EXPLANATORY STATEMENT

Biosecurity Act 2015

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements— Public Health Contact Information) Determination 2020

The *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) Declaration 2020* (the Declaration) has been made pursuant to section 475 of the *Biosecurity Act 2015* (the Act), and declares that a human biosecurity emergency exists regarding the listed human disease 'human coronavirus with pandemic potential' (COVID-19). The human biosecurity emergency period is in force for 3 months beginning immediately after registration of the Declaration, on 18 March 2020.

During a human biosecurity emergency period, the Health Minister may, in accordance with sections 477 and 478 of the Act, determine emergency requirements that he or she is satisfied are necessary to prevent or control the entry, emergence, establishment or spread of the declaration listed human disease, COVID-19, in Australian territory or a part of Australian Territory. A person who fails to comply with a requirement may commit a criminal offence (punishable by imprisonment for a maximum of 5 years, or 300 penalty units, or both).

The purpose of the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (the Determination) is to impose requirements on data collected through the COVIDSafe App (COVIDSafe App data) and any use or disclosure of COVIDSafe App data. The Determination requires COVID App data uploaded through the app to be stored in the Commonwealth's National COVIDSafe Data Store – the Commonwealth database administered by the Department of Health and the Digital Transformation Agency. The Determination's requirements regulate any collection, use, or disclosure of COVID App data, and require deletion of the National COVIDSafe Data Store at the conclusion of the pandemic.

The Determination's requirements operate in place of any inconsistent requirements that would otherwise apply under Australian law. This includes any more stringent requirements about retaining Commonwealth records under the *Archives Act 1983* or less stringent requirements about handling personal information under the *Privacy Act 1988* (Privacy Act). However, the Privacy Act would otherwise continue to apply to COVIDSafe App data that is personal information about an individual (within the meaning of the Privacy Act).

The CEO of the Digital Transformation Agency, the Acting Secretary of the Department of Health and the Commonwealth Chief Medical Officer have advised the Health Minister, and the Health Minister is satisfied, that the Determination is necessary to prevent or control the entry, emergency, establishment or spread of COVID-19 in Australian territory.

Before making an emergency requirement, the Health Minister must also be satisfied, and the Health Minister is satisfied, that the requirement:

- is likely to be effective in, or contribute to, achieving its purpose;
- is appropriate and adapted to achieve its purpose; and
- is no more restrictive or intrusive than is required in the circumstances, including, for a requirement, in the manner in which it is to be applied

In addition to being satisfied of the above effectiveness and proportionality matters, the Health Minister must also be satisfied that the period during which a requirement is to apply is only as long as is necessary. The period during which a requirement applies cannot exceed the human biosecurity emergency period.

The view that the Determination is proportionate, likely to be effective and that the length of its period of application is only as long as necessary, is supported by the advice of the CEO of the Digital Transformation Agency and the Commonwealth Chief Medical Officer. Because the requirements are in response to a human biosecurity emergency, it is considered appropriate that they be implemented immediately through a determination of the Health Minister, made under s 477 of the *Biosecurity Act*.

The Determination is drafted to avoid trespassing on rights and liberties to the greatest extent possible, consistent with the imperative of implementing the measures necessary to prevent or control the emergence, establishment and spread of COVID-19 in Australian territory.

The Determination is consistent with the approach that use of the COVIDSafe App is strictly voluntary and that a user's informed consent is required to allow the App to collect data about the user and upload that data to the National COVIDSafe Data Store. The Determination also provides legal safeguards to ensure data collected by the COVIDSafe App will only be used to facilitate contact tracing activities by State and Territory officials or those in the service of State and Territory health authorities, and for the proper functioning, integrity and security of the COVIDSafe App and the National COVIDSafe Data Store.

The Determination also allows reporting of de-identified statistics about COVID App data. This has been included to allow for evaluation and to ensure an appropriate degree of transparency and accountability about the collection, use and disclosure of COVID App data, without infringing on the privacy of any individual. De-identified data is information that is no longer about an identifiable individual or an individual who is reasonably identifiable. The Determination does not allow the production of statistical information that would disclose information about an identifiable or reasonably identifiable individual.

