processes.

8.34 If the Positive User indicates that they have been using the App, the Public Health Official will ask the Positive User:

8.34.1 to click on 'Upload my data' in the App;

8.34.2 for permission to send the Positive User a notification to the Positive User's device, containing a one-time six-digit PIN to input into the App; and

8.34.3 to confirm the Positive User's mobile phone number to which this notification should be sent.

[3] These disclosures and associated collections are out of scope for this PIA.
[4] As above, this use is out of scope.

8.35 If the Positive User agrees, the Public Health Official will then enter the mobile phone number into the State and Territory Portal to generate and send a notification via SMS to the Positive User's mobile phone, containing a one-time six-digit PIN.

8.36 The Positive User will then be required, in the App, to read through information about the collection of Digital Handshakes stored on the Positive User's device that were created in the previous 21 days (as any Digital Handshakes created prior to that time will have been automatically deleted from the Positive User's device) (**Confirmation Notification**).

8.37 If the Positive User clicks 'Continue' after reading the Confirmation Notification, and then successfully inputs the six-digit pin into the App, all Digital Handshakes currently stored on the Positive User's device will be uploaded by the App to the National COVIDSafe Data Store. All information in paragraph 8.24 above will therefore be uploaded to the National COVIDSafe Data Store. Once the Digital Handshakes have been uploaded by the App to the National COVIDSafe Data Store, these Digital Handshakes will be deleted from the Positive User's device. The Public Health Official will then refer the Positive User to the Contact Tracer to continue with the currently implemented contact tracing processes.

8.38 Public Health Officials and Contact Tracers will be unable to enter any data into the National COVIDSafe Data Store other than the mobile phone number of a person to generate a PIN.

Step 5: Storage in the National COVIDSafe Data Store

8.39 Once the Positive User's Digital Handshakes are uploaded to the National COVIDSafe Data Store, the National COVIDSafe Data Store will attach the Positive User's Unique ID with their Registration Information, and each Contact User's Unique ID with their Registration Information. Once a User's Unique ID is attached to the User's Registration Information, this information will be de-encrypted for use by the Contact Tracer (as discussed below in **Step 6**).

8.40 The National COVIDSafe Data Store is a repository for data which will be stored in a cloud-based environment certified to the "Protected" security level.

8.41 The Australian Government intends that:

8.41.1 Health will be the Commonwealth agency responsible for operating and managing the National COVIDSafe Data Store;

8.41.2 Health will be the data custodian of all information stored in the National COVIDSafe Data Store;

8.41.3 only authorised State and Territory Contact Tracers, responsible for undertaking contact tracing in connection with Positive Users, will be permitted to access the information stored in the National COVIDSafe Data Store;

8.41.4 Health, based on advice from the States and Territories, will be responsible for controlling access to the National COVIDSafe Data Store;

8.41.5 neither Health, nor any other Commonwealth agency (other than DTA in its role as ICT service provider), will access or use the information stored in the National COVIDSafe Data Store (except as authorised in the circumstances in paragraph 8.45); and

8.41.6 any access to the National COVIDSafe Data Store will only be for the period that contact tracing is required to be undertaken in connection with the COVID-19 pandemic.

8.42 The Australian Government has also made clear public statements that the information in the National COVIDSafe Data Store is not intended to be used for the purposes of compliance or enforcement of self-isolation or other COVID-19 restrictions on the movement of individuals.

8.43 ICT support services for the National COVIDSafe Data Store will be provided by:

8.43.1 AWS, in respect of the infrastructure, in accordance with the contract between DTA and AWS; and

8.43.2 DTA, in respect of the interactions between the App and the National COVIDSafe Data Store.

8.44 All data in the National COVIDSafe Data Store will be held in an encrypted form.

8.45 A User will be able to request that Health provide them with information about themselves that is held in the National COVIDSafe Data Store (unless an applicable exception in APP 12 applies).

8.46 If any User uninstalls the App from their device, this will not delete any information held in the National COVIDSafe Data Store (including information about a Positive User or any of their Contact Users).

Step 6: Contact Tracers access and use Digital Handshake information in the National COVIDSafe Data Store

8.47 An authorised State or Territory Contact Tracer will be able to access the National COVIDSafe Data Store and see the unencrypted Digital Handshake information for all Positive Users in their State or Territory.

8.48 The Contact Tracer will then use the information in the Digital Handshake to:

8.48.1 identify the mobile phone numbers of the Positive User's Contact Users, so that the Contact Users can be contacted for contact tracing purposes;

8.48.2 prioritise contacting those Contact Users, based on a risk profile determined by the Contact Tracer, including taking into account:

(a) the age of the Contact User (noting that older Contact Users will have a higher risk profile, and therefore need to be contacted with greater priority); and

(b) the postcode of the Contact User (noting that Contact users from known "hot spots" where there appears to be a localised outbreak of COVID-19, will need to be contacted with greater priority); and

8.48.3 telephone the Contact Users to notify them that they have been in close contact with someone who has tested positive for COVID-19, and provide them with advice on how to manage their health status (e.g. information about whether they should get tested for COVID-19 or take any further steps).

8.49 In accordance with the current contact tracing processes, the Australian Government intends that the Contact Tracer will not provide the Contact User with any personal information relating to the Positive User. That is, a Contact User will be informed that their App has identified them as someone who may have been in close contact with a Positive User, but will not indicate the name of the Positive User, or when or where the contact occurred.

8.50 Contact Tracers will be able to copy or extract data from the National COVIDSafe Data Store. This means that Contact Tracers will be able to use information accessed in the National COVIDSafe Data Store to create their own records, which they may subsequently store and use in State and Territory systems or other repositories.

9. Analysis of personal information, sensitive information and health information

9.1 In this section, we consider the nature of the various types of information that are being generated as part of the steps identified in paragraph 7.4 above.

Relevant Definitions

9.2 Section 6(1) of the Privacy Act defines "personal information" as

> ***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.

9.3 Section 6(1) of the Privacy Act defines "sensitive information" as:

> ***sensitive information*** means:
> (a) information or an opinion about an individual's:
> (i) racial or ethnic origin; or
> (ii) political opinions; or
> (iii) membership of a political association; or
> (iv) religious beliefs or affiliations; or
> (v) philosophical beliefs; or
> (vi) membership of a professional or trade association; or
> (vii) membership of a trade union; or
> (viii) sexual orientation or practices; or
> (ix) criminal record;
> that is also personal information; or
> (b) health information about an individual; or
> (c) genetic information about an individual that is not otherwise health information; or
> (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
> (e) biometric templates.

9.4 Section 6FA of the Privacy Act defines "health information" as:

> (a) information or an opinion about:
> (i) the health, including an illness, disability or injury, (at any time) of an individual; or
> (ii) an individual's expressed wishes about the future provision of health services to the individual; or
> (iii) a health service provided, or to be provided, to an individual;
> that is also personal information;
> (b) other personal information collected to provide, or in providing, a health service to an individual;
> (c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances;
> (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual

Different types of information

9.5 **Registration Information (Step 1):**

9.5.1 The Registration Information will include the User's first and last name. We therefore consider that because the identity of the User may be ascertained from the Registration Information, the Registration Information will be personal information.

9.5.2 Even if a User uses a pseudonym, their Registration Information may be personal information as an individual may be identifiable from their mobile phone number.

9.5.3 However, we note that the Registration Information will not include any health information or other sensitive information.[5]

9.6 **Unique ID (Step 2)**:

9.6.1 We understand that after generation of the Unique ID and acceptance of it by the User's phone, the Unique ID will be stored in both the National COVIDSafe Data Store, and on a User's device.

9.6.2 For the Unique ID to be personal information, it must be information or an opinion about an individual who is identified or reasonably identifiable.

9.6.3 We note that the Unique ID is an encrypted version of the User's mobile phone number and could not, by itself, be used to identify the User or any other individual.

9.6.4 However, when stored in the National COVIDSafe Data Store, the Unique ID will be necessarily linked to the User's account where their Registration Information will be stored. In our view, this means that the identity of the User could be reasonably ascertained from the Unique ID by persons with the relevant access to the National COVIDSafe Data Store. This means that the Unique ID should therefore be treated as personal information, when stored in the National COVIDSafe Data Store.

9.6.5 When the Unique ID is stored on the User's device, it will not be able to be accessed by the User (or the National COVIDSafe Data Store). It will also not allow identification of the User (it might allow identification of a mobile phone number if it could be decrypted). We therefore do not consider that the Unique ID stored on the User's device should be considered as personal information.

9.7 **Unique ID Reports (Step 2):**

9.7.1 A Unique ID Report will be a consolidated report setting out the number of Unique IDs that have been successfully accepted, compared to the number of Unique IDs issued for which an acceptance message was not generated (e.g. because they did not have the App open and running at the time of the Unique ID change).

9.7.2 We are instructed that a Unique ID Report will not include any information about which Users have the App open and running (or any other information drawn from Users' Registration Information, e.g., information about which postcodes have high numbers of people using the App). As Unique ID Reports will not have any information about any identified User, or information from which a User may be reasonably identified, they will not contain any personal information.

9.7.3 However, we **recommend** that:

(a) Health obtain assurance (e.g. through DTA or examination of the specifications for the National COVIDSafe Data Store) that it will not be possible to generate Unique ID Reports which do use the Registration Information of Users to identify individual Users who are using the App (and/or individual Users who have downloaded but are not using the App); and

(b) Health should publicly commit to not using the Unique IDs in such a way (e.g. as part of a frequently asked questions (**FAQ**) page on its website) (**Recommendation 10**).

[5] But see paragraph 8.11.2 below.

9.8 **Information in a Digital Handshake stored on a User's device (Step 3):**

9.8.1 In the creation of a Digital Handshake, each User's device will collect the Unique ID of the Contact User, and record this together with information about the date and time of the contact, and the strength of the Bluetooth signal during the Digital Handshake.

9.8.2 When the Digital Handshake is stored on the devices of both the User and the Contact User, it will be stored in an encrypted form. It would only be able to be accessed by a holder of the correct encryption keys (which are generated by and stored in the National COVIDSafe Data Store). The information in the Digital Handshake will not be able to be accessed by the User, or the Contact User, or any Public Health Official or Contact Tracer, whilst it is stored on the devices of the User and the Contact User.

9.8.3 We therefore consider that, for as long as the Digital Handshake is stored on the devices of the User and Contact User, no individual will be able to be identified from the Digital Handshake.

9.8.4 We have also considered the risk of an unauthorised person (e.g., a hacker) being able to access the Digital Handshake information on a device, work out the relevant encryption keys, and then as a result, put this information together with other personal information to identify either the User or the Contact User. If such a risk was sufficiently great, then the identity of the User or a Contact User could be said to be "reasonably identifiable" from the Digital Handshake, with the result that the Digital Handshake information should be considered as personal information.

9.8.5 We have considered the risks of unauthorised access further in relation to APP 11 in **Part D** of this report. As further discussed in **Part D**, we consider the implementation of **Recommendation 14,** together with the risk mitigation strategies that have already been put in place (including to limit the amount of encrypted personal information held on the Contact User's device and the regular changing of the Unique ID[6]), will significantly reduce the risks associated with unauthorised access to the encrypted Digital Handshakes. This means that the identities of the User or Contact User in the encrypted Digital Handshake will not be "reasonably identifiable".

9.8.6 We are therefore satisfied that the encrypted Digital Handshakes on the devices of the User or the Contact User will not be personal information.

9.9 **Information about a Positive User collected by Public Health Officials as a result of COVID-19 testing (Step 4):**

9.9.1 Although it is out of scope for this PIA, we note that Public Health Officials will collect personal information from Users who test positive for COVID-19. Public Health Officials will also collect information about the Positive User's illness, and may also collect other personal information in order to provide a health service (as defined in the Privacy Act) to the Positive User. This information will be "health information" and therefore "sensitive information" for the purposes of the Privacy Act.

9.10 **Digital Handshake information uploaded to the National COVIDSafe Data Store (Step 5):**

9.10.1 Only Digital Handshake information of Positive Users (i.e., Users who have tested positive for COVID-19) will be uploaded to the National COVIDSafe Data Store.

[6] We note that if a User's App is not open and running, a new Unique ID will not be accepted during this time. When the App is again open and running, it will then be able to accept a new Unique ID sent from the National COVIDSafe Data Store. Users will then be able to take advantage of this additional security feature.

9.10.2 If the National COVIDSafe Data Store will record that a Public Health Official has entered the mobile phone number of a Positive User to generate the one-time six-digit PIN, the Positive User's Registration Information should be treated at this point as personal information which is also health information and therefore sensitive information. This is because information about their health (i.e. that they have COVID-19) can be inferred (regardless of whether the Positive User inputs the PIN and uploads their Digital Handshake information).

9.10.3 Authorised Contact Tracers will be able to access and extract all of the unencrypted Digital Handshake information in their State or Territory, together with the Registration Information of the Positive User and each Contact User. As discussed above, both the unencrypted Digital Handshake information and the Registration Information will be personal information.

