VAGO

Victorian Auditor-General's Office

Security of Patients' Hospital Data

May 2019

Independent assurance report to Parliament
2018–19: 23

VAGO

Victorian Auditor-General's Office

Security of Patients' Hospital Data

Independent assurance report to Parliament

Ordered to be published

VICTORIAN GOVERNMENT PRINTER
May 2019

PP No 30, Session 2018–19

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 99% recycled content.

ISBN 978 1 925678 47 5

VAGO

Victorian Auditor-General's Office

The Hon Shaun Leane MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Colin Brooks MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report *Security of Patients' Hospital Data*.

Yours faithfully

Andrew Greaves
Auditor-General

29 May 2019

Contents

Acronyms

ASD	Australian Signals Directorate
BH	Barwon Health
DDOS	distributed denial of service
DHHS	Department of Health and Human Services
EMR	electronic medical record
HTS	Health Technology Solutions
ICT	information and communications technology
ITIL	Information Technology Infrastructure Library
MFA	multi-factor authentication
NHS	National Health Service (United Kingdom)
NIST	National Institute of Standards and Technology (United States)
OVIC	Office of the Victorian Information Commissioner
PDPA	*Privacy and Data Protection Act 2014* (Vic)
RCH	Royal Children's Hospital
RHA	Rural Health Alliance
RVEEH	Royal Victorian Eye and Ear Hospital
SLA	service level agreement
VAGO	Victorian Auditor-General's Office
VPDSS	*Victorian Protective Data Security Standards*
WAN	wide area network

Audit overview

Public hospitals collect, generate, and use a wide range of patient data—from personal details such as names and addresses, to clinical information such as diagnostic notes and test results.

Public hospitals increasingly use information and communications technology (ICT) to deliver healthcare, and to capture and store patient information. Digital records give clinicians easy access to their patients' information at the point of care and allow clinicians to quickly share information and results, with the aim of avoiding duplication and medical errors.

While digital records can improve patient care, a cybersecurity breach could alter or delete patients' personal data or permit unauthorised access to this data. A breach could also disable health services' ICT systems and prevent staff from accessing patient information.

Health services' security measures protect their ICT systems and the infrastructure used to store patient data. However, human action—either unintentional or malicious—can undermine even the most sophisticated security controls. To manage the security risk, health services need a culture of security awareness, with their staff trained to identify and respond effectively to data security risks.

Within DHHS, the **Digital Health branch** supports health services to implement clinical ICT projects and develops sector-wide standards and guidance.

HTS is a separate business unit in DHHS that provides optional ICT services to health services, including systems for clinical information and patient administration.

In this audit, we assessed whether health services are taking effective steps to protect patient data. We audited Barwon Health (BH), the Royal Children's Hospital (RCH), and the Royal Victorian Eye and Ear Hospital (RVEEH). We also examined how two different areas of the Department of Health and Human Services (DHHS) are supporting health services: the Digital Health branch and Health Technology Solutions (HTS).

Conclusion

Victoria's public health system is highly vulnerable to the kind of cyberattacks recently experienced by the National Health Service (NHS) in England, in Singapore, and at a Melbourne-based cardiology provider, which resulted in stolen or unusable patient data and disrupted hospital services.

Phishing is a social engineering technique where an attacker tricks people into providing sensitive information—such as usernames, passwords and credit card details—by disguising an email as from a trustworthy entity.

There are key weaknesses in health services' physical security, and in their logical security, which covers password management and other user access controls. Staff awareness of data security is low, which increases the likelihood of success of social engineering techniques such as phishing or tailgating into corporate areas where ICT infrastructure and servers may be located.

We exploited these weaknesses in all four audited agencies and accessed patient data to demonstrate the significant and present risk to the security of patient data and hospital services.

The audited health services are not proactive enough, and do not take a whole-of-hospital approach to security that recognises that protecting patient data is not just a task for their IT staff.

DHHS's Digital Health branch has filled an important gap in the sector by developing common cybersecurity standards and acting as the central point for advice and support. While Digital Health has developed a clear roadmap to improve security across the sector, health services have not fully implemented the security measures necessary to protect patient data.

HTS has not fully implemented Digital Health's cybersecurity controls itself, and shares many of the same security weaknesses as health services. This is a risk to the sector because HTS hosts the clinical and patient administration applications that are used by 52 of the 85 Victorian health services (61 per cent).

Rural Health Alliances are groups of small regional and rural health services that deliver core ICT services to their members, governed by a joint-venture agreement.

While HTS and the audited health services outsource key parts of their ICT operations to third-party vendors or Rural Health Alliances (RHA), they remain accountable for the security of their patient data. HTS has established processes to monitor vendor performance; however, it needs to ensure that its main vendor complies with required security controls within an agreed timeframe. The three audited health services are not fully aware of whether their service providers have the necessary security controls. Due to the sector's reliance on third-party vendors, health services need to actively monitor vendor performance to ensure that patient data is safe.

Findings

Cybersecurity in the Victorian public health sector

Digital Health

DHHS's Digital Health branch supports improved cybersecurity in the sector by developing guidance materials, running awareness and training sessions, and funding ICT infrastructure upgrades. It has also developed a set of 72 baseline cybersecurity controls for health services to improve the maturity of health services' practices. Prior to Digital Health's cybersecurity program, there were significant gaps and little consistency in how health services managed risks to patient data.

Digital Health has proactively supported health services to improve their cybersecurity by leading joint procurement processes for advanced cybersecurity tools. This has led to cost savings for health services and greater consistency in how health services detect and respond to cyber incidents.

Cybersecurity controls

While Digital Health has set a better practice standard for health services to follow, no Victorian public health service has fully implemented all 72 controls. The sector collectively has implemented 62 per cent of the 38 foundational cybersecurity controls. The audited agencies have implemented 57 per cent of the foundational controls. The audited health services advise that key barriers to implementing the controls are a lack of dedicated funding for cybersecurity projects and limited staff availability.

