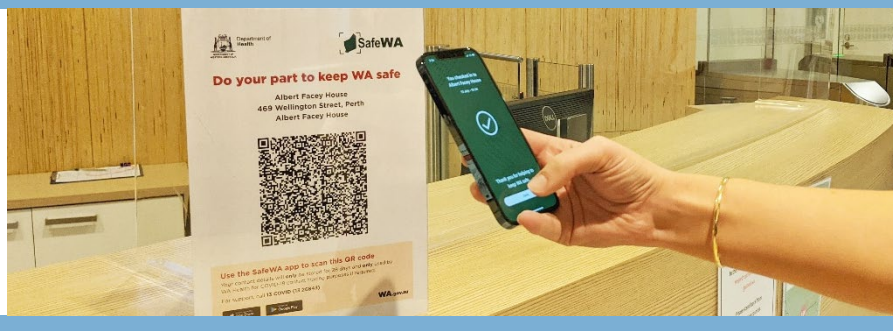
Western Australian
Auditor General's Report



SafeWA – Application Audit

Report 2: 2021-22

2 August 2021

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Jordan Langford-Smith
Michael Chumak
Paul Tilbrook

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for
those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

SafeWA – Application Audit

Report 2: 2021-22
August 2021

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

SAFEWA – APPLICATION AUDIT

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

I wish to acknowledge the entities' staff for their cooperation with this audit.

CAROLINE SPENCER
AUDITOR GENERAL
2 August 2021

Contents

Auditor General's overview

This report summarises the results of our audit of WA Health's SafeWA digital contact registration application which supports WA Health's contact tracing efforts. The purpose of this audit was to gain assurance about the integrity, availability and confidentiality of information generated by or stored in SafeWA and related systems.

The global COVID-19 pandemic has disrupted many aspects of how we live, including the way we carry out routine tasks like going to the shops and attending events.

Frontline health responses and law enforcement have had a significant role in how governments have managed and contained outbreaks, often adapting or employing new technologies in the process. Many governments both here in Australia and overseas are using mobile applications to record the proximity of people, so they can be isolated if directed to contain the spread of the virus. The SafeWA digital application was developed for the purpose of registering contact details for patrons attending venues in Western Australia. Use of the application by venue operators and patrons is voluntary, promoted as a contactless and convenient way for people to check in. If SafeWA is not used, patrons are required under public health directions to register their attendance in a paper contact register.

WA Health delivered the SafeWA application in November 2020 under significant time pressure, and has continued to work with the vendor to address weaknesses and make improvements. The system supports WA Health to carry out COVID contact tracing.

However, decisions made and programs delivered under time pressure can result in unintended consequences. Of most concern in this instance was the use of personal information collected through SafeWA for purposes other than COVID contact tracing. Urgent legislative amendments were passed in June 2021 to address this issue. Of further concern, is the ongoing limited communication around WA Health's use of personal information collected by other government entities (including Transperth SmartRider and Police G2G border crossing pass data, see Figure 2) in its contact tracing efforts. We will examine this issue further in a separate audit of WA Health's PHOCUS system, which accesses data from these and other sources, including SafeWA. In the absence of any comprehensive privacy legislation in Western Australia, including oversight mechanisms, citizens have a right to expect that their personal information will only be used by governments in line with stated purposes.

My predecessor, Des Pearson AO, made a similar observation in 2002 when he noted *"In a paper-based environment there were obvious physical limitations to the public sector's ability to monitor, collect, store, manipulate and share information. Technology has removed most of those limitations. In so doing it has created a very real risk of compromising the right to individual privacy. In this environment the public has a right to reassurance that government is addressing this risk."* [1]

Protecting the privacy of citizens' information and being transparent about the use of data helps ensure trust in public institutions is not eroded. This is necessary not only when responding to a viral pandemic, but also for the ongoing peace and prosperity of our democratic society.

[1] Auditor General for Western Australia, *Second Public Sector Performance Report 2002*, Report No 8, December 2002, p. 4

Application audits

Introduction

Applications are software programs that facilitate an organisation's key business processes such as finance, human resources, case management, licensing, billing and service delivery. They enable entities to perform important functions that are unique and essential to them. If applications and their related processes are not managed appropriately stakeholders, including the public, may be affected.

Each year we review a selection of important applications that entities rely on to deliver services. We focus on the key controls that ensure information is complete, accurately captured, processed and maintained. Failures or weaknesses in these controls have the potential to affect other organisations and the public. Impacts range from delays in service and loss of information, to possible fraudulent activity and financial loss.

Our testing may highlight weaknesses in control design or implementation that increase the risk that an application's information may be susceptible to compromise. While our tests are not designed to identify if information has been compromised, we may become aware of instances during an audit.

Audit focus and scope

Our application audits focus on people, process, technology and data. In considering these elements, we follow data from input and processing through to storage, handling and outputs. The purpose of this SafeWA audit was to gain assurance that the integrity, availability and confidentiality of information generated by or stored in SafeWA was appropriate. During the audit we identified that WA Health's Mothership and Public Health COVID Unified System (PHOCUS) access SafeWA data. We included the Mothership review in this audit and will separately report to the Parliament on the PHOCUS system.

We formally advised WA Health of the audit on 28 January 2021. However, we did not commence our testing until March 2021, after WA Health requested we defer the audit. This was to accommodate updates to SafeWA in response to the WA State Government decision to expand mandated contact registration and rollout of the State's vaccination system.

