Australian Government
Department of Health

The COVIDSafe Application

Privacy Impact Assessment

Agency Response

Department of Health

Context

This document has been prepared by the Department of Health (**Health)**. The responses below take into account the views of other agencies involved in the design and implementation of the COVIDSafe Application (the App). It is intended to respond to the recommendations provided by Maddocks in their Privacy Impact Assessment (PIA) Report dated 24 April 2020.

Maddocks 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 independent analysis and consideration.	
Response	Agreed. The PIA and source code will be released subject to consultation with the Australian Signals Directorate's Australian Cyber Security Centre.

Maddocks 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 Australian Privacy Principles (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.	
Response	Agreed. The operation of the App will be reviewed regularly, including reviewing the effectiveness of privacy controls. The Government understands there are public concerns that information collected by the App will be used or disclosed for purposes other than contact tracing, such as law enforcement. The Government takes these concerns seriously and is taking urgent action to protect information in the App so that it must be used or disclosed for contact tracing purposes only and to give these protections the force of law. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App. Any changes to the App will need to comply with these additional legal protections This will minimise the risk of "function creep".

Maddocks 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.	
Response	Agreed. The Government will regulate ahead of the launch of the App to ensure that App data is only used for purposes related to contact tracing. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App. The situations in which information from the App can be used and disclosed will be more limited than under the *Privacy Act 1988* (Cth), in recognition of the sensitivity of the personal information that the App will collect. This regulation will also ensure that individuals are not forced to use the App in a range of circumstances, including as pre-condition for employment, entry to premises, participation in activities or receipt of goods and services.

Maddocks 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.	
Response	Agreed. The screen order will be arranged as proposed. The App Privacy Policy provides a mechanism for Users to raise complaints if they consider the consent requirements of the Privacy Act have not been complied with. Users of the App will also retain their existing rights under the Privacy Act to have a complaint about the consent requirements heard by the Office of the Australian Information Commissioner. The App Privacy Policy provides advice to Users on what to do if they feel they have been pressured into using the App. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App.

Maddocks 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.	
Response	Agreed. Only age ranges will be collected. The age ranges are 0-15, 16-29,30-39,40-49,50-59,60-69,70-79,80-89,90+.

Maddocks 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.	
Response	Agreed. The design for the App seeks separate consents at the initial registration stage and the upload stage. The wording for the collection and consent notices has been 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. The Attorney-General's Department, the Australian Government Solicitor and Maddocks were consulted in development of the consent notices. The App will be reviewed within six months of the launch and the need for further consent will be considered at that time or earlier if and when issues are raised. The Government has committed to advising all users when the Pandemic is over and prompting them to delete the App.

Maddocks 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.	
Response	Agreed. After consulting with the Attorney-General's Department, the Australian Government Solicitor and Maddocks, an App Privacy Policy has been developed and will be displayed on Health's website.

Maddocks 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).	
Response	Agreed in part. Data is minimised from the outset, and the only data collected is that required to support contact tracing. Instead of users accessing their information using COVIDSafe they will be able to change their registration information by deleting and re-installing COVIDSafe. A process for users to update or correct their registration information in the National COVIDSafe Data Store will be implemented.

Maddocks 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.

Response	Agreed. A number of the Frequently Asked Questions and additional information about the purposes of the App have been included in the App. Further information, including the App Privacy Policy, the Privacy Impact Assessment Report, and the Department's response, will be included on the Department of Health Website.

Maddocks 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 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).

Response	Agreed. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App. These protections will restrict collection, use and disclosure of App data for the purpose of contact tracing, maintenance of the National COVIDSafe Data Store and producing statistical information about COVID-19 that is de-identified. Use of the App is voluntary and this will be emphasised in public communications, and Frequently Asked Questions. Information about collection, access, use and disclosure of Registration Information in the National COVIDSafe Data Store will be included in the App Privacy Policy.