Digital Health has assessed the risk profile of each health service, based on the number of controls implemented. Four out of the seven hospitals that DHHS recently assessed as ‘high risk’ have not improved their compliance with the controls since Digital Health first introduced them in March 2017. Six Victorian health services have not implemented any further controls since those they applied when Digital Health first introduced the controls.

Health services use **biomedical devices** to treat, monitor and diagnose patients. Increasingly, health services connect biomedical devices—such as infusion pumps and heart monitors—to their ICT systems and the internet, making them vulnerable to cyberattacks.

While DHHS sets targets for individual health services based on their circumstances, there are no penalties for non-compliance. It is vital that health services take a proactive approach and implement the controls, as each health service is responsible for the security of their patient data and ICT systems.

As the digital maturity of health services continues to improve there is scope for Digital Health to extend the 72 controls to include additional measures. Digital Health has advised that it plans to review the controls with a view to expanding them to cover other key risk areas, such as biomedical device security.

Effectiveness of data security in hospitals

All the audited health services need to do more to protect patient data. We identified key weaknesses in data security practices, including inadequate user access controls, weak passwords, and poor system and network monitoring.

We also found that health services do not have appropriate governance and policy frameworks to support data security. While all the audited health services have completed security testing and audits in the past, none have a clear policy that outlines when and how they will test the effectiveness of their security controls.

ICT security

Computer **ports** can be both physical and virtual and connect different devices within a computer network. Virtual network ports are vulnerable to internet attackers who search for ports with poor security that they can use to enter a network.

Network segmentation is the practice of splitting up a computer network into different segments. This can help prevent problems—such as a virus or attack—spreading to the entire network.

ICT security is fundamental to the ability of health services to protect patient data. We identified common weaknesses across all four audited agencies, such as insufficient port security, weak user passwords and limited network segmentation. One audited health service has started work to improve segmentation and network access controls.

These weaknesses limit the ability of audited agencies to effectively identify, detect, prevent and respond to potential data security incidents.

We also found deficiencies in how health services manage user access to digital records, including:

- unused and terminated employee accounts still enabled
- failure to keep user access forms as proof that users have had their access approved
- a lack of any formal, regular user access review to ensure only staff who need access have it.

These deficiencies mean that agencies cannot be sure that only authorised staff access patient records.

An **administrator account** is a user account that can make changes that impact other users. ICT staff use administrator accounts to update software, access all files, and make changes to other staff accounts.

We found staff user accounts at all audited agencies with weak passwords, which were accessible using basic hacking tools. We successfully accessed administrator accounts, which are a key target for attackers because they give ICT staff access to all system files. We also found that health services rarely used multi-factor authentication (MFA), even for ICT staff and administrator accounts.

We identified examples where audited agencies were still using default account names and passwords on key devices, including servers. Default account names and passwords are set by manufacturers when they first produce a device and are easy to find on the internet. In one audited health service, we accessed patient data in the hospital because the third-party system had a default account name and password.

Personnel security

ICT controls are policies, procedures and actions that an organisation can use to protect its ICT systems and data.

Staff behaviour is vital to effective data security because staff action can undermine even the best ICT controls. Health services are vulnerable to social engineering techniques that exploit staff because hospitals are busy, public places dedicated to caring for patients. Health services need to ensure that staff take basic action to protect patient data, such as alerting management to suspicious behaviour, locking computers, not clicking on suspicious links, keeping passwords secret, and protecting their security access passes. At all three audited health services we found digital patient data in unsecured shared files and hardcopy patient records left unattended near printers.

We found that only one audited health service provides mandatory cyber and data security training to all staff. Given that staff actions can undermine ICT and physical controls, it is vital that all staff—including clinical staff—can identify and manage the risks to patient data.

Physical security

Strong physical security measures are necessary because attackers can exploit weaknesses in physical security to bypass ICT controls and connect directly to hospital systems. While hospitals need to ensure that clinical staff can move freely to treat patients, in two of the audited agencies we gained access to areas used to store critical ICT infrastructure, such as servers. We also accessed restricted administration and corporate offices at all agencies. While hospitals are public places, all the audited health services need to improve the physical security of sensitive areas.

Health Technology Solutions and third-party vendors

It is common for health services to outsource key components of their ICT operations, such as the hosting of their patient data applications, either to HTS, an RHA, or a third-party vendor. Despite this, organisations remain accountable for protecting the security of patient data and need to assure themselves that vendors act appropriately.

Data security

HTS, a part of DHHS, has not fully implemented DHHS's cybersecurity controls, and has many of the same security weaknesses as health services. There is a particular need to improve staff awareness of common social engineering techniques. We found that although HTS's password policy aligns to better practice guidelines from the National Institute of Standards and Technology (NIST), its user accounts were still vulnerable to basic password cracking techniques. We also found that while HTS has conducted security testing of its systems in the past, it has not effectively remediated some issues identified by its testers.

Ninety-nine per cent of Victorian health services use one or more of HTS's applications. Although it is optional, 61 per cent of Victorian health services use at least one of the clinical and patient data applications that HTS hosts, while 32 other health services use the HTS-hosted financial management system. As the custodian of most of the sector's patient information, it is vital that DHHS takes steps to ensure that HTS implements the 72 controls.

Supporting health services

HTS operates a service desk to respond to issues that health services have with their patient and clinical data applications. We found that HTS meets its overall service restoration targets, and resolves 76 per cent of major incidents within three hours.

Vendor management

HTS monitors vendor performance and is taking steps to ensure that its main vendor understands its security responsibilities. However, none of the audited health services assure themselves that vendors are complying with security controls. At one of the audited health services—which is part of an RHA—we found confusion around which entity is responsible for different parts of data security.