We reviewed a sample of key controls and processes to obtain reasonable assurance that SafeWA worked as intended and that information it contained and reports generated were reliable, accessible and secure.

SafeWA – WA Health

Introduction

SafeWA is a digital COVID-19 contact registration system that was made available to the public for free in November 2020 to support WA Health's contact tracing efforts. It uses a unique venue QR code to collect the name and contact details of users attending venues. WA Health quickly developed and implemented the system in 3 weeks in response to a request from the State Government.

It was not possible to review the information security risks associated with SafeWA without looking at the additional PHOCUS system, which WA Health uses to aggregate multiple sources of information for contact tracing. Therefore, we expanded the scope of our SafeWA audit to cover PHOCUS. The detailed results from our review of PHOCUS will be included in a separate report to the Parliament.

Conclusion

WA Health successfully delivered the SafeWA digital contact registration system in November 2020 under significant time pressure following a request from the State Government. The system plays a key role in supporting WA Health to carry out COVID-19 contact tracing.

WA Health has continued to work with its vendor to improve SafeWA and related applications to address a number of identified weaknesses that could compromise the confidentiality, integrity and availability of information.

A system outage due to poor management of changes after the initial release of SafeWA, put the availability of SafeWA at risk. WA Health has addressed this risk and continues to manage the vendor contract which has required changes as the State's strategy on the use of SafeWA has evolved.

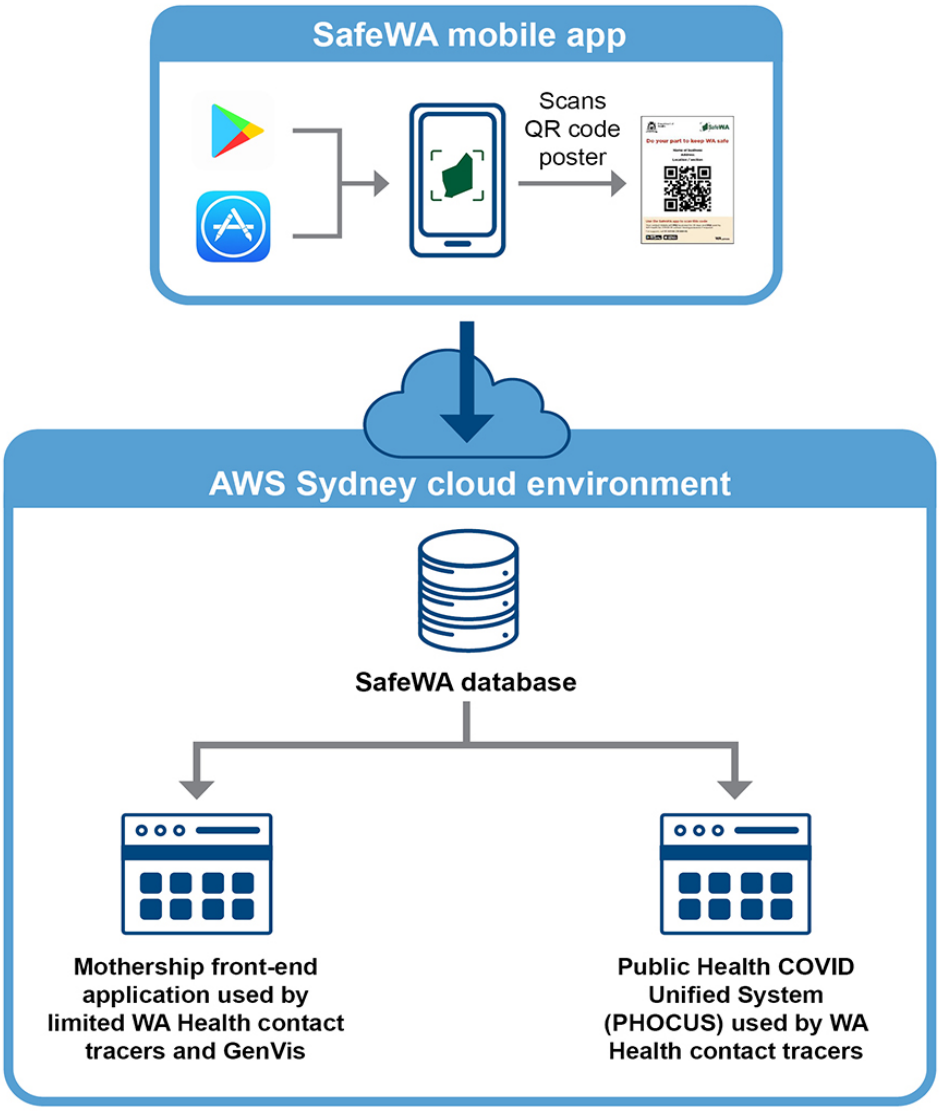
Significantly, we found that the stated narrow use of the SafeWA data and associated paper registers for only COVID-19 contact tracing purposes, had not been safeguarded. The WA Police Force ordered access to the data on 6 occasions and requested access on 1 occasion. The orders were issued by Justices of the Peace after application by the WA Police Force. WA Health ultimately provided access in response to 3 of the orders before the State Government passed urgent legislation[2] to prevent this from occurring in the future and to align with the publicly stated purpose of the data only being used for COVID-19 contact tracing. Further, there remains limited communication on how WA Health uses other personal information for contact tracing purposes.

