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

I, Greg Hunt, Minister for Health, make the following determination.

Dated 25 April 2020

Greg Hunt
Minister for Health

OPC64599 - A

Contents

Part 1—Preliminary

1 Name

This instrument is the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	11.59 pm (by legal time in the Australian Capital Territory) on the day this instrument is registered.	25 April 2020

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

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

4 Object

The object of this instrument is to make contact tracing faster and more effective by encouraging public acceptance and uptake of COVIDSafe.

5 Definitions

Note: A number of expressions used in this instrument are defined in the *Biosecurity Act 2015*, including the following:
(a) Australian law;
(b) Health Department;
(c) State or Territory body.

In this instrument:

contact tracing has the meaning given by subsection 6(4).

COVID app data has the meaning given by subsection 6(3).

COVIDSafe has the meaning given by paragraph 6(3)(a).

de-identified: information is ***de-identified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

in contact: a person 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 the proximity of the other person.

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 (within the meaning of that Act).

National COVIDSafe Data Store means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.

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

Part 2—Requirements

6 Collection, use or disclosure of COVID app data

(1) A person must not collect, use or disclose COVID app data except as provided by subsection (2).

(2) Subsection (1) does not prevent a person from collecting, using or disclosing COVID app data if:

(a) the collection, use or disclosure:

(i) is by a person employed by, or in the service of, a State or Territory health authority; and

(ii) is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing; or

(b) the collection, use or disclosure is by an officer, employee or contractor of the Health Department or the Digital Transformation Agency for the purpose of, and only to the extent required for the purpose of:

(i) enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or

(ii) ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store; or

(c) in the case of a collection or disclosure of COVID app data—the collection or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) transferring encrypted data between mobile telecommunications devices through COVIDSafe; or

(ii) transferring encrypted data, through COVIDSafe, from a mobile telecommunications device to the National COVIDSafe Data Store; or

(d) the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) investigating whether a requirement of this determination has been contravened; or

(ii) prosecuting a person for an offence against section 479 of the *Biosecurity Act 2015* in relation to a contravention of this determination; or

(e) in the case of a use of COVID app data—the use is for the purpose of, and only to the extent required for the purpose of, producing statistical information that is de-identified.

Note: The *Privacy Act 1988* continues to apply except to the extent that it is inconsistent with this determination: see subsection 477(5) of the *Biosecurity Act 2015*.

(3) ***COVID app data*** is data relating to a person that:

(a) 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

(b) is, or has been, stored on a mobile telecommunications device.

However, it does not include information obtained, from a source other than the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority.

(4) ***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, and includes:

(a) notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and

(b) notifying a person who is responsible for another person that the other person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and

(c) providing information and advice to a person who:

(i) has tested positive for the coronavirus known as COVID-19; or

(ii) is responsible for another person who has tested positive for the coronavirus known as COVID-19; or

(iii) has been in contact with a person who has tested positive for the coronavirus known as COVID-19; or

(iv) is responsible for another person who has been in contact with a person who has tested positive for the coronavirus known as COVID-19.

7 Treatment of COVID app data

COVID app data on mobile telecommunications devices

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

(2) 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.

COVID app data in the National COVIDSafe Data Store

(3) If COVID app data is uploaded from a mobile telecommunications device to the National COVIDSafe Data Store, a person must not:

(a) retain the data on a database outside Australia; or

(b) disclose the data to a person outside Australia.

(4) Paragraph (3)(b) does not apply to a disclosure by a person employed by, or in the service of, a State or Territory health authority if the disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.

(5) The Commonwealth must cause COVID app data in the National COVIDSafe Data Store to be deleted after the COVID-19 pandemic has concluded.

Note: The requirements in this section will override any obligation under an Australian law to retain data for a longer period: see subsection 477(5) of the *Biosecurity Act 2015*.

8 Decrypting COVID app data

A person must not decrypt encrypted COVID app data that is stored on a mobile telecommunications device.

9 Coercing the use of COVIDSafe

(1) A person must not require that another person:

(a) download COVIDSafe to a mobile telecommunications device; or

(b) have COVIDSafe in operation on a mobile telecommunications device; or

(c) consent to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

(2) A person must not:

(a) refuse to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or

(b) take adverse action (within the meaning of the *Fair Work Act 2009*) against another person; or

(c) refuse to allow another person to enter premises; or

(d) refuse to allow another person to participate in an activity; or

(e) refuse to receive goods or services from another person; or

(f) refuse to provide goods or services to another person;

on the ground that, or on grounds that include the ground that, the other person:

(g) has not downloaded COVIDSafe to a mobile telecommunications device; or

(h) does not have COVIDSafe in operation on a mobile telecommunications device; or

(i) has not consented to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.