Digital Health has recognised the security risks associated with third-party vendors and is in the process of conducting a risk-assessment of vendor security practices on behalf of the sector. However, both the audited health services and HTS need to actively manage their contracts with vendors to ensure they comply with required security measures.

Recommendations

We recommend that the Department of Health and Human Services:

1. continue to support the Digital Health cybersecurity program, and through Digital Health:
   - review and expand the 72 cybersecurity controls where appropriate
   - develop and deliver specialist cybersecurity training for health sector staff
   - assist the sector to jointly procure better practice cybersecurity tools (see Sections 2.2 and 2.3)
2. implement Digital Health's cybersecurity controls in Heath Technology Solutions (see Section 4.2)
3. ensure that Health Technology Solutions regularly tests its incident management process, including the capability of its third-party vendors, so it is prepared to respond to future cybersecurity incidents (see Section 4.3)
4. strengthen cooperation between Digital Health and Health Technology Solutions to ensure that both business units provide better practice support to the sector (see Section 4.2)
5. ensure that any new joint-venture agreements for Rural Health Alliances detail clear service level expectations and the security responsibilities of Rural Health Alliances and member health services (see Section 4.3).

We recommend that all Victorian health services:

6. expedite implementation of Digital Health's 72 cybersecurity controls (see Section 2.3)
7. develop and give effect to a policy that outlines when and how often they will test their information and communications technology, personnel, and physical security controls to ensure they are operating effectively to protect patient data (see Section 3.3)
8. deliver mandatory training in data security to all staff (see Section 3.5)
9. ensure that information and communications technology staff receive regular cybersecurity training (see Section 3.5)
10. align their information and communications technology password policies with Australian Signals Directorate guidelines (see Section 3.4)
11. ensure they identify and risk assess all information and communications technology assets (see Section 3.4)
12. implement multi-factor authentication for information and communications technology staff and administrator accounts (see Section 3.4)
13. conduct annual user access reviews to ensure that only relevant staff have access to digital patient data (see Section 3.4)
14. develop processes to monitor whether all third-party vendors are complying with data security requirements (see Section 4.3).

Responses to recommendations

We have consulted with DHHS, BH, RCH and RVEEH and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions or comments. We also provided a copy of the report to the Department of Premier and Cabinet.

The following is a summary of those responses. The full responses are included in Appendix A.

The audited health services and DHHS have accepted the recommendations from this audit. DHHS has provided an action plan that addresses each recommendation, and has advised it will work with health services to acquit recommendations six to 14.

1 Audit context

The *Health Records Act 2001* requires health services to protect patients' health information from unauthorised access, modification or disclosure. Health services have long-established information management practices to protect patient confidentiality and hardcopy information. With the growing use of digital technologies to treat patients and store data, health services need to introduce ICT security measures to manage the risk of cyberattacks on patient data systems.

1.1 Patient data

Patient data is the information that hospitals collect, generate and store about their patients. It includes a patient's personal information such as their name, address and date of birth, as well as clinical information including test results, clinicians' notes and prescribed medications. Clinicians use patient data in individual treatment, and researchers use aggregated and de-identified data.

An **application** is a computer software program designed to help users complete a specific task, for example word processing. In contrast, system software relates to the overall operation of a computer.

Hospitals use a variety of computer software, or applications, to store patient data, which means that health services may store information about the same patient across several applications within the same hospital. For example, a hospital may use separate applications to manage patient appointments across pharmacy, pathology, and diagnostic imaging. Typically, hospitals use two types of applications to store patient data:

- **Patient administration systems** are used for personal information and details about appointments.
- **Clinical applications** are used to record diagnostic notes and test results.

Many health services are working to phase out the use of hardcopy records, replacing them with electronic medical records (EMR). EMR systems store patients' personal and clinical information as part of a single record and allow clinicians to easily share and update records in real time.

Only one of the audited health services has an EMR system and no longer generates hardcopy records. The other two health services use multiple clinical and patient administration systems, in addition to maintaining hardcopy patient records.

1.2 Data security

The concepts of data security and privacy are closely linked. Where privacy relates to an individual's ability to control their personal information and how others use it, security refers to how organisations protect personal information. To protect the privacy of patients, hospitals need to ensure that only authorised people can access and use patient data. This protection includes managing how hospital staff access and use patient data, ensuring medical confidentiality, and preventing external parties from accessing patient data.

Victorian Protective Data Security Standards

The *Privacy and Data Protection Act 2014* (Vic) (PDPA) establishes the Victorian Protective Data Security Framework, which outlines the data security responsibilities of Victorian Government agencies. The PDPA sets out the *Victorian Protective Data Security Standards* (VPDSS), which provide criteria for the consistent application of security practices. These standards follow the Australian Government's *Protective Security Policy Framework*.

The VPDSS is designed to assist public sector agencies and other organisations to maintain the confidentiality, integrity and availability of their data. The Office of the Victorian Information Commissioner (OVIC) administers the VPDSS and recommends that agencies implement protective measures across five data security domains, as outlined in Figure 1A.

Figure 1A
Protective data security domains

Security domain	Description
Governance	Executive sponsorship of, and investment in, security management, utilising a risk-based approach.
Information	Protect information, regardless of media or format, across the information lifecycle from creation to disposal.
Personnel	Employ suitable people to access information and provide ongoing information security training.
Physical	Secure the physical environment to protect information by limiting access to facilities, servers, network devices, ICT equipment and media.
ICT	Implement secure ICT systems that process or store information.

Source: OVIC.

OVIC considers the domains crucial components in a comprehensive approach to data security. By maintaining the confidentiality, integrity and availability of information, organisations can ensure that access to information is limited to those authorised; that those authorised can access information reliably; and that information is accurate and trustworthy.