Furthermore, the Determination provides that data held in the National COVIDSafe Data Store must be retained in Australia, and COVID App data in the National COVIDSafe Data Store must not be disclosed to a person outside of Australia (except for the purposes of contact tracing by a State or Territory Government health official).

The only instance in which COVID App data can be used for law enforcement or compliance purposes is to investigate whether a breach of the Determination has occurred or to prosecute a person for an offence against s 479 of the *Biosecurity Act 2015*. This is permitted to ensure that the data protections set out in the Determination can be enforced. Any additional use of COVID App data for enforcement, compliance or other secondary purpose is strictly prohibited by the Determination. Misuse of information collected by the COVIDSafe App will constitute a breach of the Determination and attract a penalty.

The Determination specifically prohibits the use of coercion to require another person to: download the COVIDSafe App; have the App in operation; or give consent for encrypted contact information to be uploaded to the National COVIDSafe Data Store at the point of a positive COVID-19 diagnosis.

Background

On 5 January 2020, the World Health Organization (WHO) notified Member States under the *International Health Regulations (2005)* (IHR) of an outbreak of pneumonia of unknown cause in Wuhan city, China. The pathogen is a novel (new) coronavirus. On 21 January 2020 'human coronavirus with pandemic potential' became a 'listed human disease' by legislative instrument made by the Director of Human Biosecurity under s 42 of the Act. On 30 January 2020, the outbreak was declared by the WHO International Regulations Emergency Committee to constitute a Public Health Emergency of International Concern.

On 11 February 2020, the WHO announced that the International Committee on Taxonomy of Viruses named the pathogen virus 'severe acute respiratory syndrome coronavirus (SARS-CoV-2)'. It is closely related genetically to the virus that caused the 2003 outbreak of Severe Acute Respiratory Syndrome (SARS). The international name given by the WHO to the disease caused by SARS-CoV-2 is Coronavirus disease 2019 (COVID-19). On 11 March 2020, the WHO declared the outbreak of COVID-19 a pandemic.

COVID-19 has entered Australia. It represents a severe and immediate threat to human health in Australia as it has the ability to cause high levels of morbidity and mortality, and to disrupt the Australian community socially and economically.

Emergency requirements
An emergency requirement is a non-disallowable legislative instrument (s 477(2)). The Health Minister personally makes emergency requirements under Part 2 of Chapter 8 of the Act (s 474).

The requirements that the Health Minister may determine include, but are not limited to: requirements that apply to persons, goods or conveyances when entering or leaving specified places; requirements that restrict or prevent the movement of persons, goods or conveyances in or between specified places; and requirements for specified places to be evacuated (s 477(3)).

Requirements made under section 477(1) apply despite any provision of any other Australian law (s 477(5)), with the potential consequence that a person who acts in accordance with a requirement may be protected from criminal liability that would otherwise attach to the person's required actions under State, Territory or Commonwealth law.

To ensure that the Determination is in place to address emergency human biosecurity risk, the Determination commences at 11:59pm by legal time in the Australian Capital Territory on the day this instrument is registered.

Consultation

The Determination is supported by advice from the CEO of the Digital Transformation Agency, the Acting Secretary of the Department of Health and the Commonwealth Chief Medical Officer.

The requirement is a non-disallowable legislative instrument under the *Legislation Act 2003*. The Act provides for the requirement to be non-disallowable to ensure that the Commonwealth is able to take the urgent action necessary to manage a nationally significant threat or harm to Australia's human health.

A provision by provision description of the requirements is contained in the Attachment.

ATTACHMENT

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements –Public Health Contact Information) Determination 2020

Part 1 - Preliminary

1 Name

This section provides that the title of this instrument is the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements – Public Health Contact Information) Determination 2020.* This title is consistent with the wording of the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) Declaration 2020, which was made pursuant to section 475 of the *Biosecurity Act 2015* and came into effect on 18 March 2020.