Background

In response to the COVID-19 pandemic, on 5 December 2020, the State Government made it mandatory for particular businesses to maintain a contact register to improve the State's contact tracing capabilities (for timeline, see Appendix 1).

The contact registration systems (Figure 1) include the SafeWA application and contact information collected using paper registers. SafeWA captures sensitive personal information including name, email address, phone number, venue or event visited, time and date, and information about the device used to check-in. SafeWA information is hosted in the Amazon (AWS) Sydney based cloud environment.

[2] *Protection of Information (Entry Registration Information Relating to COVID-19 and Other Infectious Diseases) Act 2021*



Source: OAG using WA Health information

Figure 1: SafeWA and related systems

By the end of May 2021, over 1.9 million individuals and 66,500 businesses (with 98,569 venues) were registered in the SafeWA application. The total number of check-in scans between December 2020 and May 2021 exceeded 217 million.

Health Support Services[3], acting on behalf of WA Health engaged a third-party vendor, GenVis, and worked in partnership to develop and manage the SafeWA mobile application and its supporting infrastructure.

SafeWA stores individual and business check-in data using the AWS cloud. GenVis has processes in place to delete check-in data 28 days after collection. Should a member of the public test positive for COVID-19 or qualify as a close contact, WA Health may store a subset of the data relevant to that case indefinitely.

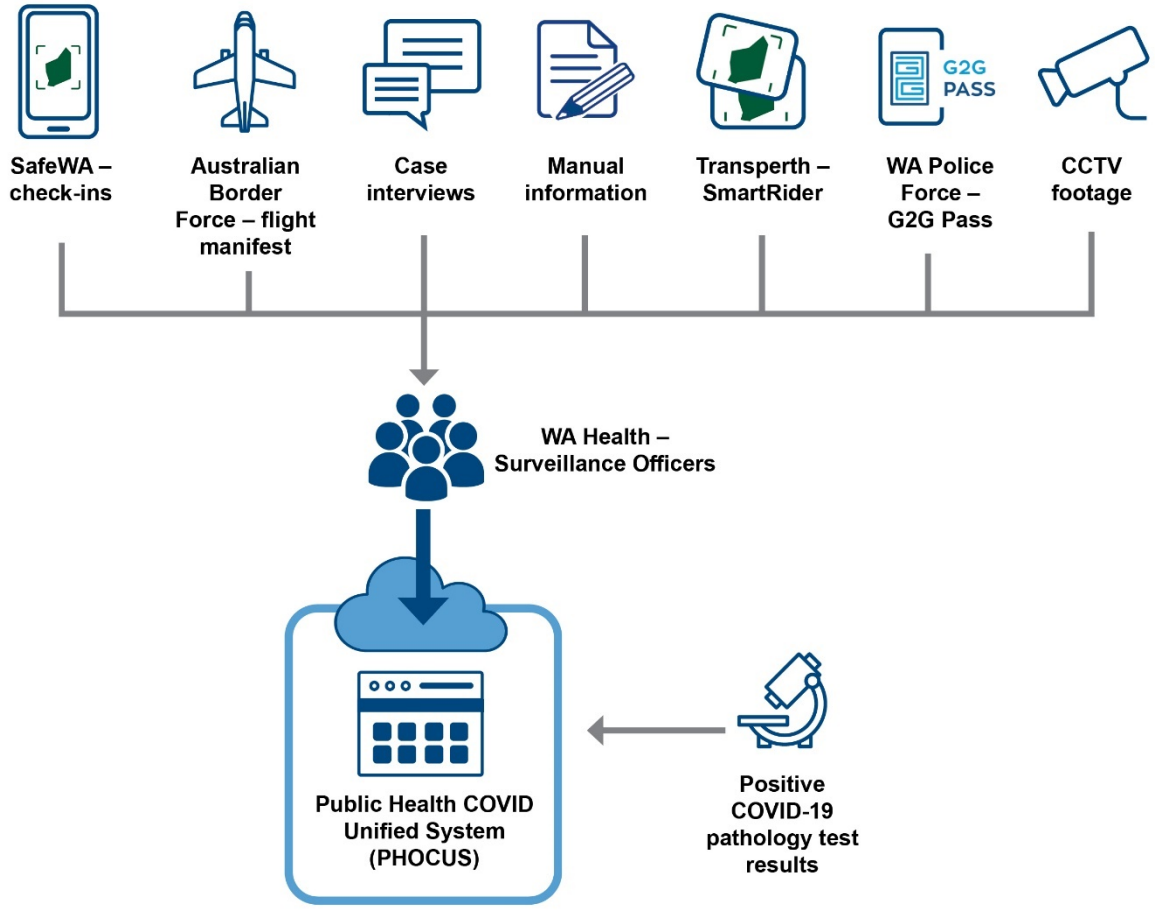
[3] Health Support Services is the shared service centre for the WA Health system and provides IT services to support WA public hospitals and health services.

GenVis also developed the front-end web application (Mothership) used by a small number of authorised WA Health contact tracers and GenVis helpdesk staff to query SafeWA check-in information.

WA Health engaged a cyber security company to carry out an independent security assessment (penetration test) prior to the release of the SafeWA mobile application.