9.10.4 In addition, when accessing the Digital Handshake information and Registration Information in the National COVIDSafe Data Store, the Contact Tracers will necessarily know that the accessed information relates to the identified Positive User (who has the COVID-19 disease), or an identified person who has been in contact with a Positive User and therefore who has a risk of having the COVID-19 disease. In other words, the accessed Digital Handshake information and Registration Information will convey health information, in addition to personal information.

9.10.5 We therefore consider that the Digital Handshake information and Registration Information should be treated at this point as personal information which is also health information, and therefore sensitive information. This is because in the case of Positive Users, information about their health (i.e. that they have COVID-19) can be inferred. In the case of Contact Users, we consider that health service information can be inferred (i.e. the individual's desire to receive a health service to assess their health).

9.10.6 For completeness, we note that the Contact Tracers are also likely to collect additional personal information and health information from Positive Users and their Contact Users during their contact tracing procedures, but this subsequent collection is outside the scope of this PIA.

10. Analysis of collections of personal information

10.1 In this section, we consider whether or not certain information flows between entities should be considered as:

10.1.1 a disclosure of personal information by one entity to another entity, with an associated collection of that personal information by the second entity; or

10.1.2 a use of personal information by the first entity.

General principles

10.2 Guidance from the OAIC indicates that, in some limited circumstances, disclosure to a contractor to perform services may be a considered a use by the relevant APP entity, rather than a disclosure to that contractor and a collection by that contractor. The guidance indicates that the key feature for such circumstances to apply is that the relevant APP entity does not release the personal information from its effective control. The guidance also notes that there should be:

10.2.1 a binding contract between the entity and the provider, which requires that the provider only handles the personal information for these limited purposes;

10.2.2 provisions in the contract, which require any subcontractors to agree to the same obligations, and

10.2.3 provisions in the contract, which give the entity effective control of how the information is handled by the provider. Issues to consider include:

(a) whether the entity retains the right or power to access, change or retrieve the information;

(b) who else will be able to access the information and for what purposes;

(c) the security measures that will be used for the storage and management of the personal information; and

(d) whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

AWS provision of cloud-based infrastructure and support for the National COVIDSafe Data Store

10.3 We understand that there is a contract between DTA and AWS (**AWS Contract**), under which AWS will be contracted to develop the App, and to supply as a cloud service the infrastructure and associated support services for the National COVIDSafe Data Store.

10.4 We understand that the AWS Contact will contain:

10.4.1 detailed functional and non-functional requirements for the App and the National COVIDSafe Data Store infrastructure;

10.4.2 detailed security requirements about the storage of information in the App and on the National COVIDSafe Data Store infrastructure, including encryption requirements, and obligations on AWS in relation to security, confidentiality and privacy requirements;

10.4.3 detailed support requirements, which limit access to the National COVIDSafe Data Store to AWS' authorised support personnel who need that access for the purposes of providing the contracted support;

10.4.4 in accordance with provisions which are commonly found in contracts for provision of cloud-based infrastructure, requirements under which:

(a) AWS is not responsible for the management of data content stored in the National COVIDSafe Data Store;

(b) the Commonwealth of Australia (acting through DTA) is given the necessary rights and powers to control access to, change, or retrieve, the information in the National COVIDSafe Data Store, so as to reflect that the Commonwealth and not AWS has effective control of the information, and how it is handled by AWS; and

(c) AWS will allow the Commonwealth to remove data content stored in the National COVIDSafe Data Store after the end of the AWS Contract, after which time it will be deleted if not removed.

10.5 If such provisions are included, we consider that this will assist in supporting a conclusion that any potential access to the National COVIDSafe Data Store by AWS, for the purposes of providing the cloud-based infrastructure and associated support services, can be categorised as a use by the Commonwealth (DTA), rather than a disclosure to, and collection by, AWS.

10.6 However, such an analysis depends on the nature of the services being undertaken by AWS (i.e., limited to infrastructure support services and not data analysis services) and there being appropriate provisions in the AWS Contract. Accordingly, we **recommend** that Health take steps to investigate and confirm the arrangements in relation to the role of AWS. This could be through Health undertaking a review of the AWS Contract, or ensuring that relevant

provisions are included in appropriate arrangements between DTA and Health (such as an MOU or other suitable administrative arrangements), as discussed below.

10.7 We **recommend** that Health also satisfy itself that the AWS Contract contains provisions that:

10.7.1 reflect the provisions in paragraph 10.4;

10.7.2 require AWS to ensure that any obligations imposed upon AWS are also imposed upon any of AWS' subcontractors and/or its service providers; and

10.7.3 require AWS to ensure that no information from the National COVIDSafe Data Store is transferred outside it (e.g. to other parts of the AWS' infrastructure environment).

(**Recommendation 16**)[7]

Role of DTA in provision of AWS infrastructure to Health

10.8 We understand that the parties intend that Health will be the data custodian of all data uploaded to the National COVIDSafe Data Store, and that DTA's role will be limited to making the AWS infrastructure and support services (including provided to it under the AWS Contract) available to Health, as a service.

10.9 We **recommend** that DTA and Health agree and document a suitable MOU or other arrangement, as soon as possible (**Recommendation 17**). Such an MOU should:

10.9.1 if necessary, contain a confirmation from DTA that the AWS Contract contains the matters set out in paragraph 10.4 and 10.7 above; and

10.9.2 clarify DTA's role in providing the relevant infrastructure (through its contractor AWS) as a service by DTA to Health[8], so as to ensure that Health is given the necessary rights and powers to exercise (or to control the exercise) of the Commonwealth rights under the AWS Contract, and places appropriate restrictions on DTAs exercise of those rights except on the express instructions from Health. This will assist in establishing that Health (and not DTA) will have effective control of the information in the National COVIDSafe Data Store.

10.10 Despite the OAIC guidance referring to "a binding legal contract" between the provider and the APP entity, it will not be possible for Health and DTA to enter into a legally binding arrangement as they are both parts of the same legal entity, being the Commonwealth of Australia. We consider that it is appropriate, in these circumstances, to look at the substance of the arrangement between the parties, rather than the form.

10.11 If **Recommendation 17** is implemented, we consider these will support a conclusion that there will be no disclosure to, or collection of, personal information by DTA in connection with the National COVIDSafe Data Store.

[7] We have also recommended other matters be included in the AWS Contract in our analysis of APPs 8, 11 and 12 in **Part D** of this report.

[8] An alternative might be for Health to administer the AWS Contract on behalf of the Commonwealth instead of DTA (with appropriate arrangements made for payments to AWS under the Contract), but given DTA's integral role in developing and supporting the App and National COVIDSafe Data Store, this may not be practical.

11. Information flows

11.1 A simplified diagram outlining the information flows is provided at **Attachment 1** to this PIA report.

11.2 In summary:

11.2.1 Individual Users will enter Registration Information into their device upon installation of the App. Health, as data custodian of information in the National COVIDSafe Data Store, will **collect** this personal information, and arrange for it to be **used** to:

(a) send a message to the User to verify the mobile number of the User;

(b) store the Registration Information in the National COVIDSafe Data Store; and

(c) generate Unique IDs and send these to the User's device.

11.2.2 Health, as data custodian of the information in the National COVIDSafe Data Store, will arrange for the Unique IDs, and the messages sent from User's devices in response to a new Unique ID, to be **used** to generate the Unique ID Reports.

11.2.3 A User will collect and store from Contact Users their Unique ID, Bluetooth strength and time and date of the contact when their devices create a Digital Handshake. However, there is no collection, use or disclosure of this information by Health at this point.

11.2.4 State and Territory Public Health Officials will collect personal information and sensitive information from Users in connection with COVID-19 testing. However, this collection and subsequent use by the Public Health Officials is out of scope for this PIA.

11.2.5 State and Territory Public Health Officials will **use** the mobile phone number provided to them by Positive Users, by inputting this into the National COVIDSafe Data Store using the State/Territory portal to generate a PIN for the User to input into their App to upload the Digital Handshake information to the National COVIDSafe Data Store. The Digital Handshake information will be about the Positive User and their Contact Users.

11.2.6 Health, as data custodian of the National COVIDSafe Data Store, **collects** the Digital Handshake information and **uses** the Unique ID in the Digital Handshake information by linking it to the Registration Information of both the Positive User and their Contact Users.

11.2.7 Health, as data custodian of the National COVIDSafe Data Store, **discloses** Digital Handshake information (being personal information and sensitive information) by giving Contact Tracers access to that information.

11.2.8 State and Territory Contact Tracers **use** the accessed information for the purposes of undertaking their current contact tracing procedures. This includes contacting the Contact Users using the Digital Handshake information (this is out of scope for this PIA).

11.2.9 State and Territory Contact Tracers may also **use** the accessed information by extracting it from the National COVIDSafe Data Store to create their own records.

Part D APP COMPLIANCE

Below is a table containing a summary analysis of the key elements of the APPs that are relevant to the operation of the App. The analysis does not address those elements of the APPs which reflect Health's broader compliance obligations, but only considers those elements that specifically relate to implementation and operation of the App and the National COVIDSafe Data Store.

1. APP 1 – open and transparent management of personal information

Text of APP 1

1 Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Analysis of compliance with APP 1

1.1 APP 1 is intended to ensure that APP entities manage personal information in an open and transparent way. Implementation of APP 1 is a responsibility of Health.

1.2 Undertaking a PIA such as this one supports the notion that Health is taking reasonable steps to implement practices, procedures and systems to comply with the APPs, as required under APP 1.2(a) and the APP Code (which requires agencies to undertake a written PIA for all "high privacy risk" projects or initiatives that involve new or changed ways of handling personal information).

1.3 We understand that there is significant public interest in respect of the privacy protections that will be inbuilt into the App and that transparency about the privacy risks and associated protections will be paramount for building community trust and confidence. We understand from our literature review (including the information contained in **Attachment 2)** that, in particular, the community will be interested in:

1.3.1 how the handling of their personal information may have been impacted as a direct result of COVID-19 (i.e. whether COVID-19 means that privacy is now being treated differently by the Australian Government);

1.3.2 whether information about their location will be collected through the App;

1.3.3 whether their personal information will be used for enforcement and compliance purposes; and

1.3.4 whether their information will be deleted once the threat of COVID-19 has passed.

1.4 We have had the benefit of seeing some early findings from a survey recently undertaken by the OAIC, which indicate that a significant number of Australians believe their privacy is more at risk than usual following the COVID-19 outbreak. Individuals are now more concerned about the protection of their personal information – particularly location information and location tracking. The results indicate that, while a significant number of Australians agree there must be some concessions on privacy to help combat COVID-19, the general view is that the current situation should not exclude compliance with the Privacy Act. It is therefore paramount that Health takes steps to ensure, to the extent possible, there is openness and transparency about the steps that have been taken to ensure compliance with the Privacy Act in relation to the App and the National COVIDSafe Data Store.

1.5 In relation to transparency, we note the following:

1.5.1 The App is being developed using a 'privacy by design' approach, which means that the protection of individuals' right to privacy has been considered during the lifecycle of the App and necessary protections are being implemented to ensure that this fundamental right is not affected. In this regard, we have been very pleased to see that during our involvement with the development of the App as part of undertaking this PIA process, Health and the other Commonwealth agencies have taken our advice about privacy issues, risks and concerns, and then made decisions and changed the design of the App to mitigate against identified risks. We believe that a privacy by design approach has been taken to date.

1.5.2 The Australian Government has made very clear statements about the voluntary nature of the App, meaning that if individuals are not satisfied that there are sufficient privacy protections in place (or if they otherwise do not wish to use the App), they will not be required to use the App (noting that individuals have been asked to consider using the App as it will save the lives of people in Australia).

1.5.3 The App will not collect location data, and again the Australian Government has clearly indicated its intention that no information collected through the App will be used for compliance and enforcement purposes associated with COVID-19.

1.5.4 The App and the National COVIDSafe Data Store will be decommissioned once the threat from COVID-19 has passed, noting that all personal information in the National COVIDSafe Data Store will be deleted or de-identified at this point (subject to any requirements specific to information that is contained in a Commonwealth record (see APP 11 for further information about the deidentification and deletion of personal information)).

1.6 To allay the concerns set out in paragraph 1.3 above, Health should ensure that prior to using the App, individuals are clearly advised of:

1.6.1 the fact that use of the App is voluntary;

1.6.2 all intended collections, uses and disclosures of personal information, noting that Health should expressly state that, as has been made very clear in public statements, location data will not be collected and no information is intended to be used for enforcement and compliance purposes;

1.6.3 the security arrangements in place to ensure that personal information is protected from misuse, interference and loss, and from unauthorised access, modification or disclosure;

1.6.4 what might happen to Users as a result of their information being uploaded into the National COVIDSafe Data Store if they become a Positive User or a Contact User (e.g. they may be advised that they need to self-isolate and if they fail to self-isolate they may separately be given a fine by a member of a State or Territory police force, or be imprisoned)[9];

1.6.5 what will happen to personal information once the App is decommissioned; and

1.6.6 how an individual may make a complaint about how the App is handling their personal information.