2 Commencement

Item 1 of the table at subsection 2(1) provides that the whole of this instrument will commence at 11.59pm by legal time in the Australian Capital Territory on the day that the instrument is registered. This is intended to ensure that the instrument commences before the 'COVIDSafe' application (described further in the explanation of section 5 below) is available for download by members of the public.

Subsection 2(2) provides that any information in column 3 of the table is not part of the instrument and that information in column 3 may be inserted or edited in any published version of this instrument.

3 Authority

This section provides that this instrument is made under subsection 477(1) of the *Biosecurity Act 2015*.

4 Object

Section 4 provides that the object of this instrument is to make contact tracing faster and more effective by encouraging public acceptance and uptake of COVIDSafe.

This instrument achieves the objective through placing strict limitations on the handling of COVID app data, to ensure that it is only used for the purpose of contact tracing, or ancillary purposes that support that purpose (for example, to ensure the integrity of the National COVIDSafe Data Store).

Public acceptance and uptake of COVIDSafe is crucial to the success of COVIDSafe and responding effectively to cases of community transmission of the coronavirus known as COVID-19. COVIDSafe will allow the States and Territories to quickly and effectively contact individuals who may have been in contact with a person who has been diagnosed with the coronavirus known as COVID-19. This reduces the risk posed to others and provides a clear public health benefit.

5 Definitions

Section 5 includes a note referring to definitions from the enabling legislation, the *Biosecurity Act 2015*. These terms are defined in section 9 of the *Biosecurity Act 2015* and mean the following:

- 'Australian law' means a law of the Commonwealth, or of a State or Territory;
- 'Health Department' means the Department administered by the Health Minister (the Health Minister meaning the Minister administering the *National Health Act 1953*); and
- 'State or Territory body' includes a Department of State, or an authority, of a State or Territory.

Section 5 provides definitions for the following terms in this instrument:

'Contact tracing' has the meaning given by subsection 6(4) of this instrument. This definition is described further in the explanation of subsection 6(4) below.

'COVID app data' has the meaning given by subsection 6(3) of this instrument. This definition is described further in the explanation of subsection 6(3) below.

'COVIDSafe' is the name of an Australian Government application for mobile telecommunications devices, and has the meaning given by paragraph 6(3)(a) of this instrument. This definition is described further in the explanation of paragraph 6(3)(a) below.

'De-identified' means information that is no longer about an identifiable individual or an individual who is reasonably identifiable. This definition aligns with the definition of the same term in subsection 6(1) of the Privacy Act. The use of COVID app data to produce de-identified statistical information is described further in the explanation of paragraph 6(2)(e) below.

'In contact' means a person who has been in contact with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in proximity of the other person.

COVIDSafe does not collect location information about users. The App works by identifying the mobile telecommunications device of people using the App when they come into contact with each other, via Bluetooth. This definition contemplates the scope of the information to be collected about users' interactions with each other.

'Mobile telecommunications device' means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*) that is used, or is capable of being used, in connection with a public mobile telecommunications service.

COVIDSafe will be available for free download to mobile telecommunications devices running Apple's iOS and Google's Android operating systems from the relevant app stores. This definition is consistent with other Commonwealth legislation and captures appropriate consumer mobile telecommunications devices capable of connecting to mobile phone networks or public Wi-Fi services. This recognises that COVIDSafe may be installed on devices with Bluetooth

capability that may not be limited to mobile phones (for example, electronic tablets).

'National COVIDSafe Data Store' means the database administered by or on behalf of the Commonwealth (in the form of the Department of Health and/or the Digital Transformation Agency) for the purpose of contact tracing.

The National COVIDSafe Data Store is the location where COVID app data will be stored when that data is uploaded from an individual's mobile telecommunications device.

'State or Territory health authority' means the State or Territory body responsible for the administration of health services in a State or Territory.

This definition ensures that the relevant health authorities can be provided with COVID app data for limited purposes. Further safeguards are described in the explanation of section 6 below.