As part of the rollout, SafeWA was integrated with WA Health's existing contact tracing application, PHOCUS, to improve the effectiveness and efficiency of its contact tracing process through automation. PHOCUS is a cloud-based Salesforce application. When WA Health receives confirmation of a positive COVID-19 case from a pathology clinic, it uses PHOCUS to collate data relevant to the case from several sources. These sources can include SafeWA, closed circuit television (CCTV) footage and Transperth SmartRider card use (Figure 2). PHOCUS ingests and presents the combined data to the contact tracing team at WA Health's Public Health Emergency Operations Centre.

Under the *Emergency Management Act 2005* and the *Public Health Act 2016*, WA Health is responsible for the planning, management and ongoing preparedness for Western Australia's response to matters related to public health, including COVID-19 outbreaks, under the direction of the State Emergency Coordinator (the Commissioner of Police). Given the personal nature of much of the information collected during the State Government's COVID-19 response, WA Health needs effective controls to protect the confidentiality, integrity and availability of information gathered through SafeWA check-ins.



Source: OAG using WA Health information

Figure 2: PHOCUS application accesses data from a variety of sources including SafeWA

Findings

WA Health released SafeWA information for purposes other than contact tracing and there is limited information provided to the public about how WA Health uses other personal information

WA Health has released SafeWA check-in information for purposes other than COVID-19 contact tracing, despite State Government messaging that the information would only be used to support contact tracing. In addition, there is limited information available to the public about how WA Health uses personal information (Figure 2) collected by other government entities as part of its contact tracing efforts. Transparency around the use of personal information improves public awareness and trust in government processes and decision-making.

In March 2021, in response to our audit questioning around data access and usage, WA Health revealed it had received requests and policing orders under the *Criminal Investigation Act 2006* to produce SafeWA data to the WA Police Force. An order is issued by a Justice of the Peace upon application by the WA Police Force.

By June 2021, WA Health had received 6 orders, issued by Justices of the Peace, from the WA Police Force to produce SafeWA information for policing purposes and 1 request which did not result in a formal order[4]. WA Health ultimately provided access in response to 3 of the orders before the State Government passed urgent legislation[5] to prevent this from occurring in the future and to align with the publicly stated purpose of the data only being used for COVID-19 contact tracing.

We were continuing our audit enquiries around these orders when on 16 June 2021, the State Government publicly announced the provision of SafeWA information to the WA Police Force, and that they had introduced new legislation into Parliament to stop future access to SafeWA information for purposes other than contact tracing.

A briefing note tabled in the Parliament (Appendix 2) on 17 June 2021 during passage of the Protection of Information Bill 2021 shows that the WA Police Force were granted orders to access SafeWA data for matters under investigation including:

- an assault that resulted in a laceration to the lip
- a stabbing
- a murder investigation
- a potential quarantine breach.

The following table provides further information on the data request and orders by the WA Police Force:

No	Date of request and orders	Data provided / not provided	Additional information
1	14 December 2020	Data provided	
2	24 December 2020	Data provided	
3	24 February 2021	Data not provided	Request did not result in a formal order to produce data

[4] Under the *Criminal Investigation Act 2006*, a police officer may apply for an order to produce (OTP) a business record to be issued by a Justice of the Peace.

[5] *Protection of Information (Entry Registration Information Relating to COVID-19 and Other Infectious Diseases) Act 2021*

No	Date of request and orders	Data provided / not provided	Additional information
4	10 March 2021	Data provided	
5	1 April 2021	Data not provided	Withheld pending outcome of the Protection of Information Bill 2021
6	7 May 2021	Data not provided	Withheld pending outcome of the Protection of Information Bill 2021
7	27 May 2021	Data not provided	Invalid order / incomplete form

Source: OAG using WA Health and WA Police Force information

Table 1: WA Police Force request and orders to access SafeWA data

The *SafeWA Privacy Policy*, which users are required to agree to, prior to using the application, sets out how WA Health collects, processes, holds, discloses and uses personal information of people who access and use the SafeWA mobile application. It states that information on individuals may be disclosed to other entities such as law enforcement, courts, tribunals or other relevant entities.

During the audit we also became aware that WA Health uses information from a variety of sources including SafeWA as part of its contact tracing efforts. However, WA Health has not provided enough information to the community about other personal information it accesses to assist its contact tracing efforts. A search of publicly available information on State government websites and media sites revealed little about WA Health's use of personal information from flight manifests, Transperth's SmartRider public transport cards, WA Police Force G2G PASS declaration information and CCTV footage (Figure 2) as part of its contact tracing efforts. Improved transparency around the government's use of personal information would help build trust in the public health contact tracing process.

The extent to which the new legislation will restrict access to other contact tracing information in PHOCUS, such as SmartRider data and CCTV footage, for policing or other purposes has not been considered as part of this audit but may be examined in our next report into PHOCUS.

The Mothership contact tracing application has security weaknesses

The Mothership front-end web application, used by limited WA Health contact tracers and GenVis helpdesk staff to query SafeWA data, did not have effective controls in place to prevent unauthorised access. We identified the following weaknesses:

- **Weak password policy** – Mothership's password policy did not align with the user access and password standard that applies to WA Health's information and communication technology (ICT) systems. The standard requires all users with access to any WA Health system or application to maintain a unique and strong password. The Mothership allowed users to set a weak password, which increased the risk of user account compromise and unauthorised access to SafeWA data. WA Health advised us that the Mothership application now requires strong passwords.
- **Inconsistent use of multi-factor authentication** – WA Health's contact tracing team could access Mothership without multi-factor authentication (MFA) using only a valid username and password. MFA provides an additional layer of security to protect systems from attackers, who use readily available tools to compromise systems that rely on single-factor authentication, such as the use of usernames and passwords alone. This further increases the risk of unauthorised access to SafeWA data. We note that GenVis enforced MFA for their technical support staff. WA Health advised us that MFA has now been enforced for contact tracers.