Privacy and data security in the health sector

The *Health Records Act 2001* (Vic) sets out Health Privacy Principles, which specifies health services' obligations for data security. Principle 4 states that a health service 'must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure'. Principle 9 covers transborder data flows and states that 'when health information travels outside Victoria, the holder has a responsibility to ensure that the privacy of the information is safeguarded'.

Under section 84 of the PDPA, health services do not need to comply with the VPDSS or its reporting obligations. The Health Privacy Principles broadly align with the core principles of the PDPA, but unlike the VPDSS they do not provide detailed guidance for how health services should apply the principles. Instead, DHHS has developed its own policies and standards to guide data security practices across the health sector.

Cybersecurity

With the increasing use of ICT applications and EMRs, health services need to protect patient data from security breaches or attacks. Cybersecurity is the practice of implementing security measures to protect ICT infrastructure, networks, and applications from unauthorised access, attack or theft. The area of cybersecurity is constantly evolving in response to new technologies and the changing techniques of cyber criminals or 'hackers'.

Within the health sector, cybersecurity measures aim to maintain ICT operations, protect patient data, and secure the internet-connected biomedical devices used in patient care. Cyberattacks have a range of possible impacts including:

- breach of patient privacy
- use of patient information for financial or identity fraud
- loss of hospital reputation
- corruption or loss of patient data
- unavailability of clinical applications or EMR systems
- damage to biomedical devices.

Figure 1B summarises some common cyberattack techniques.

Figure 1B
Common cyberattack and techniques

Type of attack	Description
Phishing	Emails that ask for sensitive information or encourage people to open malicious attachments or links to fake websites. Whaling is a phishing variant where an attacker masquerades as a senior executive via email.
Typo squatting	An external attacker purchases a website that has a name similar to a legitimate site. When someone makes a 'typo', such as typing .org instead of .com, it directs them to a site owned by the attacker with the aim of stealing personal information or infecting a user's device with malicious software.
Ransomware	Malicious software that renders data or systems unusable until the victim makes a payment.
Unauthorised system access	An attacker accesses a system by creating, stealing or exploiting user credentials (passwords and logins) to disrupt an organisation or exfiltrate data.
Distributed denial of service (DDOS)	When multiple devices (often compromised computers) flood a system with requests for access preventing legitimate users from using the system. A denial of service attack is like a DDOS attack, except it involves the use of only one device to flood the target system.
Data breach	An intentional or unintentional release of bulk private information to an untrusted party, which can result in the use of information for financial gain.

Source: VAGO, based on information from the Australian Cyber Security Centre and DHHS.

1.3 DHHS strategies

DHHS is responsible for developing and delivering policies, programs and services that support and enhance the wellbeing of all Victorians. Within DHHS, the Digital Health branch is responsible for developing sector-wide ICT standards, programs and guidance. Since 2016–17, DHHS has managed several funding programs for ICT investment in the health sector. This includes one-off funding for clinical hardware and capital projects, and the Health Projects Fund, which is funded through DHHS's internal budget.

Digitising Health Strategy

In 2016, DHHS launched the *Digitising Health Strategy,* which is designed as a roadmap to assist health services to increase the use of ICT in patient care. One of its key focus areas is for health services to continue to replace paper-based clinical and administrative systems with EMR applications. The strategy recognises the need to build digital capability within each health service, and identifies critical success factors including workplace capability, information governance, and cybersecurity. The Victorian Government has also committed to the national *Digital Health Strategy*, which plans for all private, state and Commonwealth health services to be able to securely share patients' digital health records by 2022.

Victorian Public Health Sector Cybersecurity Uplift Strategy 2018–2021

One of the seven critical success factors in the *Digitising Health Strategy* is improving the ability of hospitals to respond to cybersecurity breaches. In May 2016, DHHS engaged external experts to conduct a maturity assessment of the Victorian public health services' cybersecurity. The assessment found that health services need to do more to defend against increasing cybersecurity threats. In response, DHHS established the Victorian Health Cybersecurity Working Group in October 2016, adopted the NIST framework, set 72 baseline controls for all health services, and commenced implementing the *Victorian Public Health Sector Cybersecurity Uplift Strategy 2018–2021* (Cybersecurity Uplift Strategy) to increase cybersecurity resilience across the health sector.

The Cybersecurity Uplift Strategy includes 72 controls that health services can use to protect their ICT systems, infrastructure, and patient data. The baseline controls are categorised using the five core cybersecurity areas promoted by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*:

- identify (11 controls)
- protect (40 controls)
- detect (10 controls)
- respond (five controls)
- recover (six controls).

As part of the Cybersecurity Uplift Strategy, health services should conduct bi-annual self-assessments against the 72 controls. Each health service also needs to develop and monitor a three-year action plan—updated annually—that details how they are working to implement the controls.

1.4 Agency responsibilities

Within DHHS, the Digital Health branch is responsible for developing sector-wide ICT standards, programs and guidance.

HTS is a business unit within DHHS that provides optional ICT business systems and services to Victorian health services, which includes clinical and patient administration applications, financial systems, service management functions, infrastructure and network architecture, and two data centres.