Part 2 - Requirements

6 Collection, use or disclosure of COVID app data

Section 6 prohibits COVID app data from being collected, used or disclosed (subsection 6(1)) unless an exception applies (subsection 6(2)).

These limitations are stricter than the standard privacy protections including those in Australian Privacy Principles (APPs) 3 (regarding collection of solicited personal information) and 6 (regarding use or disclosure of personal information) under Schedule 1 of the Privacy Act. To the extent that the s 6 limitations are stricter, they will displace the Privacy Act in relation to COVID app data (see also the explanation of the note at the conclusion of subsection 6(2)).

The Privacy Act continues to apply except to the extent that it is inconsistent with the Determination.

Subsection 6(1) – Prohibition on use of COVID app data

Subsection 6(1) is a general prohibition that prevents use of COVID app data unless one of the exemptions in paragraphs 6(2)(a) to 6(2)(e) apply.

Subsection 6(2) provides that for the purposes of subsection 6(1) – which prohibits handling COVID app data – limited collection, use or disclosure of COVID app data is permitted if the circumstances provided for in paragraphs 6(2)(a) to 6(2)(e) apply.

The broad prohibition ensures that, outside of the specific exceptions listed in paragraphs 6(2)(a) to 6(2)(e), the instrument protects COVID app data from being used for any purpose, by any person, authority or body, that is not expressly provided for in an exception.

Each of the exceptions provided for in paragraphs 6(2)(a) to 6(2)(e) restrict the collection, use or disclosure of COVID app data to only the extent to which the handling is required for the relevant purpose. This protection ensures that COVID app

data is only handled to the extent necessary to achieve the purpose outlined in each exception.

Subsection 6(2) – Exceptions to the prohibition on handling COVID app data

The specific and only exemptions to the prohibition on handling COVID app data as described in subsection 6(1) of this instrument are set out in paragraphs 6(2)(a) to 6(2)(e) which are detailed below:

Paragraph 6(2)(a) – Handling of COVID app data by States and Territories

Paragraph 6(2)(a) provides that the prohibition in subsection 6(1) does not prevent COVID app data from being collected, used or disclosed by an a person employed by, or in the service of a State or Territory health authority for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing. This is set out in a two stage requirement in subparagraphs 6(2)(a)(i) and 6(2)(a)(ii).

As the States and Territories are responsible for contact tracing initiatives, paragraph 6(1)(a) allows relevant persons employed by, or in the service of, a State or Territory health authority to access COVID app data to allow them to contact COVIDSafe app users who have been identified as being in contact with a user who has been diagnosed with the coronavirus known as COVID-19 and subsequently uploaded their information to the National COVIDSafe Data Store.

Subparagraph 6(2)(a)(i) anticipates that, due to the extraordinary conditions imposed by the coronavirus known as COVID-19, there may be persons involved in the contact tracing process who are not technically employees or officers of a State or Territory health authority. Providing that a person may be 'in the service' of a State or Territory health authority allows those authorities to rely on the resources available to them to facilitate contact tracing, while retaining a requirement that there be adequate proximity and oversight by the State or Territory health authority.

Subparagraph 6(2)(a)(ii) sets out the purpose for which the persons described in subparagraph 6(2)(a)(i) may interact with the COVID app data –that is, for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing (as defined and limited in scope by subparagraph 6(4)).

Paragraph 6(2)(b) – Handling of COVID app data by the Health Department and the Digital Transformation Agency

Paragraph 6(2)(b) sets out when an officer, employee or contractor of the Commonwealth Health Department or the Digital Transformation Agency can collect, use or disclose COVID app data. Collection, use or disclosure of COVID app data by a Commonwealth Health Department or Digital Transformation Agency officer, employee or contractor may only occur for the purposes of, and only to the extent required for the purposes of:

- Subparagraph 6(2)(b)(i) – enabling contact tracing by persons employed by, or in the service of State or Territory health authorities;

- Subparagraph 6(2)(b)(ii) – ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store.