- **Missing security headers** – Mothership was missing common security headers such as HTTP[6] Strict Transport Security and Content Security Policy. Security headers are a technical control to prevent a number of web-based attacks. Without appropriate security headers in place, Mothership is vulnerable to attacks, such as person-in-the-middle[7], cross-site scripting[8] and clickjacking[9]. Security headers are relatively simple controls to improve the security of web applications. WA Health informed us that all 3 security headers have now been implemented.

Phone number validation process had weaknesses

Prior to going live, WA Health identified that SafeWA registration could be completed with an incorrect number or someone else's phone number. This was because SafeWA did not fully verify a user's phone number during the registration process. Due to the timing of SafeWA development and WA Health's need to balance risk with implementation, this issue was only partially resolved prior to going live. The remaining weaknesses could be exploited to register fake accounts and check-ins. This is due to SafeWA issuing a valid token prior to phone number verification. This could compromise the integrity of SafeWA data and impact WA Health's contact tracing efforts. WA Health informed us that the remaining issue was resolved in February 2021.

SafeWA information is stored in Australia but WA Health does not manage the encryption keys

We found that SafeWA information is hosted in the AWS Sydney cloud. While the provisions of the contract between WA Health and GenVis require that SafeWA data must not be transferred, stored or processed outside Australia, WA Health and GenVis can only request, not enforce, this on the cloud provider.

SafeWA information is encrypted[10] to prevent unauthorised access. WA Health uses provider managed encryption keys for SafeWA, which are stored in the AWS database, instead of self-managed keys where the cloud provider has no visibility or access to them. WA Health advised us that the current solution is required so that AWS can access keys through software to perform platform maintenance and support the vendor with technical issues. Although the likelihood is low, the cloud provider could be required to disclose SafeWA information to overseas authorities as it is subject to those laws. This is usually a standard clause in global cloud provider contracts.

There are situations where it is prudent to use dedicated customer managed encryption keys.

SafeWA access logs are destroyed after 28 days

SafeWA access logs, which could play a major role in detecting unauthorised access in the event of a data breach, are deleted 28 days after the event that triggered them. This is contrary to WA Health's logging and monitoring standard[11], which requires retention for at least 7 years and where possible, for the lifecycle of the system. The 28 day retention of access logs is insufficient for WA Health to effectively monitor if user access to SafeWA data

[6] HTTP – hypertext transfer protocol.

[7] In a person-in-the-middle attack, the attacker can secretly read or alter communication between two parties.

[8] Cross-site scripting refers to an attack that injects malicious code into a trusted website.

[9] Clickjacking occurs when the attacker tricks a user into clicking a link by either hiding it or disguising it as something else on the web page.

[10] Encryption makes information and data unreadable to those who do not have the secret code (decryption key).

[11] Department of Health (2021). *Logging and Monitoring Standard*.

is appropriate and lawful. WA Health informed us that it immediately addressed the log retention issue when we notified them.

Of further concern, WA Health does not monitor SafeWA access logs to identify unauthorised or inappropriate access to SafeWA information. Monitoring of logs is a detective control to determine who is accessing data, how often and if this access is appropriate.

The SafeWA system deletes digital check-in information from the database after 28 days. WA Health retains information backups to ensure availability in case of a disaster for another month, so check-in data collected through SafeWA is stored for about 56 days. WA Health informed us that backups would only be used in the event of complete data loss for a specified period within the 28 days, and since the launch of SafeWA there has not been a need for data to be restored.

SafeWA change management process required improvement

Generally, WA Health has managed changes to SafeWA well. However, GenVis could change SafeWA's server-side code without WA Health's knowledge. We identified an incident on 29 January 2021 where GenVis made a change (patch release) to SafeWA that WA Health only became aware of when users reported an outage to the application, which lasted for 1 hour and 42 minutes. Without effective change management processes, changes made to SafeWA may not be adequately recorded, authorised and tested. This may compromise the integrity and availability of SafeWA.

WA Health identified this issue and improved the change management process in response to the incident prior to our audit. However, we note that at the time of our audit the SafeWA contract did not stipulate penalties for unauthorised changes to the application made by GenVis. Penalties can deter vendors from making unauthorised changes, in-turn improving the integrity and availability of the system.