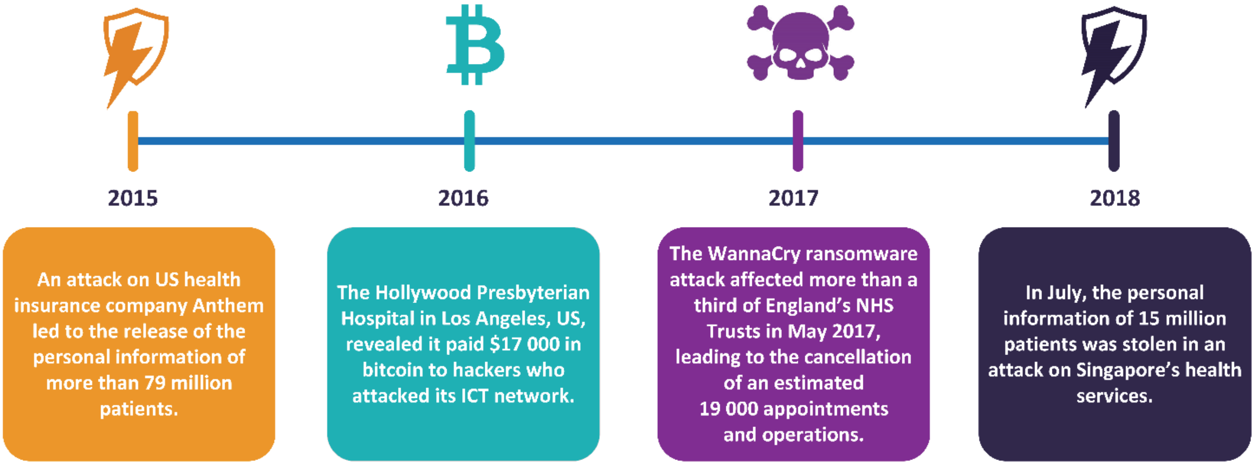
Health services and their boards are responsible for maintaining the security and accuracy of patient data. Health services make ICT decisions based on local needs and do not receive dedicated recurrent funding to invest in ICT technology and maintenance. Instead, capital funding is included in the activity-based funding model for health services. In addition, health services can bid for specific capital funding through DHHS funding programs or the state budget process.

1.5 Why this audit is important

Patient data is not only valuable to individuals and clinicians, but to cybercriminals who aim to commit identity fraud, sell or expose data, or disrupt hospital services. Cybersecurity incidents are increasing in scale and sophistication. A survey from the Australian Cyber Security Centre found that 86 per cent of their public and private member organisations faced an attempted attack during 2015–16.

In February 2019, a cardiology service provider located within a Melbourne private hospital experienced a ransomware attack. A cybercrime group gained access to the cardiology patient system, encrypted approximately 15 000 patient files, and demanded a ransom in exchange for a password to fix the data. Media reports indicated that the cardiology provider was unable to access some patient files for more than three weeks, and that patients arrived for appointments that had been deleted. Figure 1C highlights recent international cyberattacks in the health sector.

Figure 1C
International health sector attacks



2015

An attack on US health insurance company Anthem led to the release of the personal information of more than 79 million patients.

2016

The Hollywood Presbyterian Hospital in Los Angeles, US, revealed it paid $17 000 in bitcoin to hackers who attacked its ICT network.

2017

The WannaCry ransomware attack affected more than a third of England's NHS Trusts in May 2017, leading to the cancellation of an estimated 19 000 appointments and operations.

2018

In July, the personal information of 15 million patients was stolen in an attack on Singapore's health services.

Source: VAGO.

1.6 What this audit examined and how

This audit examined whether public health services' IT security policies, procedures, and practices effectively protect patient data. We focused on three health services: BH, RCH and RVEEH. The audit also examined whether two different areas of DHHS—the Digital Health branch and HTS—provided effective support to health services to identify and manage data security risks.

The methods for this audit included:

- examining documentation and data from the audited agencies and conducting interviews with relevant staff
- targeted testing of the controls governing access to patient information within the audited agencies
- scenario-based penetration testing conducted by ICT security experts to assess the effectiveness of health services' efforts to protect patient data.

We conducted our audit in accordance with section 15 of the *Audit Act 1994* and ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements related to assurance engagements. The cost of this audit was $501 000.

1.7 Report structure

The remainder of this report is structured as follows:

- Part 2 examines cybersecurity in the Victorian public health sector.
- Part 3 assesses the effectiveness of health services' efforts to protect patient data.
- Part 4 focuses on the way HTS supports health services and the security of third-party vendors.

2 Cybersecurity in the Victorian public health sector

While Victorian health services manage their ICT systems independently, cybersecurity is a common challenge. DHHS's Digital Health branch provides support to improve cybersecurity in the sector by developing guidance materials, running awareness and training sessions, and funding ICT infrastructure upgrades. It has also developed a set of 72 baseline cybersecurity controls for health services to implement by 2020–21 to improve the maturity of health services' practices.

2.1 Conclusion

Over the past three years, DHHS's Digital Health branch has completed an effective program of work to improve health services' ability to detect and respond to cyber threats. It has developed oversight of the security risks facing the health sector and targeted its support activities to address common weaknesses. Crucially, its 72 cybersecurity controls have established a consistent, sector-wide approach to data security. As health services continue to implement the controls, there is scope for Digital Health to review and expand the controls.

While Digital Health has set a clear roadmap for health services to follow, to date no health service has fully implemented the 72 controls. The audited health services advise that barriers to implementing the controls include a lack of dedicated cybersecurity staff and insufficient resources for ICT projects. While it may be challenging for health services to balance ICT security against clinical projects, implementing all the controls will provide health services with strong baseline protection against cybersecurity risks. Recent, local examples of cyberattacks in health services demonstrate the need for this work to occur.

2.2 Digital Health

DHHS's Digital Health branch—led by the Chief Digital Health Officer—works with Victoria's public health services to implement clinical ICT projects to improve patient care. The branch also performs assurance work on health services' technology and convenes several statewide working groups to support information sharing across the sector.

In early 2016, Digital Health identified cybersecurity as a key weakness in health services. It found wide variation in how health services managed data security and a low awareness of cyber risks. It also found that health services had limited staff capacity to implement security measures, with more than half of Victoria's health services lacking dedicated cybersecurity staff.

To address these weaknesses, Digital Health developed the Cybersecurity Uplift Strategy with the aim of improving cybersecurity knowledge and skills across the sector. The strategy has a regularly revised business plan that clearly links to DHHS's broader *Digital Health Strategy*. Digital Health has two full-time equivalent staff dedicated to supporting health services' cybersecurity. Other staff contribute to data security through broader projects to improve ICT operations, infrastructure, and disaster recovery.