Paragraph 6(2)(b) sets out limited circumstances where an employee, officer or contractor of the Health Department or Digital Transformation Agency can interact with COVID app data; and these circumstances do not permit any substantive interaction or use of COVID app data other than to the extent that it is required for the proper functioning, integrity and security of COVIDSafe and provision of relevant data to State and Territory health authorities to perform their contact tracing functions (as anticipated by paragraph 6(2)(a)).

This functionality provided for in paragraph 6(2)(b) limits this administrative access to officers, employees or contractors of the Health Department or Digital Transformation Agency, who will administer the National COVIDSafe Data Store in order to protect access to COVID app data to the narrowest extent practicable while allowing for proper administration of COVIDSafe and the National COVIDSafe Data Store.

The purposes for which persons permitted by subparagraph 6(2)(b)(i) can access COVID app data is limited to ensuring the proper functioning, integrity or security of the COVIDSafe system, comprising of COVIDSafe and the National COVIDSafe Data Store.

Contractors are provided for in this section (in addition to officers and employees), as both the Health Department and the Digital Transformation Agency may engage specialists on a contract basis to ensure the functionality, integrity and security of the COVIDSafe system. The same requirements and restrictions would be placed on any contractor as would be placed on an employee of the Health Department or the Digital Transformation Agency.

Paragraph 6(2)(c) – Permissible handling of COVID app data to facilitate the effective operation of COVIDSafe

Paragraph 6(2)(c) provides that collection or disclosure of COVID app data may occur for the purpose of, and only to the extent required for the purpose of, transferring encrypted data between mobile telecommunications devices through COVIDSafe; or transferring encrypted data, through COVIDSafe, from a mobile telecommunications device to the National COVIDSafe Data Store administered by the Health Department or the Digital Transformation Agency.

The effect of paragraph 6(2)(c) is to facilitate the interactions that will occur between different locations where the COVID app data is held at various times.

Subparagraph 6(2)(c)(i) facilitates the transfer of COVID app data between users' personal mobile telecommunications devices.

Subparagraph 6(2)(c)(ii) facilitates the transfer of COVID app data between a user's personal mobile telecommunications device and the National COVIDSafe Data Store. This will occur in two circumstances:

- When a user first installs COVIDSafe and registers, initial registration information will be uploaded to the National COVIDSafe Data Store.

- If a person is diagnosed with the coronavirus known as COVID-19 and consents to upload their COVID app data, that data would then be uploaded to the National COVIDSafe Data Store.

Paragraph 6(2)(a), subparagraph 6(2)(b)(i) and subparagraph 6(2)(c)(ii) together facilitate the movement of relevant COVID app data between the National COVIDSafe Data Store and a State or Territory health authority.

Paragraph 6(2)(d) – Handling of COVID app data for investigation and prosecution relating to breach of this instrument

Paragraph 6(2)(d) sets out when COVID app data can be collected, used or disclosed for investigative or enforcement purposes:

- Subparagraph 6(2)(d)(i) only allows the collection, use or disclosure of COVID app data for the purposes of, and only to the extent required for the purpose of investigating whether a provision of this instrument has been contravened.
- Subparagraph 6(2)(d)(ii) only allows the collection, use or disclosure of COVID app data for the purpose of, and only to the extent required for the purpose of, prosecuting an offence against section 479 of the *Biosecurity Act 2015* in relation to a contravention of this instrument.

Subsection 477(5) of the *Biosecurity Act 2015* provides that a requirement in a determination applies despite any other law. The instrument does not provide for any secondary uses of COVID app data, therefore COVID app data collected, used or disclosed for an authorised investigative or prosecutorial purpose cannot be used for any other purpose.

Section 479 of the *Biosecurity Act 2015* provides that it is an offence to not comply with a requirement determined under subsection 477(1) of that Act.

Limited disclosures for investigation and prosecution of this instrument and s 479 of the *Biosecurity Act 2015* are critical to the success of COVIDSafe by ensuring the integrity of the process, and protecting against misuse of COVID app data by any person, body or authority.