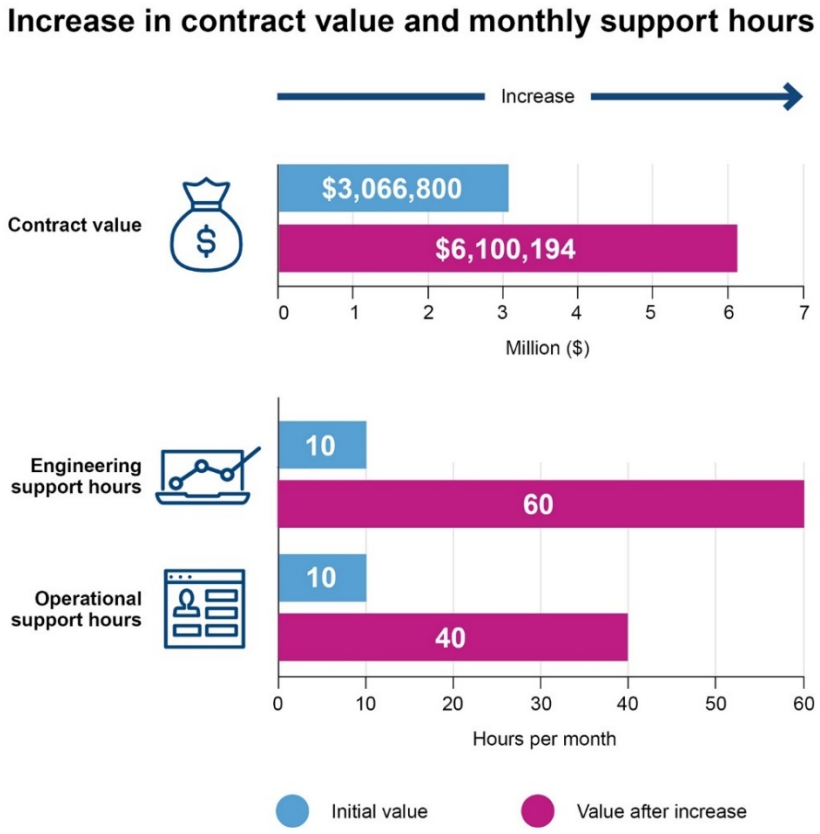
SafeWA vendor contract has continued to evolve

WA Health advised us that it negotiated and developed the vendor contract in an expedited timeline of 2 weeks. As a result, the contract required ongoing management to address a number of unknowns in relation to the State's strategy on the use of SafeWA, which were still in development at the time.

WA Health identified the initial value of the SafeWA contract was insufficient to meet the costs of the full contract term, and as the contact registration policy expanded. A significant increase in the contract value was required (Figure 3 and Appendix 1) to account for improvements and resource costs. The following timeline illustrates the evolving SafeWA contract and increase in total value:

- 18 November 2020 – the SafeWA contract between WA Health and GenVis came into effect with a total value of $3,066,800. The initial contract was signed for 1 year with 2 one-year extension options.
- 18 January 2021 – WA Health approved an additional $1,021,721 to cover enhancements. WA Health advised us that a large proportion of this amount was for Health Support Services' resources and SMS costs which were not included in the initial budget due to the urgency of the project. WA Health did not include the increase in the vendor contract until 4 months later. GenVis continued to support SafeWA in good faith.
- 29 January 2021 – a significant increase in GenVis and cloud resources was required to support SafeWA following the expansion of businesses and venues required to use a mandatory contact register, such as takeaway food and beverage services and visitors to public and private hospitals.

- 12 May 2021 – a contract management plan for the SafeWA contract was endorsed by Health Support Services.
- 1 June 2021 – WA Health formally endorsed a contract variation. The variation included an increase in monthly engineering support (from 10 to 60 hours) and operational and account support (from 10 to 40 hours). As a result, including the funding increase from 18 January 2021, the total contract value increased from $3,066,800 to $6,100,194 over 3 years.



Source: OAG using WA Health information

Figure 3: Increase in contract value and monthly hours November 2020 to 1 June 2021

Recommendations

WA Health should:

1. ensure that SafeWA information is used only for stated COVID-19 public health contact tracing purposes

   Entity response: Supported. The Department of Health will continue to collect and use SafeWA data in accordance with the SafeWA Privacy Policy and Terms of Use and relevant legislative requirements.

   Implementation timeframe: This recommendation has been implemented since 22 June 2021 (the date the Act came into operation).

2. ensure the confidentiality and integrity of SafeWA and its information by addressing the following areas:

   a. continue to ensure that access management controls are effective

   b. continue to ensure that weaknesses are identified and addressed timely

   c. continue to monitor the appropriateness of the current key management model

   d. continue to ensure that log retention is appropriate and implement processes to monitor access to SafeWA data.

   Entity response: Accepted. Activities by Health Support Services will be ongoing.

   Implementation timeframe: Ongoing.

3. continue to manage the vendor contract to address emerging risks.

   Entity response: Accepted. Health Support Services will continue to manage the vendor contract accordingly.

   Implementation timeframe: Ongoing.

Response from WA Health

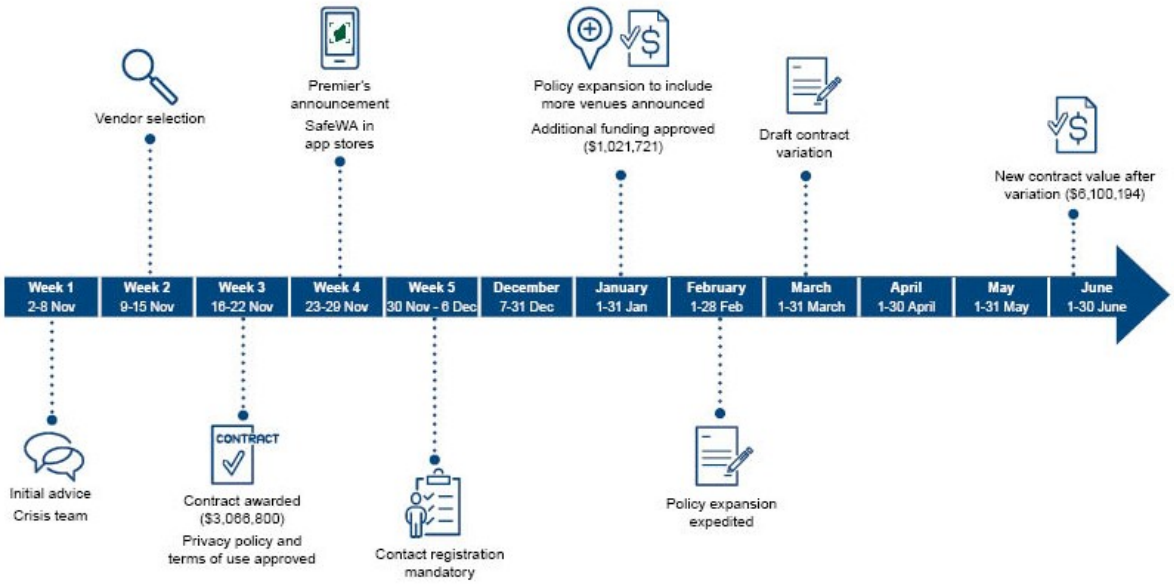
WA Health accepts the report, findings and recommendations.