Digital Health has no dedicated funding stream to support sector-wide cybersecurity initiatives. Digital Health administers a fund to refresh health services' clinical ICT infrastructure, and allocates this on a case-by-case basis. Digital Health has secured funding through the state budget process for capital projects to uplift cybersecurity maturity across the health sector. It received $11.9 million in 2017–18 and $12 million in 2018–19.

Sector support activities

Penetration testing examines ICT systems to identify and exploit weaknesses in a system. It aims to demonstrate the potential for a hacker or other unauthorised person to access a system and its data.

Digital Health's support activities have improved how individual health services manage data security and developed greater consistency and cooperation across the sector. The audited health services have advised that Digital Health's support activities are highly valued and have enabled health services to implement security measures or attend training that their health service could not otherwise have funded.

Digital Health has provided an extensive range of data security guidance and support to health services, including:

- cybersecurity awareness training
- mock cyber incident response exercises
- assisting health services to run security awareness campaigns for staff
- template policies on data security and training materials
- funding sector-wide penetration testing
- running phishing awareness campaigns
- assisting in remediation of cyber incidents
- guidance on common cyberattacks and updates on international incidents.

Previously, health services managed cyber incidents individually and did not always report issues to DHHS. As part of the Cybersecurity Uplift Strategy, Digital Health has developed an incident communication protocol that directs health services to report all suspected cyber incidents to DHHS. It also assists health services with cyber incident management and post-incident reviews on request. The communication protocol has allowed DHHS to coordinate advice and incident responses, which in some instances effectively prevented cyber threats from spreading by allowing health services to remediate issues. Digital Health also acts as the key point of contact between health services and key agencies, including the Department of Premier and Cabinet, Australian Signals Directorate (ASD), AusCERT, and the Australian Digital Health Agency.

Another mechanism for increasing cooperation and consistency has been Digital Health's monthly Cybersecurity Working Group, which brings together cybersecurity and ICT staff within health services to share their knowledge and develop skills. The audited health services advise that the working group is an important forum for staff to discuss how their health services are implementing the 72 controls and provide feedback to Digital Health on the kind of support they require.

Procurement

Digital Health has proactively supported health services to improve their cybersecurity by leading joint procurement processes for advanced cybersecurity tools. These procurement activities have led to greater consistency in the tools that health services use to detect and respond to cyberattacks, which has improved the overall resilience of the sector.

In 2017–18, Digital Health managed the procurement of a vulnerability management tool and a phishing solution. Digital Health is currently arranging the purchase of a security operations centre, which will improve the ability of health services to actively monitor their systems and networks. While it is not mandatory for health services to participate in Digital Health procurement activities, the overwhelming majority have done so due to cost savings and the ability to secure higher quality products as a group.

Digital Health is also in the process of developing a clinical-grade wide area network (WAN), which will provide secure telecommunications and internet services to health services. When health services shift their internet and internal networks to the WAN, Digital Health plans to procure security tools, such as a firewall, that will cover the whole sector and provide a baseline level of protection from cyber threats.

Future work

Digital Health has a clear plan to continue its cybersecurity program and is targeting its future work to address health services' common weaknesses. Key projects planned include developing advice on managing biomedical devices; establishing a group contract that allows health services to access specialist cybersecurity advice on an as-needed basis; and conducting a sector-wide risk assessment of the security practices used by third-party vendors, such as software suppliers. Digital Health also plans to continue to fund cybersecurity awareness and technical training for health services' ICT staff and assist health services to manage and review their incident response processes.

2.3 Cybersecurity controls

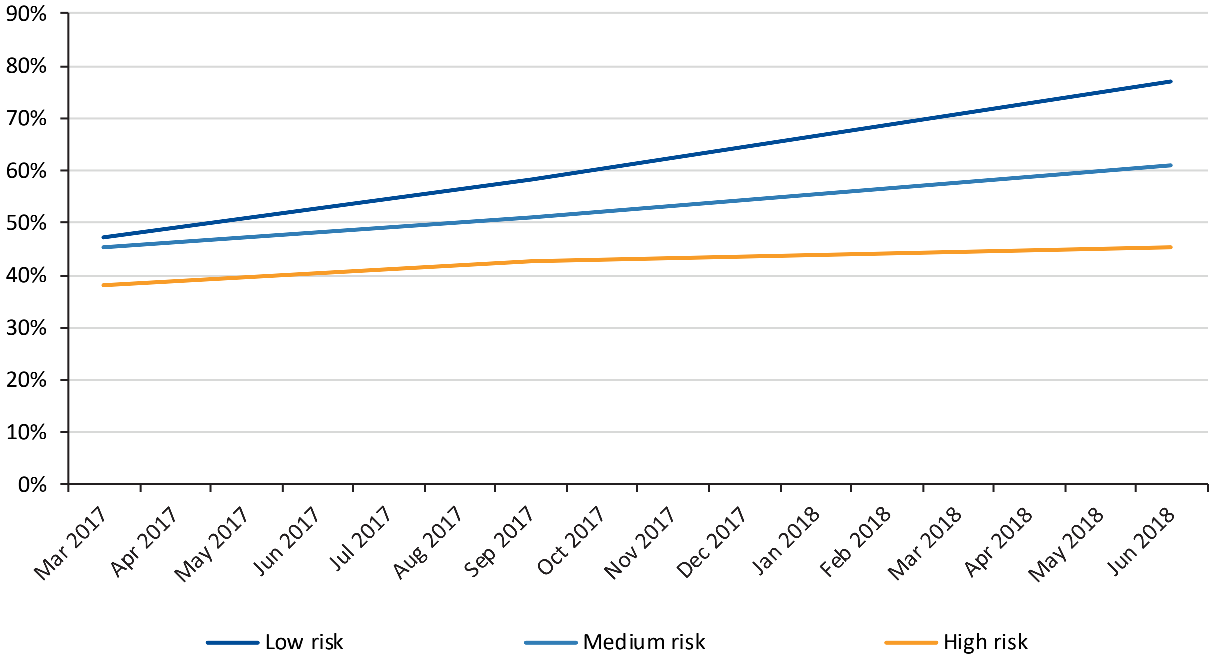
The key project in Digital Health's Cybersecurity Uplift Strategy has been developing and implementing a set of ICT controls to give the health sector a consistent, better practice approach to cybersecurity. Based on advice from an external consultant and internationally recognised security models such as NIST and the ASD Essential Eight, Digital Health developed the 72 cybersecurity controls outlined in Section 1.3.