Paragraph 6(2)(e) – use of COVID app data for producing statistical information

Paragraph 6(2)(e) provides that where COVID app data has been collected through an exemption in subsection 6(2), it is permissible to use the COVID app data for the purpose of, and only to the extent required for the purpose of, producing statistical information that is de-identified. The term ‘de-identified’ is a defined term in section 5 of this instrument.

Limited use of de-identified information for statistical purposes is central to the purpose of COVIDSafe as this information is needed for evaluation purposes – for example, to identify what proportion of the population is using the app, or whether there are outbreaks occurring in certain parts of Australia.

The use of de-identified statistical information is important as understanding the coronavirus known as COVID-19 and the effects of community transmission is a critical public health function. However, to protect the privacy of COVIDSafe

users, it will only be permissible to produce this statistical information if the information has been de-identified so it is no longer about an identifiable or reasonably identifiable individual.

The use of de-identified statistical information is also important to ensure a degree of transparency and accountability in relation to the collection, use and disclosure of COVID App data.

Note at the conclusion of subsection 6(2) – Interaction with the Privacy Act

The note at the end of subsection 6(2) clarifies that the Privacy Act will continue to apply except to the extent that it is inconsistent with this instrument.

Subsection 477(5) of the *Biosecurity Act 2015* (which is the enabling Act for this instrument) provides that the provisions in this instrument apply despite any other Australian law.

The purpose of this note is to clarify that other statutory provisions, such as the more expansive collection, use and disclosure provisions in the Privacy Act, or other collection powers in the legislation of law enforcement or other regulatory bodies will be superseded by this instrument to the extent that there are inconsistencies in the manner in which COVID app data may be handled.

Where an inconsistency with this instrument does not occur, other Australian laws, including the Privacy Act will continue to apply. For example, to the extent that this instrument does not explicitly address privacy protections, the requirements to maintain a privacy policy under Australian Privacy Principle 1, take reasonable steps to ensure the security of personal information under Australian Privacy Principle 11, and to notify certain kinds of data breaches under Part IIIC of the Privacy Act, would apply (to the extent that COVID app data is personal information for the purposes of that Act).

Subsection 6(3) – Definition of COVID app data

Subsection 6(3) defines COVID app data. Under this subsection, COVID app data is data that has been collected or generated through the operation of an app (COVIDSafe) that is made available, by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing; and is, or has been stored on a mobile telecommunications device.

This definition of COVID app data ensures that the protections in this instrument are appropriately targeted by identifying the key information that is central to the operation of COVIDSafe.

The final sentence of subsection 6(3) confirms that, where a State or Territory health authority undertakes contact tracing on the basis of COVID app data, any information obtained during the contact tracing process (that is, obtained from a source other than the National COVIDSafe Data Store such as a subsequent contact tracing interview) is not considered to be COVID app data. This has been included to make clear that the instrument does not hinder the effectiveness of State and Territory health authorities' contact tracing processes.

Subsection 6(4) – Definition of contact tracing

Subsection 6(4) defines contact tracing. Under this subsection, for the purposes of this instrument, contact tracing is the process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID-19. The term 'in contact' is a defined term under section 5 of this instrument.

Paragraphs 6(4)(a) to 6(4)(c) set out what is included in the definition of 'contact tracing' and includes notifying, or providing information or advice to a person who has come in contact with a person who has been diagnosed with the coronavirus known as COVID-19 (or a person responsible for that person); or providing information or advice to a person who has tested positive for the coronavirus known as COVID-19 (or is responsible for a person who meets one of those criteria).

The restrictions placed on contact tracing ensure that COVID app data is used for a legitimate public health purpose in identifying and contacting individuals who are at greater risk of contracting the coronavirus known as COVID-19, or providing advice to those who have been diagnosed with the coronavirus known as COVID-19.

Subsection 6(4) allows COVID app data to be used to contact both the individual about whom the information relates, or, where applicable, the person responsible for that person. This recognises that there are vulnerable individuals within the community who may require another person to be the contact point for them, such as children, the elderly, or persons with disability. By allowing this additional use for COVID app data, it ensures that individuals who have a carer or other responsible person who is a more appropriate contact are not restricted from utilising COVIDSafe on the basis that the second person could not be contacted under a more restrictive definition.