1.7 Health should ensure that Users are aware of the matters set out in paragraph 1.6 above. For example, the information could be included in the notices to be provided to Users when seeking consent clearly set out this information (**Recommendation 6**), and/or in an App-specific Privacy Policy which we recommend be developed for the App (**App Privacy Policy)**, in paragraphs 1.11 to 1.14 below (**Recommendation 7**).

1.8 Health should also consider ensuring that its website contains all relevant information about the App, including a FAQ page, to ensure that potential and current Users are provided with as broad a range of information as possible (**Recommendation 9**).

1.9 Additionally, to increase public trust and confidence in the App, we **recommend** that Health consider publishing this PIA report and making the source code for the App publicly available. Given the length and detail of this PIA report, we also **recommend** that Health consider developing material which summarises the information in this report and making this publicly available (e.g. on its website). This will assist Health to demonstrate that it has taken a "privacy by design" approach to the development and implementation of the App, and allow individuals, if they wish, to examine in greater detail the protections that have been developed and included in connection with the App, before deciding whether they wish to use it (see **Recommendation 1**).

1.10 We note that the proposed model for the App is a centralised model (i.e. with all data being stored in a central repository), and that there may be other potential models that would involve more de-centralised approaches. We acknowledge the increased intrusiveness of a centralised model, but understand this has been balanced from a policy perspective against

[9] If a legislative framework was introduced to limit the ability to collect, use or disclose information through the App (so that potential enforcement could not flow from information uploaded to the National COVIDSafe Data Store), then this recommendation would not be required.

the ability of government to most effectively track potentially infected persons and to reduce the spread of COVID-19 in a manner consistent with the objects of the Privacy Act.

APP privacy policy

1.11 APP 1.3 provides that an APP entity must have a clearly expressed and up to date Privacy Policy that contains all information prescribed by APP 1.4.

1.12 We **recommend** that Health ensure that an App Privacy Policy is developed and made clearly available when using the App ensuring that it contains all information prescribed by APP 1.4 and that it also includes a link to Health's full Privacy Policy (**Recommendation 7**).

1.13 APP 1.5 provides that an APP entity must take such steps as are reasonable, in the circumstances, to make its Privacy Policy available free of charge, and in such form as is appropriate. We consider that if Health makes its Privacy Policy available via a link in the App (noting that the App is free to use), Health will comply with APP 1.5. We also suggest that Health make it available on or from its website.

1.14 APP 1.6 provides that if a person or body requests a copy of a Privacy Policy in a particular form (i.e. a hard copy), the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. We assume that Health will use the general procedures that it has in place to ensure compliance with APP 1.6 (i.e. if someone contacts Health and asks for a copy of the Privacy Policy in a different form, Health will manage the request in accordance with its existing procedures).

2. APP 2 – anonymity and pseudonymity

Text of APP 2

> **2 Australian Privacy Principle 2—anonymity and pseudonymity**
>
> 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
>
> 2.2 Subclause 2.1 does not apply if, in relation to that matter:
>
> (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
>
> (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Analysis of compliance with APP 2

2.1 APP 2.1 requires APP entities to give individuals the options of not identifying themselves, or of using a pseudonym, when dealing with the entity in relation to a particular matter, unless an exception under APP 2.2 applies.

2.2 APP 2.2(b) provides that APP 2.1 does not apply if it is impracticable for the APP entity to deal with individuals who have not identified themselves, or who have used a pseudonym.

2.3 Anonymity requires that an individual may deal with Health without providing any personal information or identifiers.[10] Pseudonymity requires that an individual may deal with Health by using a name, term or descriptor that is different to the individual's actual name.[11]

2.4 As discussed in relation to APP 3 below, we are satisfied that it is reasonable for Health to collect a name from Users, as the purpose of the App is to facilitate more efficient contact tracing, and Public Health Officials will require some form of identifier to ensure they are speaking with the right person when making telephone calls to Contact Users of a Positive User.

2.5 We acknowledge that anonymous use of the App is not possible as this would not enable Positive Users to be called by Contact Tracers.

2.6 However, we are of the view that, while it may be more inconvenient, it would not be impracticable for Health to deal with Users who use a pseudonym. A Public Health Official could just as easily use a pseudonym as a real name to identify that they are speaking with the person who downloaded and used the App, as long as the contact details are correct. This is because, so long as Public Health Officials are able, when making telephone calls to conduct contact tracing, to identify the Contact User by the same name provided in a Positive User's Digital Handshakes (for example, "Mickey Mouse") to ensure they are speaking to the right Contact User, Public Health Officials will be able to send the User the SMS notification with the one-time PIN to allow the upload of the Digital Handshake information to the National COVIDSafe Data Store.

2.7 Guidance from the OAIC states that an APP entity should ensure that, if applicable, individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.[12] Accordingly, we **recommend** that Health clearly and expressly notifies Users, before registering for use of the App, that they may, when providing their Registration Information, use a pseudonym (for example, a note under the name field could be included to clarify that the User can give a "fake name") **Recommendation 13**. Further, we **recommend** that Health, in its notices provided to Users when seeking consent and/or in the App Privacy Policy, indicate that Users may use a pseudonym (see **Recommendation 6** and **Recommendation 7**).

[10] APP Guidelines, Chapter 2, paragraph 2.4.
[11] APP Guidelines, Chapter 2, paragraph 2.6.
[12] APP Guidelines, Chapter 2, paragraph 2.12.

2.8 We note for completeness that an individual may wish to make a complaint about, or give feedback on, the App using other methods of contacting Health (i.e. not through use of the App). We assume that such complaints will be handled in accordance with Health's usual procedures and may be made anonymously (even if Health's ability to respond to that complaint may be more limited if it is made anonymously). If so, we consider this to be consistent with the requirements for APP 2 compliance.

3. APP 3 – collection of solicited personal information

Text of APP 3

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

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

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Analysis of compliance with APP 3

Application of APP 3

3.1 APP 3 only applies to personal information which is 'solicited' (APP 3.7). An APP entity 'solicits' personal information if it requests another entity (including an individual) to provide the personal information, or to provide a kind of information in which that personal information is included (section 6(1) of the Privacy Act). Personal information is also solicited if active steps are taken to facilitate the provision of personal information.[13]

3.2 In our view, all personal information that is collected in connection with the App will be solicited. The App will actively seek specific personal information from the User when it asks the User to input the Registration Information. The App will also take active steps to seek specific personal information from Positive Users, in connection with the creation of Digital Handshakes. Public Health Officials will actively seek the provision of Digital Handshake information (through the Confirmation Notice). Contact Tracers will seek the Digital Handshake information through access to the National COVIDSafe Data Store. Neither the App nor the National COVIDSafe Data Store contains any "free text" or other fields that might permit the unintended collection of unsolicited personal information.

Collection of personal information (other than sensitive information) (APP 3.1)

3.3 An agency, like Health, may only collect personal information (other than sensitive information) that is reasonably necessary for or directly related to one or more of the agency's functions or activities (APPs 3.1).[14]

3.4 This is an important part of ensuring that boundaries are set for the personal information that can and should be collected (and what can and should then be done with the data and for what purposes). The proposed purposes should be supported by evidence that the collection and use of the personal information actually addresses a particular need. In addition, the amount, manner and duration of the information collected, and then used and disclosed, should be relevant, necessary and proportionate to the desired objectives, and it is important to consider whether the same objectives could be reached with less information, or by using aggregated or anonymised data; and whether the approach is proportional to the goal that is trying to be achieved.[15]

3.5 Determining whether a collection of personal information is permitted under APP 3.1 requires a two-step process:

3.5.1 **Step 1** – identifying an APP entity's functions or activities; and

3.5.2 **Step 2** – determining whether the relevant collection of personal information is reasonably necessary for or directly related to one of those functions or activities.[16]

3.6 For **Step 1**, we note that Health's functions include administering matters in relation to "public health, including health protection", "health promotion and disease prevention", "specific health services, including human quarantine" and "biosecurity, in relation to human health" (*Administrative Arrangements Order*, effective 1 February 2020).

[13] APP Guidelines, Chapter 3, paragraphs 3.4 – 3.8.
[14] As none of the entities collecting personal information in the identified information flows will be "organisations" for the purposes of the Privacy Act, APP 3.2 is not relevant (but see our discussion in relation to the potential application of section 6F of the Privacy Act in our analysis of APP 6).
[15] See https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/04/covid-19_meets_privacy_a_case_study_for_accountability_-_centre_for_information_policy_leadership__april_2020_.pdf
[16] APP Guidelines, Chapter 3, paragraphs 3.8 – 3.9.

3.7 In accordance with these functions, Health's activities in relation to COVID-19 include working with the State and Territory governments to provide the best possible care, move resources to where they are needed, and ensure the approach to COVID-19 is consistent and integrated across the country. This includes ensuring that there are efficient and effective mechanisms in place to enable effective contact tracing, in order to reduce the further spread of COVID-19.

3.8 We understand that there is a real need for the current contact tracing processes to be streamlined, and for new procedures to be introduced so that less reliance is placed on the memory recall of individuals who test positive for COVID-19. In our view, Health's functions and activities therefore include making a system available to the States and Territories, with nationally consistent processes, which will enable quicker and more effective identification of persons who may have been in contact with someone who has tested positive for COVID-19.

3.9 In applying this to **Step 2**, we note that an objective test should be used to determine whether a collection of personal information is "reasonably necessary" for an APP entity's functions or activities (i.e. whether a reasonable person who is properly informed would agree that the collection is necessary). It is the responsibility of an APP entity to be able to justify that each particular collection is reasonably necessary. Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

3.9.1 the primary purpose of collection;

3.9.2 how the personal information will be used; and

3.9.3 whether the entity could undertake the function or activity without collecting that personal information.

3.10 The term "necessary" is not defined in the Privacy Act, and is interpreted in a practical sense. The High Court of Australia has noted that *"there is, in Australia, a long history of judicial and legislative use of the term "necessary", not as meaning essential or indispensable but as meaning reasonably appropriate and adapted"*.[17] However, the OAIC considers that in the context of the Privacy Act it would not be sufficient if the collection is merely helpful, desirable or convenient.[18] A collection, use or disclosure usually will not be considered "necessary" if there are reasonable alternatives available to handling information in that way, for example if de-identified information would be sufficient for the function or activity.[19]

3.11 To be "directly related to" an agency's functions or activities, a clear and direct connection must exist between the personal information being collected and an agency's functions or activities.

3.12 Best practice also 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.

3.13 We have considered below each type of personal information that will be collected by the App, when it will be collected, and whether that collection is reasonably necessary for and/or directly related to the functions and activities of Health, as described in paragraph 3.6 above. Each of the below types of personal information is collected and stored in the National COVIDSafe Data Store as part of the Registration Information collected immediately after installation of the App.

[17] *Mulholland v Australian Electoral Commissioner* [2004] HCA 41 per Gleeson CJ at paragraph 39.
[18] APP Guidelines, Chapter B, paragraph B.113.
[19] APP Guidelines, Chapter B, paragraph B.115.

3.13.1 **Mobile phone number** of the User/Contact User:

(a) This information will be collected:

(i) **Initially:** to enable the generation of a verification PIN which will be sent via SMS to the User's mobile phone number (which must be entered into the App as prompted to finalise the installation process, upload the Registration Information to the National COVIDSafe Data Store, and allow the App to be used); and

(ii) **Subsequently:** if a Positive User's Digital Handshake indicates that the User may have been in contact with the Positive User, for the Contact Tracer to telephone a Contact User.

(b) We have carefully considered whether it can be said to be reasonably necessary for the User's mobile number (and the other Registration Information described below), to be collected and stored in the National COVIDSafe Data Store at the initial point, given that there will be no need to use that information for contact tracing purposes unless and until there is a contact with a Positive User.

(c) Health and DTA have explained that the reason for doing so is because the only other viable alternative would be for all of the Registration Information to be stored (in an encrypted way) on the devices of each User, and then for all of the Registration Information to be included in the Digital Handshake information stored on Contact Users' devices. In Health's view, this would involve increased security and privacy risks, because it would involve a greater amount of information being stored on Users' devices which are unlikely to have the same level of security protections as the National COVIDSafe Data Store.

(d) While we agree that there is merit in this argument, we think it will be important to ensure that Users are fully aware of how their Registration Information will be collected and stored, before they enter that information into the App (**Recommendation 9**).

(e) In addition, we **recommend** that Health take steps to alleviate concerns that the Registration Information will be used in ways other than those contemplated in this PIA report. For example, Health could take steps to ensure that it will not be possible, either for the Australian Government or State and Territory governments (through their Public Health Officials or Contact Tracers) to access the Registration Information of a User before they have tested positive for COVID-19, or have been identified as a Contact User for someone who has tested positive. Health should also provide a public commitment that the Registration Information will not be used in this way (e.g. as part of a FAQ on its website) (**Recommendation 10**).

(f) The mobile phone number is also collected so that an SMS can be generated and sent to a Positive User, in order for them to be able to upload their Digital Handshake information if they agree. In our view, this is an important step in ensuring that the Positive User actively confirms their consent to upload the Digital Handshake information from their device to the National COVIDSafe Data Store. Accordingly, we consider that the collection of this information is reasonably necessary for, or directly related to, Health's functions and activities.