In response to the COVID-19 pandemic significant work was undertaken by Department of Health employees and Health Support Services to stand up the SafeWA app to support the essential work of contact tracing. The SafeWA app was efficiently and effectively developed in a short time period and has continued to evolve to respond to the State Government's strategy for managing WA's COVID-19 response.

Health Support Services (WA Health's ICT Service provider) has already completed a number of activities to address the audit findings as acknowledged in the Report and will continue to monitor and address these as recommended. Health Support Services is committed to ensuring the SafeWA application continues to operate effectively, with the necessary governance and controls in place to ensure the security and integrity of the data it contains. In relation to the SafeWA data backup processes in the event of a disaster recovery event, HSS has confirmed that the backup data is stored in a separate encrypted database, and if backup restoration was required, any data older than 28 days is automatically deleted as part of the predefined restoration procedure. Therefore check in data greater than 28 days old is not accessible.

While acknowledging the finding that SafeWA information was released for purposes other than contact tracing, it must be noted that the Department of Health was legally required to comply with Orders to Produce a Business Record issued pursuant to section 53 of the *Criminal Investigation Act 2006* seeking access to SafeWA data. In response to the orders to produce, the Department of Health raised concerns with WA Police regarding the legal requirement to provide SafeWA data. Prior to the conclusion of this audit, the *Protection of Information (Entry Registration Information Relating to COVID-19 and Other Infectious Diseases) Act 2021* (the Act) was introduced into parliament on 15 June 2021 and was assented to on 21 June 2021. This Act provides that entry registration information, including information collected through SafeWA, can only be used for contact tracing and some other specified purposes.

Appendix 1: SafeWA development timeline



Source: OAG using WA Health information

Appendix 2: Legislative Council Question without Notice 284 – SafeWA App – Access – Police investigations (Tabled in Parliament)

The following paper was tabled in the Legislative Council.[12]

FOR INFORMATION REF: 4-200064

BRIEFING NOTE

ISSUE
Use of the SafeWA App data for police investigations.

KEY MESSAGES

- The Western Australia Police Force (WAPOL) has requested to use SafeWA data as part of police investigations unrelated to COVID-19.
- The development of the SafeWA app was on the proviso that data would only be used for public health contact tracing purposes.
- The SafeWA app relies on the willingness of the public to use it when visiting public places.
- There is a risk that public confidence in the app could be lost if was to be regularly used for other purposes other than contract tracing.

BACKGROUND

- In November 2020, it was announced that specific businesses were required to maintain contact registers. One way to record details of individuals for contact tracing purposes was through the SafeWA app. The media statement at this time stated that the data collected 'will only be used for necessary COVID-19 contact tracing, should the Department of Health require it.'
- The SafeWA Privacy Policy does allow for the disclosure of information to 'those to whom WA Health must (by law) disclose your information (e.g. a court or tribunal, or another government body).'
- WAPOL has requested to use SafeWA data to investigate police matters. This has included in relation to a laceration of a lip, a stabbing, a murder, and a potential breach of quarantine.
- An order to produce a business record requires a police officer to apply to a Justice of the Peace to request the information.
- The use of SafeWA for police investigations may undermine public confidence in the use of the system. For the SafeWA app to be useful, from a contact tracing point of view, it relies on a high level of use from the community.
- The Department of Health is concerned that the public will be less inclined to use the SafeWA app if it was to be used for anything beyond its original purpose.
- The federal government has stated publicly that they have not allowed police to use the COVIDSafe app for non-COVID-19 related purposes.

CURRENT SITUATION

- WAPOL has issued an order to produce a business record to WA Health by 31 March 2021 for SafeWA app data in relation to a police investigation.
- In response to this, and previous requests, the Director General of the Department of Health wrote to the Commissioner of Police on 12 March 2021 (attachment 1) expressing concern with the requests to use data which may result in a loss of public confidence.
- The Commissioner of Police provided a reply to this correspondence on 19 March 2021 (attachment 2)

RECOMMENDATION/ACTION
Minister to note that SafeWA is being used on specific occasions for purposes other than contact tracing.

1

[12] Parliament of Western Australia, Tabled Paper No. 290, Legislative Council debates (Hansard), 17 June 2021, p. 1633.