The controls apply to all Victorian public health services, Dental Health Services Victoria, Ambulance Victoria and HTS. Digital Health requires health services to complete an annual self-assessment against the controls and a three-year action plan on how they plan to implement the controls by 2021. Given that the ICT maturity of health services varies widely, Digital Health sets each health service a target to comply with the controls based on a digital maturity assessment. The target number of controls to implement is based on the uptake of ICT services; a health service that has a higher uptake of ICT services requires a higher level of cyber maturity.

As at June 2018, Victorian health services have collectively implemented 62 per cent of the foundational controls. Digital Health categorises 38 of the 72 controls as 'foundational' controls designed to provide a baseline level of security. Digital Health expects health services with a higher uptake of ICT services to have implemented more controls than health services with less digital services.

Digital Health risk-assessed each health services' level of compliance with the controls, and categorised health services as low, medium, high or critical risk based on the potential consequences of non-compliance. Figure 2A outlines the progress that health services in each category have made towards implementing the controls. While health services in the 'low risk' category have made strong progress, four out of the seven hospitals in the 'high risk' category have not improved their compliance with the controls since Digital Health first introduced them in March 2017. Six Victorian health services have not made any progress in implementing the controls since their introduction.

Figure 2A
Average level of health services' compliance with foundational controls based on risk rating as at June 2018



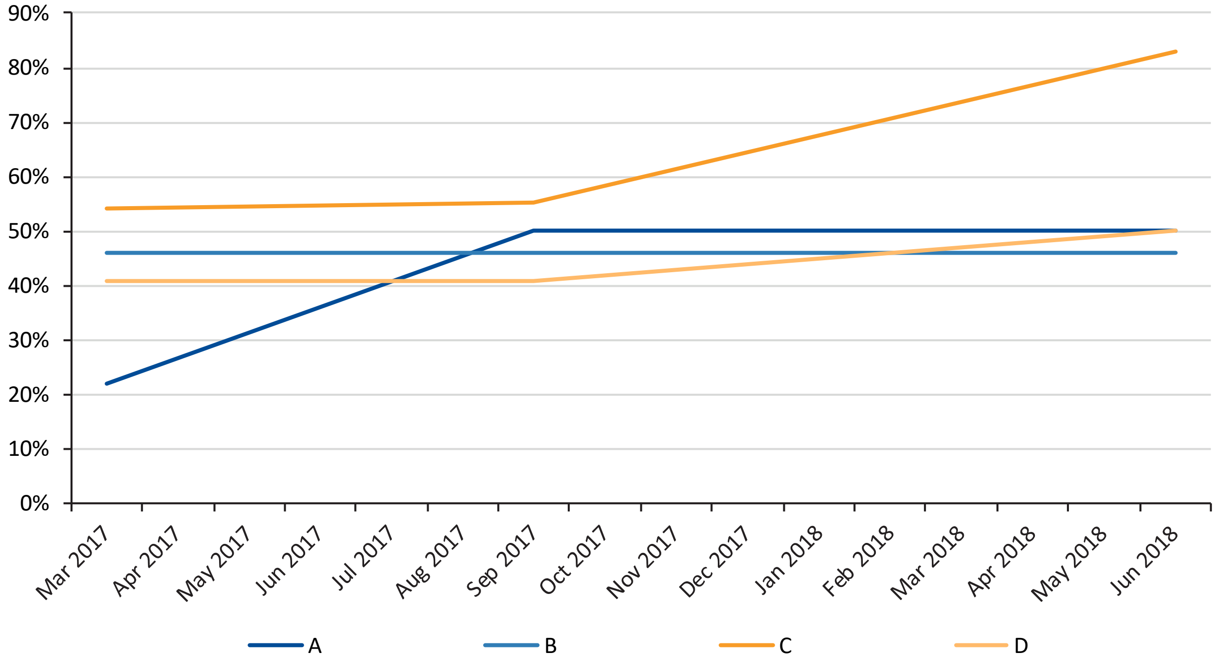
Note: Results include all Victorian health services, Ambulance Victoria, Dental Services Victoria, and HTS.

Note: Health services' individual risk rating may move between 'low risk', 'medium risk' and 'high risk' based on the number of controls implemented.

Source: VAGO, from DHHS data.

Figure 2B outlines the progress of the audited health services in implementing the controls. As at June 2018, one of the audited health services had implemented 83 per cent of the foundational controls. The three other audited health services have made minimal progress implementing the controls since March 2017.

Figure 2B
Audited agencies' progress implementing the controls from March 2017, September 2017 and June 2018



Note: Audited agencies include three health services and HTS, and have been de-identified above as A–D.
Source: VAGO, from DHHS data.

In their self-assessments, health services outline when they expect to implement each control and identify any barriers to their progress.

The audited health services advised that key issues are a lack of dedicated funding for cybersecurity projects above ICT operational costs and limited staff availability. Except for HTS—which is part of DHHS—none of the audited agencies have dedicated cybersecurity staff, and all advised that they need to complete work to implement the controls alongside day-to-day application and system support, and in the case of one health service, alongside the roll-out of a new patient data application. As health services continue to digitise, they may need to expand their IT teams to manage their increased cyber risks.