(g) We have also considered whether an alternative system might be possible so that mobile numbers are not required to be provided at all. For example, whether there could be a system under which the National COVIDSafe Data Store would simply send a push notification to Contact Users through the App if required. While this may avoid delays in the Contact Tracer telephoning the Contact User, we understand that such a system would involve additional unnecessary health risks for Contact Users because:

(i) a User can turn off push notifications, or the push notifications may be blocked by device IDs, so that a Contact User may not receive such an automatic message (meaning they would remain unaware of their contact with a Positive User)[20]; and

(ii) immediate human contact in a phone call with a Contact Tracer has the benefit of immediate communication with an informed person about health risks and mitigation strategies (meaning that any immediate health needs can be met, and health concerns and mental distress can be immediately addressed).

(h) In these circumstances, we consider that a reasonable person who is properly informed would consider that it is necessary for mobile phone numbers to be collected through the App.

3.13.2 **Age** of the User/Contact User:

(a) This information is only required once a case has been referred to a Contact Tracer. The discussion in paragraphs 3.13.1(b) to 3.13.1(e) therefore also applies to the initial collection of the User's age upon registration.

(b) If a Digital Handshake of a User is subsequently uploaded to the National COVIDSafe Data Store, the age is needed so that the Contact Tracer can prioritise telephone calls if a Positive User has a number of Digital Handshakes. Health has consulted the State and Territories and received medical advice that older persons have a higher risk of worse health outcomes if they contract COVID-19, compared to younger persons[21]. Therefore if a Positive User had many Digital Handshakes, there are benefits in the Contact Tracer being able to contact older persons first. Further, collecting a User's age will allow Public Health Officials and Contact Tracers to identify whether a Positive User or a Contact User is a Child User (i.e. under the age of 16) and accordingly, whether they need to take such steps as are appropriate (e.g. ask to speak to the Child User's parent/guardian) (**Recommendation 11**). We consider that a reasonable person who is properly informed would therefore consider that it is reasonably necessary for an indication of age to be collected.

(c) We have considered whether the precise age is reasonably required to obtain the benefit outlined above. Although we understand that consultations with State and Territory contact tracing units have requested that the precise age be used, we suggest that Health should consider whether this is supported by medical evidence, or whether the same benefits could be achieved by requiring Users to only nominate a bracket of ages into which the User falls (e.g. 16-20; 20-25; etc), with Contact Tracers prioritising calls to those within an older bracket before those in a younger bracket.

[20] We assume that it is not technically possible for the App to circumvent this risk so that push notifications cannot be disabled.
[21] This is consistent with advice in the CDNA National Guidelines for Public Health Units (https://www1.health.gov.au/internet/main/publishing.nsf/Content/cdna-song-novel-coronavirus.htm).

(d) Accordingly, we **recommend** that Health consider undertaking further consultation as required about whether it should change the proposed design of the App so that only an age range of the User is collected through the App (**Recommendation 5**). If there is no clear medical reason for collecting the precise age, using an age range would enhance compliance with APP 3, and have the additional benefits of being consistent with the data minimisation principle, and further reduce risks of more precise personal data being disclosed if there was to be a data breach.

3.13.3 **First and last name** of the User/Contact User:

(a) This information is only required once a case has been referred to a Contact Tracer. The discussion in paragraphs 3.13.1(b) to 3.13.1(e) therefore also applies to the initial collection of the User's name upon registration.

(b) This information is sought in order to enable the Contact Tracer to confirm that they are speaking to the person who downloaded and used the App, if they telephone a Contact User as a result of a Digital Handshake. For example, there may be risk that another person (for example, in the same household) could answer the call made to the mobile phone number.

(c) We have considered whether it is reasonably necessary to collect both the first and last names of the User, or whether the identified benefits could be obtained by only collecting the first name. We are aware that contact tracing apps used in some other jurisdictions, for example, in Singapore, do not collect the name of the User at all (the person doing the contact tracing in those jurisdictions simply has the phone number to call, and does not know who will be on the other end of the call).

(d) We agree that it will be important for the Contact Tracer to identify that they are speaking to the person who downloaded and used the App. Otherwise, there is a privacy risk that the Contact Tracer may disclose sensitive information (health information) to the wrong person.

(e) We agree that including both names will provide a greater level of confidence that the Contact Tracer is speaking with the appropriate person. We therefore think that it is reasonable to conclude that collection of both first and last names is reasonable to achieve Health's functions and activities (noting that if a pseudonym is used, as per our **Recommendation 13** in relation to APP 2, this would still allow the appropriate person to be ascertained).

3.13.4 **Postcode** of the User/Contact User:

(a) This information is only required once a case has been referred to a Contact Tracer. The discussion in paragraphs 3.13.1(b) to 3.13.1(e) therefore also applies to the initial collection of the User's postcode upon registration.

(b) This information is required to allow the National COVIDSafe Data Store to ensure that each State or Territory is only provided with access to information in the National COVIDSafe Data Store about residents of their State or Territory (for which they are responsible for undertaking contact tracing).

(c) It may also be used by Contact Tracers to prioritise calls to Contact Users, for example, if they are aware that there is a localised outbreak of COVID-19 in a particular postcode, calls to Contact Users with that postcode with a greater health risk can be prioritised.

(d) We have considered whether a larger region might be used instead (e.g. local council region) to reduce specificity, but understand that many Users may not easily be able to recall this information.

(e) We therefore consider that a reasonable person who is properly informed would consider that it is necessary for postcodes to be collected through the App.

3.13.5 **Unique ID of the User/Contact User:**

(a) This information is collected upon generation by the National COVIDSafe Data Store, and again if and when a Positive User's Digital Handshake information is uploaded to the National COVIDSafe Data Store.

(b) It is required to allow the National COVIDSafe Data Store to determine the appropriate Registration Information (as held in the National COVIDSafe Data Store) that relates to the two Users who have been in contact, and make this information accessible to authorised Contact Tracers. Without this Registration Information, the Contact Tracers will not be able to contact Users.

(c) We therefore consider that a reasonable person who is properly informed would consider that it is necessary for the Unique ID to be collected through the App.

3.13.6 **Time and date that the Digital Handshake was created:**

(a) This information is generated partly so that the App will know when to automatically delete a Digital Handshake (i.e. 21 days after creation).

(b) It is collected in the National COVIDSafe Data Store as part of a Digital Handshake so that the Contact Tracers can use this in order to prioritise calls to Contact Users, based on their clinical assessment of health risk. Knowledge about COVID-19 and risks of exposure (e.g. after symptoms develop) is increasing daily, and Contact Tracers will be able to use this knowledge to ensure an appropriate priority is given to those Contact Users who may have a more immediate need to take steps to prevent the further spread of COVID-19.

(c) We therefore consider that a reasonable person who is properly informed would consider that it is necessary for this information to be collected through the App.

3.13.7 **Bluetooth signal strength:**

(a) This information is only collected if and when a Positive User's Digital Handshake information is uploaded to the National COVIDSafe Data Store.

(b) This information is required in order to allow the Contact Tracers to assess the risks associated with a particular contact with a Positive User, prioritise calls to Contact Users (given the increased health risk associated with closer proximity), and work with Contact Users to determine the steps that need to be taken as a result of the contact with a Positive User.

(c) We therefore consider that a reasonable person who is properly informed would consider that it is necessary for this information to be collected through the App.

3.13.8 **Inferred information:**

(a) We note that inferences may be drawn from personal information which stored in the National COVIDSafe Data Store during the period of that storage (e.g. that a person has tested positive for COVID-19 or has a risk of being positive because of exposure to COVID-19). For the reasons explained in paragraph 9.10 of **Part C**, this inferred information will be health information which is sensitive information.

Collection of sensitive information (APP 3.3 and 3.4)

3.14 APP 3.3 provides that sensitive information may only be collected by Health if the individual consents to the collection of the information (and the information is reasonably necessary for, or directly related to, one or more of Health's functions or activities) or an exception under APP 3.4 applies. This will apply to all sensitive information, including inferred sensitive information.

3.15 Health is intending to implement a consent-based model for use of the App, and for all information flows resulting from use of the App. For the purposes of the APPs, consent is defined as 'express consent or implied consent'. Health does not intend to rely upon implied consent, but will seek the express consent as needed to collect personal information and facilitate the information flows. Similarly, Health does not intend to rely on any of the exceptions in APP 3.4.

3.16 The four key elements needed to establish consent are:

3.16.1 the individual is adequately informed before giving consent;

3.16.2 the individual gives consent voluntarily;

3.16.3 the consent is current and specific; and

3.16.4 the individual has the capacity to understand and communicate their consent.[22]

3.17 Each of these elements is discussed below.

3.18 **Informed:**

3.18.1 Before giving consent, an individual needs to be properly and clearly informed about how their personal information will be handled, so that they can decide whether or not to give their consent. They should be made aware of the implications if they provide or withhold their consent.[23]

3.18.2 Information should be written in plain English, without legal or industry jargon.

3.18.3 We **recommend** that:

(a) Health ensure that all Users are provided with sufficient information about how their personal information will be collected, and then used and disclosed for all information flows, before providing their consent to the collection of the Registration Information. In particular, Users should be clearly informed about how their information may be uploaded to the National COVIDSafe Data Store – this will be important to mitigate against privacy concerns that have been raised about Users who are potentially unaffected by COVID-19,

[22] APP Guidelines, Chapter B, paragraph B35.
[23] APP Guidelines, paragraph B.47.

losing control over their information[24] (**Recommendation 6** and **Recommendation 7**).

(b) Health ensure that Positive Users are provided with further information about how the Digital Handshake information (including information that will be inferred) will be handled, before they agree to upload that information to the National COVIDSafe Data Store (**Recommendation 6** and **Recommendation 7**).

(c) Health ensure that the sequencing of screens displayed to the User when registering to use the App and when they are asked for consideration to upload their Digital Handshake information, is such that the above information is provided to the User before they are asked to provide consent (**Recommendation 4**).

(d) Health consider developing training and/or a script for Public Health Officials to use when asking Positive Users to use their mobile number in the App to send them an SMS to upload their data, which clearly asks for permission to enter their mobile number into the National COVIDSafe Data Store in order to generate and send the SMS to the Positive User (**Recommendation 11**).

3.19 **Voluntary:**

3.19.1 For consent to be voluntary, the individual needs to have had a genuine opportunity to provide or withhold their consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will[25].

3.19.2 For example, it will be important to ensure that the Public Health Official makes it clear that the Positive User is not required to consent to either the SMS with the PIN number being sent, or to then consent to upload their Digital Handshakes to the National COVIDSafe Data Store. This will be particularly the case if the Public Health Official remains on the phone, or is in the same room, with the Positive User, and waits for the Positive User to choose to make their selection. Implementation of training and a script for Public Health Officials to use **Recommendation 11** (in paragraph 3.18.3(d) above) would mitigate this risk. Ideally, the Public Health Official should not be able to tell whether or not the Positive User has consented, or not consented to the upload of their Digital Handshakes (the script could simply require the Public Health Official to ask "*Have you made your choice?*" rather than "*Have you agreed to upload your Digital Handshakes?*"[26]

3.19.3 Ideally, all screens where the User is asked to provide consent should have options that would allow the User to either provide, or indicate that they do not provide, their consent. This would assist in supporting a voluntary consent process, by ensuring that the User is given a clear choice, with confirmation provided that their information has not been collected because they have chosen to provide their consent (e.g. a message that "*None of your information has been collected*"). However, if this functionality is not possible, at a minimum the User should be able to choose to return to the "home" screen of the App at any stage whilst using the App, which we understand to be the case.

3.19.4 The Australian Government has also given clear indications that it will not be mandatory for any person to install or to use the App. However, there may be a potential risk of circumstances in which a particular individual does feel pressured to download the App (e.g. a supermarket insisting on customers showing that they

[24] See https://eng.unimelb.edu.au/ingenium/research-stories/world-class-research/real-world-impact/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia.
[25] APP Guidelines, paragraph B.43.
[26] If a User chose not to input the PIN sent to them by the Public Health Official, this would be a decision to refuse consent.

are using the App before being permitted to enter the store; or an employer insisting that their employees demonstrate that they are using the App before being permitted to start or continue work).

3.19.5 We note that Health will have little control over such third parties. However, we **recommend** that Health issue appropriate written public communications about the voluntary nature of the App. Health may also wish to seek advice, including through consultation with AGD, the OAIC and the AHRC as appropriate, as to whether there are additional measures that could be put in place to protect the rights of individuals who to decide not to use the App (for example, actions such as those described in paragraph 3.19.4 may constitute a breach of human rights) (**Recommendation 3**). Finally, information could be included on the App about what to do if a User feels they have been pressured into using the App, unless a legislative framework is introduced to address this risk (**Recommendation 4**).

3.20 **Current and specific:**

3.20.1 Health should not assume that consents given in connection with the App will endure indefinitely, and it is good practice to inform the individual of the period for which the consent will be relied upon[27].