FOR INFORMATION REF: 4-200064

Prepared by: Dr Ben Scalley
OPERATIONS COORDINATOR
PUBLIC HEALTH EMERGENCY OPERATIONS CENTRE

Date: 25 March 2021

Sign off: Dr Andrew Robertson
CHIEF HEALTH OFFICER

30/3/21

Sign off: Dr D J Russell-Weisz
DIRECTOR GENERAL

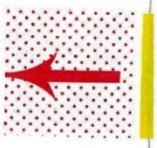
Approved ☐

Not Approved ☐

Noted ☒

Comments:

Signed _____ **Date** 31/3/2021
MINISTER FOR HEALTH



Att:
1. *Copy of letter from Director General Department of Health to the Commissioner of Police on 12 March 2021.*
2. *Copy of letter from Commissioner of Police to Director General Department of Health on 19 March 2021.*

2

Government of **Western Australia**
Department of **Health**

Our Ref: LOG21/401

Mr Chris Dawson
Commissioner of Police
Western Australia Police Force

Via email: [redacted]

Dear Commissioner ~~Dawson~~ Chris

USE OF SAFEWA APPLICATION FOR PURPOSES OTHER THAN CONTACT TRACING

As per our recent discussions, I write regarding the recent requests from the Western Australia Police Force (WAPOL) to use the SafeWA application for investigations. While I am advised that this use is permitted legally, I am concerned that its use for this purpose may undermine public confidence in using the application. The SafeWA application, unlike some other data sources, relies heavily on the public using the application voluntarily. A loss of public confidence could significantly undermine its use for contact tracing purposes.

While the terms and conditions do allow for other uses, the public messaging has not reflected this. For example, the media release to announce the SafeWA application last year included that '*records would only be used for the purpose of COVID-19 contact tracing, should it be required, and will only be kept for 28 days and not used for any other purpose.*'

To date, WAPOL have requested information regarding patrons entering venues related to an assault that resulted in a laceration to a lip, a stabbing, a murder investigation, and a potential quarantine breach.

I appreciate efforts by WAPOL thus far to centralise applications and to further consider the need for some applications for this data. It is important both agencies work together further to maintain public confidence in this system, and I think we need clarity from WAPOL in relation to any future requests.

Yours sincerely

Dr D J Russell-Weisz
DIRECTOR GENERAL

12 March 2021

cc *Dr Andy Robertson, Chief Health Officer, Department of Health*

189 Royal Street East Perth Western Australia 6004
Telephone (08) 9222 4222 TTY 133 677
PO Box 8172 Perth Business Centre Western Australia 6849
ABN 28 684 750 332
www.health.wa.gov.au

WESTERN AUSTRALIA POLICE FORCE

OFFICE OF COMMISSIONER OF POLICE

Your Ref: LOG21/401
Our Ref: fA1873104
Inquiries: [redacted]

POLICE HEADQUARTERS
6TH FLOOR
2 ADELAIDE TERRACE, EAST PERTH
WESTERN AUSTRALIA 6004
TELEPHONE: (08) 9222 1474

Dr Russell-Weisz
Director General, Health
Department of Health
PO Box 8172
PERTH BUSINESS CENTRE WA 6849

BY EMAIL ONLY: [redacted]

Dear Dr Russell-Weisz

RELEASE OF INFORMATION OBTAINED DURING THE COVID-19 STATE OF EMERGENCY BY THE DEPARTMENT OF HEALTH

Thank you for your letter dated 12 March 2021.

You have raised concerns with me on behalf of the Department of Health (DoH) around the release of information obtained by the DoH for contact tracing purposes. Those concerns are that the use of personal information for purposes other than emergency management objectives, may undermine public confidence and cooperation.

I have considered this against the importance of solving serious crime in our community, for which this information may be required to identify or convict a suspect. The State Solicitors Office (SSO) has provided advice indicating that these records can be obtained under appropriate legal parameters. In your correspondence you have also acknowledged that stored information may be obtained pursuant to the *Criminal Investigation Act 2006* (WA) (CIA), through the issuance of an Order to Produce (business records) (OTP).

Generally, the information sought will be stored on the DoH administrated application, SafeWA, or hard copy at individual business premises. I also note the SafeWA Privacy Policy, in part, advises each user, before being permitted to register for the application, that their information may be used by those to whom WA Health must (by law) disclose their information.

Whilst you have accurately described the public messaging around access to the data, the SSO advice observes that the CIA makes it an offence to fail to obey an OTP without reasonable excuse. As such the information must be provided on receipt of a OTP

To provide some assurance to you, as well as the required scrutiny by a Justice of the Peace as to the veracity of the grounds to issue an OTP, I have instructed my State Emergency

Coordinator's Directorate (SECD) to issue Operational Guidance to officers as to the process for considering SafeWA information for an investigation. I have required for a senior officer at the SECD to assess each request by an investigator to access stored information, prior to obtaining an OTP to ensure that this information is only accessed where it is defensible and required. This will ensure every request is justified and necessary and is specific to a serious crime. I envisage relatively low numbers of requests.

I would be happy to arrange a presentation from the SECD to outline the assurance process to your team responsible for information provision if this is of assistance. I trust this provides you with the clarity you seek in relation to the measures WA Police has implemented in this matter.

Yours sincerely

CHRIS DAWSON
COMMISSIONER OF POLICE
STATE EMERGENCY COORDINATOR

19 March 2021

Auditor General's 2021-22 reports

Number	Title	Date tabled
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia