Australian Government

Office of the Australian Information Commissioner

COVIDSafe Report May–November 2022

Report under Part VIIIA of the *Privacy Act 1988*

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

30 November 2022

OAIC

Contents

About this report

The Australian Government launched the voluntary COVIDSafe app (COVIDSafe) on 27 April 2020.

On 16 May 2020, the Office of the Australian Information Commissioner (OAIC) was granted additional functions and powers in relation to COVIDSafe under Part VIIIA of the *Privacy Act 1988*.

The object of Part VIIIA was to assist in preventing and controlling the entry, emergence, establishment or spread of COVID-19 into or within Australia by providing stronger privacy protections for COVID app data and COVIDSafe users.

Part VIIIA expanded the Commissioner's regulatory oversight role to apply to state and territory health authorities, to the extent that they dealt with COVID app data.

It enhanced the Commissioner's role in dealing with eligible data breaches and conducting assessments and investigations in relation to COVIDSafe and COVID app data. It enabled the Commissioner to refer matters to, and share information or documents with, state or territory privacy authorities. It also applied the Privacy Act's rules and privacy protections and Commonwealth oversight to state and territory health authorities in relation to COVID app data.

In accordance with s 94ZB of the Privacy Act, this report sets out the performance of the Commissioner's functions and the exercise of the Commissioner's powers under or in relation to Part VIIIA.

The Minister for Health and Aged Care determined on 16 August 2022 that COVIDSafe was no longer required to prevent or control the entry, emergence, establishment or spread of COVID-19 in Australia.

This is the OAIC's final report under s 94ZB, covering the period **16 May to 15 November 2022**.

Executive summary

The OAIC's first COVIDSafe report detailed the Commissioner's powers in relation to the COVIDSafe system.

During the reporting period 16 May to 15 November 2022, the OAIC received **no enquiries or complaints** about the COVIDSafe system.

We completed the COVIDSafe Assessment Program, finalising **2 assessments**.

The Commissioner was not required to exercise her powers in relation to complaints, investigations, information sharing and data breaches.

Commissioner's powers

During the reporting period of 16 May to 15 November 2022, the following matters were recorded in relation to Part VIIIA:

Table 1 — Number of matters related to the COVIDSafe system

Regulatory function	Number
Enquiries received	0
Complaints received	0
Investigations	0
Commissioner-initiated investigations	0
Information sharing	0
Assessments finalised	2
Assessments underway	0
Data breach notifications received	0

COVIDSafe guidance and advice

The OAIC published a Privacy update on the COVIDSafe app following the Minister for Health and Aged Care's determination that COVIDSafe is no longer required to prevent or control the entry, emergence, establishment or spread of COVID-19 in Australia.

The guidance outlines the determination's purpose and explains next steps for the deletion of COVID app data, as required by Part VIIIA.

To avoid confusion, the OAIC removed the following COVIDSafe guidance from our website:

- The COVIDSafe app and my privacy rights
- The COVIDSafe app and my privacy rights in other languages (Arabic, Greek, Italian, Spanish, Thai, Hindi, Punjabi, Vietnamese, Traditional Chinese and Simplified Chinese)
- Guidance for state and territory authorities regarding COVIDSafe and COVID app data
- Privacy obligations regarding COVIDSafe and COVID app data.

Assessments

We detailed our COVIDSafe Assessment Program in the first COVIDSafe report. This program was completed during the reporting period with the finalisation of COVIDSafe assessments 2 and 5.

Summary of COVIDSafe Assessment 2

Assessment 2 examined the access controls applied to COVID app data by state and territory health authorities.

At the time of fieldwork, 3 state and territory health authorities had accessed COVID app data in the National COVIDSafe Data Store.

The assessment found state and territory health authorities were:

- generally taking reasonable steps to secure the personal information of COVIDSafe registered users in accordance with the requirements of Australian Privacy Principle 11.1
- complying with the relevant data handling provisions under Part VIIIA of the Privacy Act.

The OAIC identified 20 medium privacy risks and 23 low privacy risks associated with state and territory health authorities' handling of COVID app data. Risk areas included:

- the collection of COVID app data into paper or electronic records by the 3 state and territory health authorities
- documentation of processes and procedures around the collection, use, storage and disclosure of COVID app data
- privacy impact assessments not being undertaken or, where undertaken, recommendations not being actioned.

The OAIC made 20 recommendations and 23 suggestions to address those privacy risks. More information on the assessment is available in the summary report.

Summary of COVIDSafe Assessment 5

Assessment 5 examined the compliance of the National COVIDSafe Data Store Administrator with the deletion and notification requirements for the end of the COVIDSafe data period under s 94P of the Privacy Act.

At the time of fieldwork, the Department of Health and Aged Care was the Data Store Administrator.

The assessment found the Data Store Administrator:

- had complied with its obligations to not collect any COVID app data and to ensure COVIDSafe is not available for download
- had deleted all COVID app data from the Data Store as soon as reasonably practicable
- was taking all reasonable steps to inform COVIDSafe users that COVID app data had been deleted from the Data Store and they should delete COVIDSafe from their communication device
- had not taken all reasonable steps to inform COVIDSafe users that COVID app data can no longer be collected.