3.20.2 As discussed further in connection with APP 12, the Australian Government does not intend that any information in the National COVIDSafe Data Store will be accessed or used after the end of the COVID-19 pandemic. However, it is not possible to determine how long the COVID-19 pandemic will continue in Australia.

3.20.3 Accordingly, we **recommend** that Health consider imposing a time limit on the initial consent obtained in connection with the Registration Information (for example, 6 or 12 months), and ensuring that the functionality of the App will require a further consent notice to be displayed to the User after this time period, which must be accepted to allow further use of the App.

3.20.4 Health should ensure that consents are not broader than the purposes required.

(**Recommendation 6** and **Recommendation 7**)

3.21 **Capacity:**

3.21.1 For a consent to be valid, the person giving the consent must have capacity to understand the nature of the consent, form a view based on reasoned judgement, and communicate that consent. Consent may be an issue if, for example, the individual is a minor, has a physical or mental disability, or limited understanding of English.

Age

3.21.2 Guidance from the OAIC indicates that, if it is not practical for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, it may presume that an individual 15 and over has sufficient capacity to consent (unless the APP entity is aware of circumstances which would alter that presumption), and conversely, it should not be presumed that an individual aged under 15 has capacity to give consent.

3.21.3 In such a case, consent must be obtained from an adult (such as a parent/guardian) on behalf of the individual. It is important that the consent provided by the parent/guardian meets the four elements of consent (see paragraph 3.16 above) required for their consent to be sufficient.

[27] APP Guidelines, paragraph B 49.

3.21.4 As discussed in paragraph 8.7 of **Part C**, we understand that if a User, when entering their Registration Information, indicates they are under 16 years of age (i.e. they are a Child User), the App will direct the Child User to another screen on which they must confirm that their parent/guardian has consented to Health collecting the Child User's information via the App, before the Child User is able to continue with the registration process. This means that, unless the Child User confirms in the App that they have their parent/guardian's consent, no Registration Information or subsequent Digital Handshake Information will be sent to the National COVIDSafe Data Store.

3.21.5 We understand that this approach has been adopted to ensure that the consent of a parent/guardian is obtained, noting the nature of the App and the circumstances in which a child is likely to want to download it (noting that it is unlikely to be attractive to younger children, but teenagers may wish to use it in order to help combat COVID-19).

3.21.6 Nevertheless, we are concerned that there will be a lack of certainty as to whether a parent/guardian will have, in fact, given their consent (as it will be relatively easy for a child to tick a box to indicate that they have obtained their parent/ guardian's consent, without ever having done so). In addition, for the parent/guardian's consent to be informed, the parent/guardian should be informed about the information that will be collected about the Child User via the App, and how that information will be collected, used, disclosed, and deleted in connection with the App.

3.21.7 Information about a Child User which is uploaded to the National COVIDSafe Data Store will become sensitive information if the Child User becomes a Positive User, or a Positive User uploads Digital Handshake information about the Child User. Health should therefore be satisfied about the robustness of the consent on which it is relying to authorise the collection, and subsequent use or disclosure, of that sensitive information.

3.21.8 We therefore **recommend** that Health further consider the processes in the App if a User is a Child User, to strengthen the processes to ensure that informed consent is obtained from an adult on behalf of the Child User (**Recommendation 19**). There are different mechanisms that could be used. For example, a process of "verified consent" could be obtained from the parent/guardian. Such a process could involve the Child User providing their parent/guardian's mobile phone number or email address, with a message being generated and sent to their parent/guardian's device, with a PIN that must be inputted correctly into the Child User's App for their registration process to continue. The message sent to the parent/guardian could provide appropriate information to the parent/guardian about the handling of their child's personal information.

3.21.9 In addition, we note that the App does not currently contain a clear option for the Child User to indicate that they do not have the consent of their parent/guardian. Ideally, this would be included, with the Child User then being presented with an appropriate message (e.g. prompting them to uninstall the App).

3.21.10 We note that such a process would not remove all risk (a Child User could provide their own email address or the phone number of a friend). In addition, it would also involve additional collections and uses of the parent/guardian's mobile number or email address, that would need to be considered. Health may therefore wish to consult with further stakeholders, such as the OAIC and the eSafety Commissioner, about the different available options.

Disability and CALD community access

3.21.11 In accordance with usual Commonwealth practice, Health should ensure that the design and specifications for the App meet best practice accessibility requirements, which will facilitate those with a disability, or those from culturally and linguistically diverse communities, being able to understand the form of consent which is displayed to them.

3.22 **Withdrawal of consent:**

3.22.1 An individual should be able to withdraw their consent at any time, using an easy and accessible process.[28]

3.22.2 A User can easily delete the App from their device at any time. If this happens, the User's consent will be withdrawn, and no further information about the User will be collected.

3.22.3 However, deletion of the App will not delete, or de-identify, any Registration Information that has already been uploaded to the National COVIDSafe Data Store before the App is deleted.

3.22.4 In addition, there is no technical way for the User to be able to remove encrypted Digital Handshakes which have been created and stored on the devices of their Contact Users before they have deleted their App. Deleting the App will not prevent Digital Handshakes created in the previous 21 days from continuing to exist, or then being uploaded to the National COVIDSafe Data Store, if one of the Contact Users tests positive for COVID-19 in the following 21 days.

3.22.5 The OAIC guidance also indicates that once an individual has withdrawn consent, an APP entity should no longer rely on that past consent for any future use or disclosure of the individual's personal information. There is therefore a compliance risk in relation to the collection of sensitive information obtained in respect of Contact Users who have deleted the App.

3.22.6 To mitigate the impacts of this risk, we understand that there will be a functionality which will allow Users who have deleted the App and do not want their personal information in the National COVIDSafe Data Store, or held on other Contact User's devices to be used if uploaded to the National COVIDSafe Data Store, to register their mobile number that they had used in the App within a separate part of the National COVIDSafe Data Store. The National COVIDSafe Data Store will delete or de-identify all personal information associated with that mobile number (if this is consistent with the Archives Act).

3.22.7 If this is not possible because of Commonwealth record-keeping obligations, we suggest that further consideration be given as to whether there is an appropriate mechanism that could be implemented instead (e.g. whether it is feasible for a system where, before a Contact Tracer was able to access information in the National COVIDSafe Data Store, the system could automatically check the Digital Handshake information against the registered mobile numbers in the facility, and only release the Digital Handshake information for use if the User's number was not listed).

3.23 We also **recommend** that Health ensure that Users are made aware of the effect of deleting the App, and of the continuing nature of the consent after deletion for the limited time and purpose, as set out in **Part C**. This could be done in the notices provided to Users when seeking consent and/or the App Privacy Policy (see **Recommendation 6** and **Recommendation 7**).

[28] APP Guidelines, paragraph B.51.

Collection by fair and lawful means (APP 3.5)

3.24 Under APP 3.5, an APP entity must collect personal information "only by lawful and fair means". A collection of personal information is lawful if it is not contrary to law. Conversely, a means of collection will not be lawful if a law, legal order or legal principle prevents that means of collection. For example, a collection will be unlawful if it is:

3.24.1 in breach of legislation, such as computer hacking, using telephone interception or a listening device except under the authority of a warrant, or requesting or requiring information with, or for the purposes of, an act of discrimination;

3.24.2 by a means that would constitute a civil wrong, such as by trespassing on private property or threatening damage to a person unless information is provided; or

3.24.3 contrary to a court or tribunal order, such as an injunction issued against the collector.[29]

3.25 No law, legal order or legal principles prevent Health from collecting information as data custodian of the National COVIDSafe Data Store, so the collection is therefore by "lawful means".

3.26 A "fair means" of collecting personal information is one that is not oppressive, does not involve intimidation or deception, and is not unreasonably intrusive. Whether a collection uses unfair means would depend on the circumstances.[30]

3.27 We note that fairness of consent will depend on Health being open and transparent about the operation of the App any why particular information is being collected. Fairness also requires appropriate protections to guard against function creep. Collection of personal information about children should be particularly carefully examined, to make sure that the collection in the circumstances is "fair".[31]

3.28 We are satisfied that, if the recommendations in this PIA report are adopted, all collections of personal information by Health will be by "fair means" as required by APP 3.5, particularly if the recommendations in paragraph 3.19.5 above are implemented.

Collecting directly from the individual (APP 3.6)

3.29 APP 3.6 provides that Health must collect personal information about an individual only from the individual unless particular exemptions apply:

3.29.1 the individual consents to the collection of the information from someone other than the individual (APP 3.6(a)(i));

3.29.2 the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual (APP 3.6(a)(ii)); or

3.29.3 it is unreasonable or impracticable for the APP entity to collect the personal information from the individual (APP 3.6(b)).

3.30 We note that the User's Registration Information and information about the Positive User in Digital Handshakes will be collected into the National COVIDSafe Data Store from the Positive User (so that APP 3.6 will not be relevant to these collections).

---

[29] APP Guidelines, Chapter 3, paragraphs 3.60 – 3.61.
[30] APP Guidelines, Chapter 3, paragraph 3.62 – 3.63.
[31] We note the United Kingdom Information Commissioner's Office has published guidance on this: https://webarchive.nationalarchives.gov.uk/20100402111239/http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf.

3.31 However, information about Contact Users in Digital Handshakes will also be collected from the Positive User, rather than from the Contact User concerned. In order to ensure that Contact Users have already consented to the upload, we **recommend** that Health should ensure that the Contact User has consented to that collection, so that APP 3.6 will be satisfied (**Recommendation 6** and **Recommendation 7**).

3.32 We note that our discussion about the collection of Digital Handshake information about Contact Users after the Contact User has deleted their App (i.e. withdrawn their consent), in paragraph 3.22 is also relevant here.

Other issues

3.33 We note that, if consent of a Positive User is obtained, all of their Digital Handshakes will be uploaded. We understand that this is then analysed by the Contact Tracer to determine the Digital Handshakes that represent an exposure risk (because there are Digital Handshakes which, in total, represent a period of 15 minutes of contact with a Bluetooth signal strength which is a proxy for 1.5 metres).

3.34 In our view, this represents unnecessary access to, and use of, personal information which is not required for the purpose of collection – the Contact Tracer should not be required, or be provided with, access to information about individuals who, based on the defined risk parameters (currently 1.5 metres and 15 minutes duration), do not have a risk of exposure to COVID-19. Such collection and use is inconsistent with the data minimisation principle discussed in paragraph 3.12 above.

3.35 We **recommend** that:

3.35.1 Health investigate whether it is technologically possible to only record Digital Handshakes if they meet risk parameters, set on the basis of medical advice about the risks of exposure to COVID-19 (i.e. so that the minimum amount of information required for contact tracing is collected from Users); or

3.35.2 if this is not possible, whether it is technologically possible to only upload Digital Handshakes if they meet those risk parameters; or

3.35.3 if this is not possible, whether it is technologically possible for the National COVIDSafe Data Store to, once Digital Handshakes are uploaded, automatically delete (or de-identify if deletion is not possible) any Digital Handshakes that do not meet those risk parameters; or

3.35.4 if this is not possible, for access to the Digital Handshakes stored in the National COVIDSafe Data Store to be limited to those Digital Handshakes which meet those risk parameters.

(**Recommendation 18**)

4. APP 4 – dealing with unsolicited personal information

Text of APP 4

4 Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Analysis of compliance with APP 4

4.1 APP 4 only applies where an APP entity receives unsolicited personal information (i.e. information that it receives but has taken no active steps to collect).

4.2 As discussed in APP 3 (paragraph 3.2 of this **Part D**), we consider that all information collected in connection with the App will be solicited. Further, the App does not contain any "free text" or other fields that may permit Health to collect unsolicited personal information.

4.3 Accordingly, we consider it unlikely that any unsolicited personal information will be collected in connection with the App. However, in the unlikely event that unsolicited personal information is received by Health, it must manage that unsolicited information in accordance with its usual practices for complying with APP 4.

5. APP 5 – notification of the collection of personal information

Text of APP 5

5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Analysis of compliance with APP 5

5.1 APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters (referred to as "APP 5 matters"), or otherwise ensure that the individual is aware of those matters. This notification must occur at or before the time of collection, or as soon as practicable afterwards.

5.2 The "reasonable steps" test is an objective test, that considers whether a reasonable person in those circumstances would agree that the entity had acted reasonably in providing notice or ensuring awareness of the APP 5 matters. The reasonable steps for an APP entity will depend on circumstances that include:

5.2.1 the type of personal information collected, including whether it includes any sensitive information;

5.2.2 the possible adverse consequences for an individual as a result of the collection;

5.2.3 any special needs of the individual; and

5.2.4 the practicability, including time and cost involved (although the entity is not automatically excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so, and whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances).

Collection Notices

5.3 We consider there to be two points at which Health should obtain Users' consent in relation to the App. These are when:

5.3.1 the User downloads the App, before they input their Registration Information; and

5.3.2 the Positive User receives an SMS message from a Public Health Official to agree to the upload of their Digital Handshake Information.