Maddocks Recommendation 11:	Development of training and/or scripts

We r**ecommend** 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 Contract Tracers are granted access to the National COVIDSafe Data Store

Response	Agreed. Health is liaising with State and Territory health authorities to assess what additional assistance is required to support the use of the App. Protocols with appropriate minimum standards, regarding the appropriate interaction between Public Health officials and people under 16 years, will be confirmed after consultation with State and Territory health authorities. Access will be provided only after these protocols are in place.

Maddocks 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 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.

Response	Agreed. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App. These protections will restrict collection, use and disclosure of App data for the purpose of contact tracing, maintenance of the National COVIDSafe Data Store and producing statistical information about COVID-19 that is de-identified by State and Territory health authorities. Health will consider other arrangements as necessary to manage access to, collection, use and disclosure of information from the National COVIDSafe Data Store. This includes ensuring that any App data disclosed to State and Territory health authorities for contact tracing will be securely handled. Public Health officials will be required to acknowledge the terms and conditions of use, and work is underway to determine the form of this acknowledgement.

Maddocks 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 App Privacy Policy should indicate that Users may use a pseudonym.

Response	Agreed. The Name field in the App allows users to enter a pseudonym. The App Privacy Policy indicates that Users may provide a pseudonym.

Maddocks 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.

Response	Agreed. Health is seeking independent advice from the Australian Signals Directorate's Australian Cyber Security Centre security experts and will consider making this information publically available subject to an assessment of whether publication results in an increased security risk. The Notifiable Data Breaches Scheme will continue to apply to the Department of Health in respect of information collected under the App that is held by the Department including where it is stored with Amazon Web Services (AWS). Health is ensuring that appropriate arrangements are in place with AWS, the Digital Transformation Agency (DTA) and the States and Territories so that the risk of data breaches is minimised, and that an efficient and effective investigation

	process can occur to reduce the impact should a breach occur.

Maddocks 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).	
Response	Agreed. Work is being undertaken to strengthen privacy protections via legislation with respect to the information that is collected, and additional legal protections will be in place when the App is launched limiting the collection, use, and disclosure of App data. The Minister for Health has made a Determination under the *Biosecurity Act 2015* to protect data collected by the App for an interim period until legislation can be enacted. The Attorney-General will introduce legislation in the next Parliamentary sitting week to establish a strict legal framework for information handling in the App. These enhanced protections will require all data in the National COVIDSafe Data Store to be deleted after the pandemic has concluded, and will override any obligation under an Australian law to retain data for a longer period, including record-keeping obligations under the *Archives Act 1983*.

Maddocks 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 the DTA and Health (such as a memorandum of understanding (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 requirement information to DTA (which will, if **Recommendation 17** is implemented, be required to provide 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 it (e.g. to other parts of the AWS' infrastructure environment).

Response	Agreed. AWS are engaged through the DTA under a standard Commonwealth procurement policy that ensures service providers adhere to government policy including security, privacy and confidentiality controls. Health will work with the DTA to immediately review the contract with AWS to ensure relevant provisions are included, assess adherence with the Protective Security Policy Framework and audit access management arrangements.

Maddocks 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;

[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.

- 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.

Response	Agreed. Health will implement appropriate arrangements with the DTA to clarify roles and responsibilities regarding appropriate security and information flows. Health will also work with DTA regarding contractual arrangements with relevant ICT and other service providers.

Maddocks 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 Digital Handshakes which meet those risk parameters.

Response	Agreed. Access restrictions to Digital Handshakes will be put in place. Personnel in State and Territory health authorities can only access Digital Handshakes which meet the risk parameters.

Maddocks 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.	
Response	Agreed. The current App design requires a person under 16 years of age to confirm that their parent or guardian has consented to the collection of their registration information and contact data. Protocols with appropriate minimum standards, regarding the appropriate interaction between Public Health Officials and people under 16 years, will be confirmed after consultation with State and Territory health authorities. These protocols will ensure that consent from a parent, guardian or other responsible adult is obtained before a child’s contact history is uploaded and that, for children under 16, a health professional speaks with a parent, guardian or other responsible adult where the child may have been in contact with a person who has tested positive for COVID-19. Access will be provided only after these protocols are in place.