7 Treatment of COVID app data

Section 7 sets out broad prohibitions and relevant exceptions for how COVID app data is uploaded to the National COVIDSafe Data Store and how COVID app data must be handled and stored after it has been uploaded.

Section 7 is divided into two topics – regarding COVID app data on mobile telecommunications devices, and COVID app data in the National COVIDSafe Data Store. Subsections 7(1) and 7(2) address COVID app data held on a mobile telecommunications device while subsections 7(3) to 7(5) address COVID app data held in the National COVIDSafe Data Store.

Subsection 7(1) – prohibition on upload of COVID app data to the National COVIDSafe Data Store without consent

Subsection 7(1) provides that a person must not upload COVID app data from a mobile communications device to the National COVIDSafe Data Store except with the consent of the person who has possession or control of the device.

Subsection 7(1) provides protections for individuals by ensuring that individuals must consent before their information is uploaded to the National COVIDSafe Data Store.

The protections in subsection 7(1) underpin that participation in COVIDSafe is voluntary, and that individuals will not be required to upload information to the National COVIDSafe Data Store at any time without their consent (the voluntary nature of COVIDSafe is further addressed in section 9 of this instrument).

Subsection 7(2) – Prohibition of retention of COVID app data on a mobile telecommunications device beyond 21 days

Subsection 7(2) provides that a person must not cause COVID app data (other than initial registration data or a unique identifier) to be retained on a mobile telecommunications device for more than 21 days.

This restriction prevents COVIDSafe from retaining COVID app data on an individual's mobile telecommunications device (other than initial registration data or a unique identifier) for a period of longer than 21 days.

Subsection 7(3) – prohibition on overseas retention or disclosure of COVID app data held in the National COVIDSafe Data Store

Subsection 7(3) requires that where app data is uploaded from a mobile telecommunications device to the National COVIDSafe Data Store, a person must not (under paragraph 7(3)(a)), retain the data on a database outside Australia; or (under paragraph 7(3)(b)), disclose the data to a person outside Australia except as provided in subsection 7(4) (described further below).

Subsection 7(3) only applies to the National COVIDSafe Data Store, and does not apply to any COVID app data while it is stored on an individual's personal mobile telecommunications device.

Paragraph 7(3)(a) – Prohibition on overseas retention

Paragraph 7(3)(a) creates a prohibition that ensures COVID app data uploaded to the National COVIDSafe Data Store is held in Australia (by prohibiting the information from being retained outside Australia). This is a safeguard to provide an additional layer of protection for COVID app data by ensuring that the National COVIDSafe Data Store is physically within Australia's jurisdiction.

Paragraph 7(3)(b) – Prohibition on overseas disclosure

Paragraph 7(3)(b) creates a prohibition against disclosing COVID app data that has been uploaded to the National COVIDSafe Data Store to a person outside Australia. This prohibition ensures that where COVID app data is held in the COVIDSafe Data Store, that data cannot be disclosed outside Australia without contravening this instrument.

Due to the operation of subsection 477(5) of the *Biosecurity Act 2015*, this prohibition extends to any requirements, rights or obligations in other Australian laws that may require or allow COVID app data to be provided to a person outside Australia.

Subsection 7(4) – Exemption to the overseas disclosure prohibition in paragraph 6(3)(b) to facilitate contact tracing with persons who may be overseas

Subsection 7(4) provides an exemption to paragraph 7(3)(b) to allow COVID app data to be disclosed to a person outside Australia where two conditions are met:

- Firstly, the disclosure must be by a person employed by, or in the service of, a State or Territory heath authority; and
- Secondly, the disclosure must be for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.

Paragraph 6(2)(a) and subsection 6(4) of this instrument set out the scope of how authorised State and Territory health authority persons may handle COVID app information and what is considered to be 'contact tracing' for the purposes of this instrument. Subsection 7(4) acts to ensure that contact tracing efforts using COVID app data are not hindered or frustrated because a person is outside of Australia.