5.4 As discussed in relation to APP 3 (paragraph 3.18.3 of this **Part D**), we **recommend** that Health:

5.4.1 ensures that Users are provided with sufficient information about how their personal information will be collected, and then used and disclosed for all information flows, before providing their consent to the collection of the Registration Information. As discussed in paragraph 3.18.3 of this **Part D**, it is important that Health considers the sequencing of the screens displayed to the User carefully. The collection and consent notices need to address all of the matters specified in APP 5.2 which are relevant, and as are reasonable in the circumstances (taking into account the impracticality of displaying very lengthy notices on devices which is likely to decrease the likelihood of the User taking the time to read and understand the content; and the inclusion of more detailed information in an easily accessible privacy policy); and

5.4.2 ensures that Positive Users are provided with further information about how the Digital Handshake information will be handled, before they agree to upload that information.

(**Recommendation 6** and **Recommendation 7**)

5.5 If Health adopts these recommendations, this will enhance Health's compliance with the requirements of APP 5 (and requirements of other APPs).

6. APP 6 – use or disclosure of personal information

Text of APP 6

6 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

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

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

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

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

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

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

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

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

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

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

Analysis of compliance with APP 6

6.1 APP 6 provides that an APP entity must not use or disclose personal information that was collected for a primary purposes for another purpose (a secondary purpose), unless the individual has consented to the use or disclosure of the information, or APP 6.2 or APP 6.3 applies.

Primary purpose for collection

6.2 We are instructed that the primary purpose for collection of any personal information that Health collects as custodian of the National COVIDSafe Data Store, is to facilitate authorised State and Territory Contact Tracers being able to access that information in order to undertake contact tracing procedures in connection with the COVID-19 pandemic and help prevent the spread of COVID-19 in Australia.

6.3 In managing the National COVIDSafe Data Store, Health will be:

6.3.1 using the information in the National COVIDSafe Data Store to require that Unique IDs are generated, to ensure that there is appropriate security for the storage of Digital Handshake information on User's devices;

6.3.2 using the information in the National COVIDSafe Data Store to send Positive Users a PIN that will allow them to decide to upload the Digital Handshake information on their device to the National COVIDSafe Data Store; and

6.3.3 disclosing to Contact Tracers, through provision of access to the National COVIDSafe Data Store, personal information that has been collected and stored in the National COVIDSafe Data Store.

In our view, these uses and disclosures will fall within the primary purpose for collection.

6.4 We note that, although the Unique ID Reports (as discussed in paragraph 9.7 in **Part C**) will not contain personal information, the Unique IDs will also be used to generate them. To ensure compliance with APP 6, we **recommend** that a reference to this additional use is included in the wording of the App Privacy Policy (**Recommendation 7**).

Potential uses and disclosures of the personal information for a secondary purpose

6.5 As stated above, Health must not use or disclose the personal information for a secondary purpose unless the individual has consented to the use or disclosure of the information (APP 6.1(a)), or one of the exceptions in APP 6.2 or APP 6.3 apply (APP 6.1(b)).

6.6 While Health does not currently intend for personal information to be used or disclosed for any secondary purpose, it cannot rule out the need to do so, for example, if it was required by law or a Court or Tribunal to disclose information held in the National COVIDSafe Data Store. We have therefore considered potential secondary disclosures below.

6.7 We note that the risks associated with secondary uses and disclosures could potentially be addressed by a legislative framework (**Recommendation 3**). For example, if a legislative framework is introduced that does prohibit secondary uses or disclosures, consideration of the exceptions in APP 6.2 may not be required.

Use or disclosure authorised by law

6.8 APP 6.2(b) provides that the use or disclosure of personal information for a secondary purpose is permitted if the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order.

6.9 Health may be required to use personal information in the National COVIDSafe Data Store to comply with its obligations under APP 12, and provide information about an individual to them in accordance with the individual's request. On the grounds that access to the personal information is required by law (as APP 12 requires Health to provide access to the information unless that exception applies), we consider that this secondary use complies with APP 6.1(b) by virtue of the exception at APP 6.2(b).

6.10 In addition, if Health or any other party is required or authorised by or under an Australian law or a court/tribunal order to disclose information collected via the App, the information may be disclosed and the disclosure of that information will comply with APP 6.1 by virtue of the exception at APP 6.2(b).

Permitted general situation

6.11 In addition, we note that there is the possibility that in the future Health may have to use or disclose personal information for a secondary purpose due to the existence of a permitted general situation, noting that this disclosure would comply with APP 6.1 by virtue of the exception at APP 6.2(c).

6.12 APP 6.2(c) also provides that the use or disclosure of personal information for a secondary purpose is allowed if a permitted general situation exists in relation to the use or disclosure. Section 16A of the Privacy Act sets out when a permitted general situation exists. Relevantly, section 16A provides that a permitted general situation exists, amongst other things, if the APP entity determines that:

6.12.1 it is unreasonable or impracticable to obtain the individual's consent to the collection, use and disclosure of their personal information; and

6.12.2 the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

6.13 In respect of the App, this means that if Health reasonably believes that the use or disclosure of a User's personal information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and Health is satisfied that it would be unreasonable or impracticable to obtain the User's consent, Health could use or disclose the information in accordance with the exception at APP 6.2(c).

6.14 Given the potential for a secondary use that would be permitted by the Privacy Act, we **recommend** that for transparency, and to ensure that the consent obtained is properly informed, Health should ensure that the App Privacy Policy and/or the notices provided to Users when seeking consent clearly set out that the above circumstances may mean that Health could be required to, or otherwise need to, use or disclose the collected personal information as permitted by the Privacy Act (**Recommendation 6** and **Recommendation 7**).

Access by AWS and DTA in connection with the infrastructure

6.15 We note that AWS and DTA may have access to personal information in the National COVIDSafe Data Store for the purposes of providing ICT support services.

6.16 As discussed in **Part C**, we have conducted our analysis on the basis that if Health implements **Recommendation 16** and **Recommendation 17**, there will be no disclosure to, or collection by, either AWS or DTA.

6.17 However, to ensure complete transparency, and to ensure that the consent obtained is properly informed, we **recommend** that Health should ensure that the App Privacy Policy clearly advises Users that contracted service providers may have access to personal information in the National COVIDSafe Data Store, for the sole purpose of providing ICT support services, and subject to strict privacy, confidentiality and security obligations (**Recommendation 7**).

Use by State and Territory Contact Tracers

6.18 We note that Health will disclose personal information to State and Territory Contact Tracers to enable the Contact Tracers to obtain the names and telephone numbers of Contact Users. Contact Tracers will use these telephone numbers to telephone the relevant Contact User, advise that they have been in contact with someone who has tested positive for COVID-19 and provide further advice and information. The use of this personal information is outside the scope of this PIA, and, as discussed in paragraph 6.3 of this **Part D** above, we consider that Health's disclosure of the information to the Contact Tracers (via Contact Tracers being allowed to access the National COVIDSafe Data Store) is consistent with the primary purpose of collection and therefore Health will comply with APP 6.

6.19 However, we appreciate that there is community concern about whether Contact Tracers will only use the personal information collected from Health for the purposes contemplated in the PIA (e.g. the community is concerned that Contact Tracers could further disclose the information for enforcement and compliance purposes). This could be through the Contact Tracer extracting information from the National COVIDSafe Data Store to create new records from the accessed information. We note that, if Contact Tracers are given the ability to easily extract data, this will be increase the likelihood of it occurring and therefore increase the privacy risks.

6.20 There is also an additional risk because Contact Tracers in the different States and Territories will be subject to different privacy regimes in relation to their handling of any personal information, with some regimes being more comprehensive than others.

6.21 Whilst Health will not have effective control over the information once it has been disclosed to Contact Tracers, we consider that there are steps that Health could take to try and ensure that the personal information is only used by Contact Tracers for the purposes contemplated in this PIA.[32] For example, we **recommend** that Health ensure that it has contractual or other administrative arrangements in place with the State and Territory public health authorities responsible for contact tracing. These arrangements should contain terms and conditions for access to, and use and disclosure of, information obtained from, the National COVIDSafe Data Store. Additionally, the arrangements should clarify how long the information can be retained. Essentially, State and Territory public health authorities should be required to agree to only use, access and disclose personal information for the purposes contemplated in this PIA.

6.22 In addition, arrangements with the States and Territories should impose appropriate requirements about what information can be extracted, and how that extraction must occur, and include requirements about the security of any systems that will be used to store the extracted data (including storage and subsequent access to any physical and electronic records created as a result). Ideally, State and Territory public health authorities should also be required to comply with the Privacy Act as if they were an APP entity (**Recommendation 12**).

6.23 Those arrangements with the States and Territory public health authorities should also deal with the situation where a Public Health Official or a Contact Users needs to contact a Child User. For example, such arrangements could include appropriate procedures (including "scripts" if appropriate) to be followed which would ensure that information is not inappropriately disclosed to a child (e.g. that they may have been exposed to COVID-19), and to facilitate consent to upload Digital Handshake information being given by the responsible adult rather than the Child User (**Recommendation 11**).

6.24 Further, we also **recommend** that each time a Contact Tracer accesses the National COVIDSafe Data Store, they be required to agree to terms and conditions of use, which clearly set out the limited ways in which Contact Tracers are permitted to use, access and disclose information stored on the National COVIDSafe Data Store (**Recommendation 12**).

[32] [32] This discussion assumes that there is no specific legislative framework in place dealing with further use or disclosure of personal information obtained via the App.

6.25 We note that all uses and disclosures of personal information should be clearly stated, if sufficient community uptake of the App is to be achieved. In these circumstances, it may be appropriate for restrictions to be placed on Commonwealth departments and agencies, and States and Territories (which includes the relevant health authorities, Public Health Officials, and Contact Tracers) in relation to the collection, use, disclosure and deletion of personal information obtained via the App. Accordingly, we **recommend** that Health continue to consider and investigate the legislative options in relation to the collection, use, disclosure, and deletion, of information in connection with the App (**Recommendation 3**).

Declaration under section 6F of the Privacy Act

6.26 As discussed in paragraph 6.21 of this **Part D** above, we consider that ideally State and Territory public health authorities should be contractually required (through contracts with Health) to comply with the Privacy Act as if they were APP entities. However, we recognise that it may be difficult to obtain such agreement, particularly in the compressed timeframes involved.

6.27 An alternative way of ensuring that such authorities are required to comply with the APPs might be to have the Governor-General make a regulation under section 6F of the Privacy Act.

6.28 Section 6F of the Privacy Act provides that the Governor-General may make regulations prescribing that a State or Territory authority, or the instrumentality of a State or Territory, is an organisation for the purposes of the Privacy Act (and therefore must comply with the Privacy Act as if it were an organisation).

6.29 Before the making of such regulations, the Minister must:

6.29.1 be satisfied that the relevant State or Territory has requested that the authority or instrumentality be prescribed as an organisation for the purposes of the Privacy Act; and

6.29.2 consult the OAIC about whether it is desirable for the authority or instrumentality to be an organisation for the purposes of the Privacy Act, such that its collection, holding, use, correction and disclosure of personal information must occur in accordance with the requirements of the Privacy Act (including the APPs at Schedule 1).

6.30 We do note that this would require further consideration and analysis, since deeming an entity to be an "organisation" would not necessarily overcome some of the privacy risks we have identified in this PIA report. In addition, issues of jurisdiction and conflict of laws would need to be considered (e.g., in relation to compliance and regulation under both the Privacy Act and the applicable State or Territory privacy laws).

6.31 We therefore **recommend** that Health continue to consult with appropriate agencies, including with AGD and the OAIC as appropriate, about whether there are legislative options that would assist in ensuring that all States and Territories will be required to handle personal information in the National COVIDSafe Data Store in a consistent and appropriate manner (**Recommendation 3**).

7. APP 7 – direct marketing

Text of APP 7

7 Australian Privacy Principle 7—direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the ***first organisation***) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Analysis of compliance with APP 7

7.1 APP 7 only applies to "organisations" as defined in the Privacy Act, rather than to agencies like Health.

7.2 Under section 7A of the Privacy Act, an act or practice of an agency may, in the prescribed circumstances, be treated as an act or practice of an organisation. This applies to:

7.2.1 a prescribed agency specified in Part I of Schedule 2 to the Freedom of Information Act 1982 (**FOI Act**); or

7.2.2 an agency specified in Division 1 of Part II of Schedule 2 to the FOI Act.

7.3 Health is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 7 does not apply to Health.

7.4 We do not consider that any further steps are required for Health to comply with APP 7.

8. APP 8 – cross-border disclosure of personal information

Text of APP 8

8 Australian Privacy Principle 8—cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

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

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For ***permitted general situation***, see section 16A.

Analysis of compliance with APP 8

8.1 APP 8 requires entities to take particular steps if they intend on disclosing personal information to an overseas recipient.

8.2 We understand that no personal information collected via the App will be stored on overseas ICT infrastructure or transferred to any overseas recipient, noting that we understand that the AWS Contract with DTA requires all data to be stored on infrastructure located in Australia.