The OAIC made 2 suggestions to address privacy risks. More information on the assessment is available in the assessment report.

Inspector-General of Intelligence and Security COVIDSafe report

The Inspector-General of Intelligence and Security assists ministers in overseeing and reviewing the legality and propriety of the activities of 6 of Australia's intelligence and security agencies, including their compliance with Part VIIIA of the Privacy Act. These agencies are:

- Australian Security Intelligence Organisation
- Australian Secret Intelligence Service
- Australian Signals Directorate
- Australian Geospatial-Intelligence Organisation
- Defence Intelligence Organisation
- Office of National Intelligence.

The Inspector-General reviewed the agencies' compliance with Part VIIIA between 16 May and 15 November 2022 and provided an unclassified report for the Commissioner to consider in preparing this report.

The report notes:

- There is no evidence that any agency has deliberately targeted, decrypted, accessed or used any COVID app data.
- IGIS found the agencies have appropriate policies and procedures in place regarding any incidental collection of COVID app data and are adhering to them. Agencies are taking reasonable steps to quarantine and delete such data as soon as practicable after becoming aware it has been collected.
- IGIS has not received any complaints or public interest disclosures about COVID app data.

The IGIS report is provided as Attachment A to this report and is also published on the IGIS website.

Glossary

Term	Definition
Australian Privacy Principles (APPs)	The APPs are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers. There are 13 APPs and they govern standards, rights and obligations around: • the collection, use and disclosure of personal information • an organisation or agency's governance and accountability • integrity and correction of personal information • the rights of individuals to access their personal information.
Contact tracing	Section 94D(6): 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 a parent, guardian or carer of 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 a parent, guardian or carer of 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 a parent, guardian or carer of another person who has been in contact with a person who has tested positive for the coronavirus known as COVID-19.
COVID app data	Section 94D(5): Data relating to a person that:

	(a) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and (b) either: (i) is registration data; or (ii) is stored, or has been stored (including before the commencement of this Part), on a communication device. However, it does not include: (c) information obtained, from a source other than directly from 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; or (d) de-identified statistical information about the total number of registrations through COVIDSafe that is produced by: (i) an officer or employee of the data store administrator; or (ii) a contracted service provider for a government contract with the data store administrator.
COVIDSafe app (COVIDSafe)	Section 6(1): An app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.
National COVIDSafe Data Store (Data Store)	Section 6(1): The database administered by or on behalf of the Commonwealth for the purpose of contact tracing.
National COVIDSafe Data Store Administrator (Data Store Administrator)	From 16 May 2020 to 26 September 2021 the Digital Transformation Agency (DTA) was the sole Data Store Administrator. Between 27 September and 4 October 2021, this function transitioned to the Department of Health. From 5 October 2021, the Department of Health is the sole Data Store Administrator and the DTA no longer has access to COVID app data and information collected through COVIDSafe. Under an Administrative Arrangements Order, the Department of Health became the Department of Health and Aged Care on 1 July 2022.

Attachment A: COVID app data and Intelligence Agencies within IGIS jurisdiction

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

COVID app data and Intelligence Agencies within IGIS jurisdiction

16 May 2022 – 15 Nov 2022

Fifth and Final Report

The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security

21 November 2022

IGIS Report to the Office of the Australian Information Commissioner (OAIC) on COVID app data – 16 May 2022 to 15 November 2022

Background

This is the fifth and final six-monthly report[1] by the Inspector-General of Intelligence and Security (IGIS) regarding intelligence agencies within jurisdiction and their compliance with Part VIIIA of the *Privacy Act 1988* (the Privacy Act). This report is provided to the Privacy Commissioner so that she may take this information into account when preparing her report under s 94ZB of the Privacy Act.

Summary of findings

The Inspector-General's staff have continued to work with relevant[2] agencies to monitor their activities in ensuring compliance with Part VIIIA of the Privacy Act. IGIS staff have also conducted inspections of these agencies to determine whether COVID app data that has been collected incidentally[3] has not been accessed or used, and is deleted as soon as practicable after the agency becomes aware it has been collected.

The key findings from these inspections are as follows:

- There is no evidence to suggest agencies have deliberately targeted or have decrypted, accessed or used COVID app data.
- Relevant agencies continue to take reasonable steps to quarantine and delete COVID app data.
- Appropriate policies and procedures remain in place and are being adhered to regarding any incidental collection of COVID app data that is identified.

Prohibition against 'disclosure'

In previous reports the Inspector-General has flagged the requirement for discussions between relevant agencies and the OAIC to address prohibitions against disclosure. The Inspector-General is aware these discussions have occurred and appropriate agreement has been reached between the parties.

Complaints

- No complaints or public interest disclosures about COVID app data have been received.

Next steps

- This will be IGIS' final report on the intelligence agencies' compliance with Part VIIIA of the Privacy Act. The COVID app has now been decommissioned and the relevant parts of the Privacy Act have been repealed.

---

[1] This and the first four reports are available at www.igis.gov.au/what-we-do/inspections/cross-agency-matters

[2] Not all intelligence agencies with IGIS's jurisdiction have functions or technical capabilities which may enable them to collect COVID app data.

[3] The Privacy Act recognises that incidental collection of COVID app data may occur as part of agency functions.