From a practical perspective, based on the limited information collected, it is not possible to know whether a person is located in Australia at the time they are being contacted for the purposes of contact tracing. This is due to COVID app information recording interactions between users that may have occurred within the previous 21 days. This ensures that authorised persons undertaking contact tracing do not unintentionally breach subsection 7(4) whilst undertaking legitimate contact tracing activities as specified in section 6(4).

Subsection 7(5) – Prohibition on COVID app data being retained on the National COVIDSafe Data Store after the end of the coronavirus known as COVID-19 pandemic has concluded.

Subsection 7(5) requires the Commonwealth to delete any COVID app data retained in the National COVIDSafe Data Store after the conclusion of the coronavirus known as COVID-19 pandemic. This is a positive obligation placed on the Commonwealth to delete COVID app data, and failure to do so would constitute a breach of this instrument.

The deletion of all centrally held COVID app data is a safeguard that recognises that once the COVID-19 pandemic has concluded, there is no legitimate purpose for COVID app information to be retained. Subsection 7(5) therefore protects against misuse or unauthorised access to COVID app data in the period after that information has served its legitimate purpose.

For the purpose of this instrument, the conclusion of the COVID-19 pandemic would be determined based on advice from the Australian Health Protection Principal Committee. This ensures that independent medical advice and best practice is adhered to in considering the appropriateness of terminating the COVIDSafe app and deleting all COVID app data stored in the National COVIDSafe Data Store due to the conclusion of the COVID-19 pandemic.

Note after subsection 7(5) – override of other Australian data retention laws

The note at the end of subsection 7(5) clarifies that the requirement in subsection 7(5) for the Commonwealth to delete all COVID app data retained on the National COVIDSafe Data Store has the effect of overriding any other obligations under

Australian law (for example, under the *Archives Act 1983*) that requires that information or data be retained, in accordance with Subsection 477(5) of the *Biosecurity Act 2015*.

8 Decrypting COVID app data

Section 8 prohibits a person from decrypting encrypted COVID app data that is stored on a mobile telecommunications device.

Section 8 places a blanket prohibition, with no exceptions, on decrypting encrypted COVID app data that is stored on a mobile telecommunications device. This prohibition is provided for as there is no legitimate purpose for COVID app data to be decrypted while remaining on an individual's mobile telecommunications device.

An effect of section 8 of this instrument is that it protects against access to COVID app data by law enforcement in circumstances where a law enforcement agency has legitimate access to an individual's mobile telecommunications device under statute (for example under a provision that may allow access for the purposes of pursuing an investigation).

9 Coercing the use of COVIDSafe

Section 9 of this instrument ensures that individuals cannot be coerced or otherwise required to use or install COVIDSafe, whether via positive obligation, or adverse consequence on the basis of refusal to participate in the App.

Subsection 9(1) provides that a person must not require another person to download COVIDSafe to a mobile telecommunications device, have COVIDSafe in operation on a mobile telecommunications device; or consent to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

Subsection 9(2) provides a prohibition against disadvantaging a person on the basis that a person has not downloaded COVIDSafe to a mobile telecommunications device; does not have COVIDSafe in operation on a mobile telecommunications device; or has not consented to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

These protections include prohibiting a person from:

- refusing to enter into, or continue, a contract or arrangement with another person (including a contract of employment);
- taking adverse action (within the meaning of the *Fair Work Act 2009*) against another person;
- refusing to allow another person to enter premises;
- refusing to allow another person to participate in an activity;
- refusing to receive goods or services from another person; or
- refusing to provide goods or services to another person.

on the ground that, or on grounds that include the ground that, the other person has not downloaded COVIDSafe to a mobile telecommunications device; does not have COVIDSafe in operation on a mobile device; or has not consented to uploading COVIDSafe data from a mobile device to the National COVIDSafe Data Store.

Subsection 9(1) and subsection 9(2) operate in tandem to create a comprehensive framework to protect individuals from disadvantage on the basis of choosing not to install COVIDSafe.

These protections are necessary to protect a person's choice to install COVIDSafe.