8.3 However, it is possible that AWS, like many large ICT vendors, may offer some ICT support services that can be provided by individuals located overseas who access data stored in Australia for the sole purpose of providing ICT support (for example if there is a 24/7 “follow the sun” support offering).

8.4 If this is the case, and there may be access to personal information in the National COVIDSafe Data Store for the purposes of AWS delivering its contracted services, consideration of the application of APP 8 is necessary.

8.5 APP 8.1(b) provides that if an entity discloses personal information to an overseas recipient (who is not the entity or the individual), the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information.

8.6 Health will need to ensure that the AWS Contract contain appropriate mechanisms that require any parties that provide support services from outside Australia to comply with the APPs. We also **recommend** that the AWS Contract contain a provision which requires AWS to not take any information from the App, or the National COVIDSafe Data Store outside Australia, or allow such information to be accessed from or stored outside of Australia, without the prior written consent of Health (**Recommendation 16**). We consider that this represents a reasonable step by Health to ensure that any overseas recipients of personal information do not breach the APPs, as required by APP 8.

8.7 If States and Territories are permitted to extract data from the National COVIDSafe Data Store, the arrangements between Health and the States and Territories should also include similar restrictions (**Recommendation 12**).

9. APP 9 – adoption, use or disclosure of government related identifiers

Text of APP 9

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

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

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For ***permitted general situation***, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Analysis of compliance with APP 9

9.1 APP 9 applies to "organisations" as defined in the Privacy Act, rather than to agencies like Health.

9.2 Under section 7A of the Privacy Act, an act or practice of an agency may, in the prescribed circumstances, be treated as an act or practice of an organisation. This applies to:

9.2.1 a prescribed agency specified in Part I of Schedule 2 to the Freedom of Information Act 1982 (**FOI Act**); or

9.2.2 an agency specified in Division 1 of Part II of Schedule 2 to the FOI Act.

9.3 Health is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 9 does not apply to Health. We note that no government related identifiers will be collected by the App, or used or stored in the National COVIDSafe Data Store.

9.4 We therefore do not consider that any further steps are required for Health to comply with APP 9.

10. APP 10 – quality of personal information

Text of APP 10

> **10 Australian Privacy Principle 10—quality of personal information**
>
> 10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.
>
> 10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Analysis of compliance with APP 10

10.1 Under APP 10, Health needs to determine what steps (if any) are reasonable for it to take to be satisfied that personal information that is used and/or disclosed in connection with the App is accurate, up to date, complete and relevant (having regard to the purposes of the use or disclosure).

10.2 In the context of APP 10, the "reasonable steps" that an entity should take will depend upon circumstances that include:

10.2.1 the sensitivity of the personal information;

10.2.2 the nature of the entity (including its size, resources and business models);

10.2.3 the possible adverse consequences for an individual if the quality of personal information is not ensured; and

10.2.4 the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.[33]

10.3 It is important to note that none of the information collected in the National COVIDSafe Data Store is verified as accurate, up to date or complete (other than the mobile number which is initially verified), although we do note that if **Recommendation 11** is implemented, the Contact Tracer will check the accuracy of the information provided at that point, which will assist in ensuring the quality of the information, before further consequences which may have an impact on the Contact User occur. In addition, a User cannot choose to upload their Digital Handshake information unless and until a Public Health Official, having determined that the User is a Positive User, authorises that upload. This will assist in ensuring that only relevant Digital Handshake information is uploaded.

10.4 There is also an inherent risk associated with the use of Bluetooth technology as the mechanism for collection of Digital Handshakes. For example, this technology relies on signal strength as a proxy for distance between Users, and does not take into account whether there is any barrier (such as a glass window, or thin apartment walls) through which Bluetooth signals may pass. This means that more Digital Handshakes will be created, and may be uploaded into the National COVIDSafe Data Store, where there is no or little risk of infection with COVID-19. We note that if more Contact Users are identified than those who have actually come within the infectious range, there is a risk that the burden on Contact Tracers will be increased and more people than necessary diverted into self-isolation.[34]

---

[33] APP Guidelines, Chapter 10, paragraph 10.6.

[34] See https://thespinoff.co.nz/society/16-04-2020/even-in-extraordinary-times-the-right-to-privacy-remains/?mkt_tok=eyJpIjoiTjJNNE16ZGhNR1JsTWpReCIsInQiOiJvSk9cL0dZa3R4TVNuWGc2Vk5yblYzSENWYktZRkJhY05FNHVTMEhabzY1R1pCdkhHYklUNkJUVXlCUTZtZHdOT2RcLzZ0SE96OVRnellNYU1vcGdJT3FDbFk5VktscXZcL3pjdHRzQytpQm1IRTlNXC9cL1VRNkVvZ2JFZzdUVGpPOXY2In0%3D

However, we suggest that most Australians would prefer this outcome to the risks associated with the unnecessary further spread of COVID-19.

10.5 In addition, Bluetooth technology needs to be enabled, and the device screen unlocked, for the App to function most efficiently. This means that some Digital Handshakes may not be created, even though there is a risk of infection from COVID-19. We assume that this will be taken into account by the Contact Tracers, and note that contact tracing is not solely reliant on use of data from the App.

10.6 To address these risks, we **recommend** that Health satisfy itself that Bluetooth technology is the most appropriate available technology to use for the App (**Recommendation 14**), and ensure that Contact Tracers are aware of the limitations of the information in the National COVIDSafe Data Store when undertaking contact tracing procedures (**Recommendation 11**).

10.7 We also have considered the relevance of the personal information that will be collected (i.e. an examination of the connection of the information to the purpose for which it will be used or disclosed) in our analysis of APP 3. Implementation of the recommendations discussed in APP 3 will assist in ensuring that all personal information collected is relevant, and will enhance Health's compliance with APP 10.

11. APP 11 – security of personal information

Text of APP 11

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Analysis of compliance with APP 11

Protection of personal information

11.1 APP 11.1 requires an APP entity to take such steps as are reasonable to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The term "reasonable" is not defined in the Privacy Act, but the APP Guidelines provide that the term bears its ordinary meaning, as being based upon or according to reason and capable of sound explanation.[35] What is reasonable can be influenced by current standards and practices.[36]

11.2 We understand that the community will wish to be assured that their personal information will be protected appropriately, including to ensure that it will not be accessed without authority by malicious third parties. In light of this concern, and as is always the practice by APP entities, a number of security protections have been applied to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

11.3 These security measures have been implemented:

11.3.1 at the App level (i.e. to protect information on User's devices); and

11.3.2 in respect of the National COVIDSafe Data Store.

11.4 At the device level, these measures include:

11.4.1 the process has been designed to minimise the amount of personal information that is stored on a User's device (through the use of a Unique ID), in order to reduce the consequences to Users should unauthorised access be gained to their device;

11.4.2 all information uploaded to the National COVIDSafe Data Store from a User's device will be encrypted in flight; and

11.4.3 all information that is encrypted on the User's device will be deleted 21 days after it has been captured, which will again minimise the amount of personal information stored on Users' devices.

[35] APP Guidelines, Chapter B, paragraph B.105.
[36] *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 (Mason, Wilson and Dawson JJ at paragraph 12).

11.5 We do note that the App will work most effectively on some types of devices when the User's device is unlocked. If Users were to be advised to leave their device unlocked, that would involve a higher risk of unauthorised access for Users (because if their device is misplaced or stolen, it will not have the security protections associated with a locked phone). We **recommend** that Health consider whether there are additional technological solutions that could be implemented to reduce this risk, or whether it is necessary to advise Users to keep their device unlocked (**Recommendation 14**). If such advice is to be given, at a minimum, Users should be provided with information (ideally through App screens) about how to minimise the security risks associated with having an unlocked device.

11.6 We understand that in terms of the National COVIDSafe Data Store, the following security protections exist:

11.6.1 Contact Tracers will only be provided with access to information about Users in the State or Territory in which they are conducting contact tracing (which minimises the amount of personal information a Contact Tracer is able to access); and

11.6.2 all access to, and use of, the National COVIDSafe Data Store will be logged, and regularly audited, to ensure appropriate access and use for the primary purpose for collection.

11.7 However, ideally, this PIA report would also include information about the security protections in the AWS Contract, and how and when Contact Tracers can access the National COVIDSafe Data Store, including information about the access, access monitoring, and access auditing processes, however this has not been possible in the required urgent timeframes for this PIA.

11.8 Accordingly, we **recommend** that Health, if it has not already done so, seek independent assurance from security experts (including as appropriate the Australian Signals Directorate and the Australian Cybersecurity Centre), to provide additional testing and assurance that the security arrangements for the App and the National COVIDSafe Data Store, and the use of information in it, are appropriate. This will assist Health to demonstrate that it has taken all reasonable measures to comply with its obligations under APP 11.1. We also **recommend** that this assurance be made publicly available (without providing any information that would pose an additional security risk) (**Recommendation 14**).

11.9 We note that issues that will need to be considered when looking at access rights for State and Territory officers will include:

11.9.1 Will the access privileges for Public Health Officials be "locked down" so that only authorised persons with a need to do so can create a PIN and will other access to the National COVIDSafe Data Store be restricted (i.e. will this be their only access)?

11.9.2 Will there be flags in the system if a User's records are viewed by multiple Contact Tracers?

11.9.3 Will there be flags in the system if a User's records are viewed sometime after the initial contact tracing occurs?

11.9.4 Will the arrangements ensure that each State and Territory agency regularly confirms a list of Public Health Official and Contact Tracers who require ongoing access to limit unauthorised access?

11.10 Additionally, we **recommend** that Health:

11.10.1 ensure that there are appropriate governance arrangements, including in contractual arrangements with the State and Territory agencies as appropriate, to control access, and ensure sufficient security arrangements for any information that is extracted from the National COVIDSafe Data Store (**Recommendation 12**);

11.10.2 ensure that appropriate security training (including privacy briefings) is made available and undertaken by the individual Contact Tracers before being granted access to the National COVIDSafe Data Store (**Recommendation 11**); and

11.10.3 consider developing appropriate written public communications designed to enhance understanding, and recognition of, the security protections that have been put in place (without providing information that would pose an additional security risk) (**Recommendation 10**).

11.11 We note that making the source code for the App public may also assist in assuring the Australian community that appropriate security arrangements have been put in place (see **Recommendation 1**).

Data Breaches

11.12 In additional to the discussion in paragraph 1.10 of this **Part D**, we note the "security trade off" involved in minimising the amount of personal information held on User's devices is that the National COVIDSafe Data Store will hold all of the relevant personal information.

11.13 We understand that, if there was to be a data breach in relation to the National COVIDSafe Data Store, Health would implement its data breach response plan. However, noting the many parties that are involved in the administration, operation and use of the National COVIDSafe Data Store, we **recommend** that Health undertake appropriate planning, and ensure that appropriate arrangements are in place, so that steps can be taken immediately to minimise the effect of any such breach, and an efficient and effective investigation process undertaken as soon as possible (**Recommendation 14**).

11.14 This may involve ensuring that appropriate contractual (or administrative) provisions are included in the AWS Contract, the MOU arrangements with DTA and the contractual or other arrangements with the State and Territory agencies.

Retention of personal information in the National COVIDSafe Data Store

11.15 We understand that all Digital Handshakes (encrypted data) stored on a User's device will be automatically deleted 21 days after they have been collected. In addition, after a Digital Handshake is uploaded to the National COVIDSafe Data Store, it will be deleted from the User's device.

11.16 The Australian Government has publicly stated that the National COVIDSafe Data Store will only be kept operational for as long as the personal information in it is needed for contact tracing in connection with the COVID-19 pandemic.

11.17 This is consistent with the general intent of APP 11.2(b), which provides that, subject to particular exceptions, if an APP entity holds personal information about an individual and the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs, the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is deidentified.

11.18 However, we note that personal information may be stored within the National COVIDSafe Data Store in a "Commonwealth record" for the purposes of the Archives Act, such that Health will need to comply with the record-keeping and disposal obligations in the Archives Act.

11.19 Accordingly, we **recommend** that Health promptly, and before the finalisation of the notices that will be provided to Users when seeking consent, and the release of the App, seek advice (including consultation with the National Archives of Australia as appropriate):

11.19.1 as to whether the personal information in the National COVIDSafe Data Store will be subject to the Archives Act;

11.19.2 if so, whether the records will be able to be deleted or de-identified after the personal information in the National COVIDSafe Data Store is no longer required (for example, it may be necessary to determine whether a records disposal authority should be obtained in advance of the release of the App, or other legislative action taken, to enable deletion or de-identification of the personal information as required); and

11.19.3 whether retention of the records is required by any other law or legal requirement (e.g. if a complaint or legal action was brought by a User after decommissioning of the National COVIDSafe Data Store).

(**Recommendation 15**)

11.20 In addition, noting that the States and Territories may not be subject to the same privacy obligations as Health, it will be important for the contractual (or other) arrangements with States and Territories to include provisions for the deletion, de-identification or no further use of information obtained from the National COVIDSafe Data Store after the time of its decommissioning (see **Recommendation 12**).

12. APP 12 – access to personal information

Text of APP 12

12 Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Analysis of compliance with APP 12

12.1 Under APP 12, an APP entity is required to give an individual access to the personal information held by it unless particular exceptions apply (depending on whether the APP entity is an agency or organisation).

12.2 As Health is an agency, it must give an individual access to the personal information held in the National COVIDSafe Data Store unless an exception under APP 12.2 applies. Relevantly, APP 12.2 provides that an agency does not need to give access to an individual under APP 12.1 if the agency is required or authorised to refuse to give the individual access to the personal information by or under:

12.2.1 the *Freedom of Information Act 1982* (Cth) (**FOI Act**); or

12.2.2 any other Act of the Commonwealth (or a Norfolk Island enactment) that provides for access by persons to documents.[37]

12.3 We note that it is possible that a legislative framework (as recommended by **Recommendation 3**) could potentially restrict access by Users to their personal information. Any such decision would need to into account all of the relevant circumstances (e.g. balancing the privacy benefits in individuals having access to their own personal information against circumstances in which providing access may be a significant administrative burden for Health (such that it would divert resources required to manage the response to COVID-19). If such a legislative framework were to be implemented, it may not be necessary to provide access in accordance with APP 12.1 (and our recommendations discussed below will not be applicable).

12.4 However, on the assumption that the exceptions at APP 12.2 will not apply (noting that a User can usually obtain access to their own personal information under the FOI Act), we assume that Health will implement the usual processes that it has in place to ensure that it can consider the relevant request in order to meet the requirements of APP 12, particularly in respect of the timeframe for complying with such requests.

12.5 Assuming access under APP 12 will not be prohibited by a legislative framework, we note that Health will not itself have access rights to the National COVIDSafe Data Store. We therefore **recommend** that Health consider how it will obtain access to the information for the purposes of APP 12.

[37] If Health were to refuse access to information by virtue of the exemption at APP 12.2, Health must provide a written notice of this decision, in compliance with APP 12.9.

12.6 For example, Health may need to ask DTA to obtain the information from AWS. If Health does need to ask DTA to obtain the information from the National COVIDSafe Data Store, we **recommend** that:

12.6.1 Health consider whether processes could be adopted to facilitate easy requests being made by User (e.g. a form in the App) which will facilitate the request process and ensure consent to access the National COVIDSafe Data Store is provided by the User (**Recommendation 8**); and

12.6.2 the AWS Contract contains an obligation to provide the required information to DTA or Health (the MOU between Health and DTA should set out the processes for Health to request information from DTA (and AWS) to meet its obligations under APP 12) (**Recommendation 16** and **Recommendation 17**).

13. APP 13 – correction of personal information

Text of APP 13

13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

Analysis of compliance with APP 13

13.1 APP 13 requires an entity holding personal information to take such steps as are reasonable in the circumstances to permit correction of that information, except in limited circumstances.[38]

[38] If Health refuses to correct the personal information as requested by a User, it must give the User a written notice that includes the matters specified in APP 13.3.

13.2 We understand that Users will not have the ability to correct their Registration Information through the App, but will need to delete the App and then re-install it with the correct information. This should be made clear to Users of the App in the App Privacy Policy (see **Recommendation 7**).

13.3 We assume that if Health receives a request from a User to correct their information that it holds in the National COVIDSafe Data Store (which will be the User's Digital Handshake Information), Health has standard procedures and processes in place to consider such a request and ensure that it meets the requirements of APP 13, particularly in respect of the timeframe for complying with such requests.[39]

13.4 As for APP 12, given that Health will not itself have access rights to the National COVIDSafe Data Store, we **recommend** that Health consider how access to the information will be provided, if correction is required.

13.5 We suggest that **Recommendation 8**, **Recommendation 16** and **Recommendation 17** (discussed in APP 12) should also be considered in connection with the correction, rather than the provision, of personal information. This will assist in ensuring compliance with APP 13.

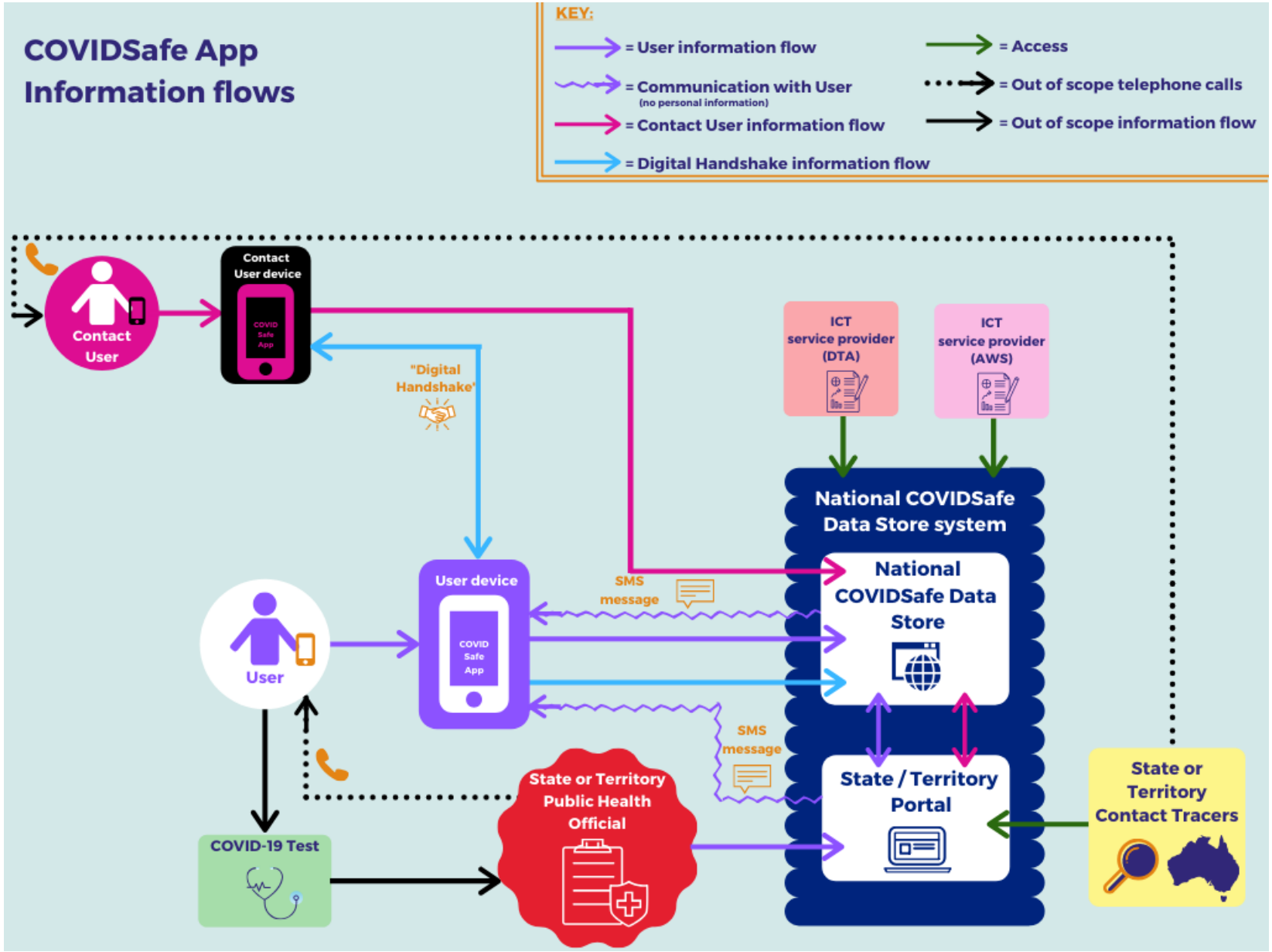
[39] As Health is an agency, under APP 13.4(a)(ii), Health must respond to a request made by a User within 30 days after the request is made.

Part E GLOSSARY

Definitions	
AGD	means the Commonwealth Attorney-General's Department.
AHRC	means the Australian Human Rights Commission.
App	means the Australian Government's new COVIDSafe Application.
App Privacy Policy	means a privacy policy, developed in accordance with the Privacy Act, specifically for the handling of personal information in relation to the App.
APP, or Australian Privacy Principle	has the meaning given to it in the Privacy Act.
APP Code	means the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.
Archives Act	means the *Archives Act 1983* (Cth).
AWS	means DTA's contracted service provider, trading as Amazon Web Services.
AWS Contract	means the agreement between DTA and AWS.
Child User	means a User (including a Positive User or a Contact User, as relevant) who is under the age of 16.
Confirmation Notification	means the information that is presented on the App to a Positive User before they input the one-off six-digit PIN they receive from a Public Health Official.
Contact Tracer	mean a State or Territory public health officer who is responsible for identifying and contacting persons who may have been exposed to a risk of contracting COVID-19.
Contact User	means for each User, the other User involved in a Digital Handshake between the two Users.
COVID-19	means the coronavirus disease caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).
Digital Handshake	means when two Users are within the defined proximity for a defined period of time, and each User's App creates an encrypted file, stored on each User's device.
DTA	means the Commonwealth of Australia, as represented by the Digital Transformation Agency.
Eligible Data Breach	has the meaning given to that term in the Privacy Act.

Guide	means the '*Guide to Accessing and Correcting Your Personal Information'* which sets out how individuals can access and correct their personal information held Health, available at https://docs.employment.gov.au/documents/guide-accessing-and-correcting-your-personal-information.
Health	means the Commonwealth of Australia, as represented by its Department of Health.
National COVIDSafe Data Store	means the repository which will be established for storage of information collected through the App.
OAIC	means the Office of the Australian Information Commissioner.
personal information	has the meaning given in section 6 of the Privacy Act.
PIA	means this privacy impact assessment.
Positive User	means a User who is contacted by a Public Health Official after testing positive to COVID-19.
Privacy Act	means the *Privacy Act 1988* (Cth).
Public Health Official	means the State or Territory public health officer responsible for contacting persons who have tested positive for COVID-19.
Quarantined Information	means all information that has already been submitted through the App.
Registration Information	means the information inputted into by the User after they have accepted to the terms of the Registration Notice.
Registration Notice	means the information displayed to the User about, and the terms of use the User has to agree to before using, the App when the User open the App for the first time.
sensitive information	has the meaning given in section 6 of the Privacy Act.
Unique ID	means the temporary unique identifier that the User's App will change every two hours if it is open and running on the User's device.
Unique ID Reports	mean the reports about whether a new Unique ID for a User has been accepted by the User's App.
User	means any individual using the App.

Attachment 1 Diagram of information flows



Attachment 2 Material reviewed

1. *Apple and Google joint initiative on COVID-19 contact tracing technology,* British Office of the Information Commissioner (ICO), 17 April 2020 (available at https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf).

2. *Blog: Combatting COVID-19 through data: some considerations for privacy*, A blog by Elizabeth Denham, British Information Commissioner, 17 April 2020 (available at http://ico.org.uk/about-the-ico/news-and-events/blog-combatting-covid-19-through-data-some-considerations-for-privacy/).

3. *Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures,* 16 April 2020 (available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670).

4. *Covid-19 Meets Privacy: A Case Study for Accountability*, Bojana Bellamy, President, Centre for Information Policy Leadership, April 2020 (available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/04/covid-19_meets_privacy_a_case_study_for_accountability_-_centre_for_information_policy_leadership__april_2020_.pdf).

5. *EHealth, Network Mobile application to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States,* Version 1.0, 15 April 2020 (available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf).

6. *Even in extraordinary times, the right to privacy remains*, John Edwards, published online 16 April 2020 (available at https://thespinoff.co.nz/society/16-04-2020/even-in-extraordinary-times-the-right-to-privacy-remains/?mkt_tok=eyJpIjoiTjJNNE16ZGhNR1JsTWpReCIsInQiOiJvSk9cL0dZa3R4TVNuWGc2Vk5yblYzSENWYktZRkJhY05FNHVTMEhabzY1R1pCdkhHYklUNkJUVXlCUTZtZHdOT2RcLzZ0SE96OVRnellNYU1vcGdJT3FDbFk5VktscXZcL3pjdHRzQytpQm1IRTlNXC9cL1VRNkVvZ2JFZzdUVGpPOXY2In0%3D).

7. *On the privacy of TraceTogether, the Singaporean COVID-19 contact tracing mobile app, and recommendations for Australia,* Dr Hassan Asghar (Macquarie University), Dr Farhad Farokhi (University of Melbourne), Progressor Dali Kaafar (Macquarie University) and Associate Professor Ben Rubenstein (University of Melbourne), 6 April 2020 (available at https://eng.unimelb.edu.au/ingenium/research-stories/world-class-research/real-world-impact/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia).

   Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks, COVID-19 Rapid Response Impact Initiative | White Paper 5, Harvard Centre for Ethics, Hart et al, 3 April 2020 (available at https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf).

8. *Privacy in a pandemic: Keep calm, and remember first principles*, Anna Johnston, published online 31 March 2020 (available at https://www.salingerprivacy.com.au/2020/03/31/privacy-in-a-pandemic/).