Aligning with better practice

Digital Health advised that they developed the 72 controls to align with a range of better practice standards, including NIST guidance, NHS guidance, and ASD's Essential Eight security mitigation strategies. While the controls do broadly align with these standards, they are a unique set of controls developed for the Victorian public health sector. This means that although Digital Health has tailored the controls to the needs of health services, they are not a publicly known standard that can be easily accessed and compared with other control systems. One audited health service suggested that this can make it difficult for their third-party vendors to understand and comply with their security needs. While Digital Health should increase public transparency around the controls, it is the responsibility of health services to ensure that their vendors understand their security responsibilities.

While our analysis confirms that the controls do align with the core elements of better practice, some Digital Health controls are less onerous than other standards. For example, Digital Health recommends patching operating systems within one month, whereas the ASD recommends applying patches within 48 hours for vulnerabilities that pose an extreme risk and within one month for moderate and low risk vulnerabilities. Other standards also emphasise that cybersecurity is only one part of effective data security and include controls that address other security domains such as information management and governance. While it is understandable that the 72 controls focus on cybersecurity—as it is a key weakness for some health services—health services need to better integrate their approaches to cybersecurity, information management and patient confidentiality.

Improving the 72 controls

While our audited health services strongly support the 72 controls, they advised that some of the controls do not have enough detail about how to implement them.

Further, because Digital Health relies on health services to self-report their compliance, it is difficult for them to understand whether they implement the controls to the same standard. Digital Health has recognised the limitations of self-reporting and plans to commission an independent assessment of controls compliance in 2018–19.

As the digital maturity of health services continues to improve, there is scope for Digital Health to extend the 72 controls to include additional measures. Digital Health has advised that it plans to review the controls with a view to expand them to cover other key risk areas, such as biomedical device security.

3 Effectiveness of data security in health services

Digital Health has established a clear roadmap for health services to follow to improve patient data security. However, it is the responsibility of health services to implement and monitor their own measures across the key data security domains of ICT security, personnel security and physical security. This part examines the effectiveness of data security practices at the audited health services and HTS.

3.1 Conclusion

Our testing demonstrated that all the audited health services are vulnerable to attacks that could steal or alter patient data. While the audited health services and HTS have implemented a range of security measures to guard their systems from external, internet-based attacks, they need to improve their internal network and physical security to ensure that patient data is safe and secure.

We identified key weaknesses in data security practices, including inadequate user access controls, weak passwords, and limited network monitoring. Our testing found that once attackers gained access to health services' systems—either through phishing or by implanting a rogue device within a hospital—they could exploit these weaknesses to access patient data. We also found gaps in health services' governance frameworks and policies, which are the foundation of good data security practices.

We found that staff awareness is a critical issue for health services and HTS, as staff action can undermine even the strictest ICT and physical controls. Only one audited health service provides mandatory cyber and data security training to all staff. As health services continue to introduce digital records systems to improve clinical outcomes, it is vital that all staff—including clinical staff—can identify and manage risks to patient data security.

3.2 Penetration testing results

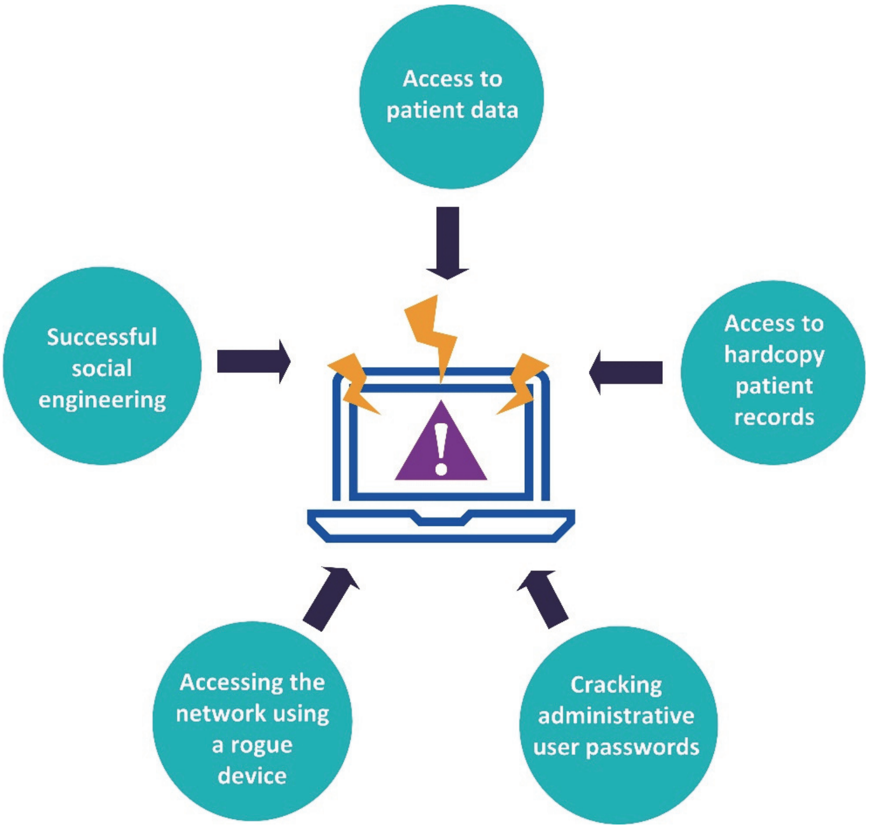
We tested whether health services and HTS have effective data security practices. The testing was based on the common techniques and tools that cybercriminals or malicious 'insiders' use to attack, such as hospital staff or patients with unsupervised access to hospital systems.

In late 2018, DHHS funded penetration testing for all Victorian health services. Overall, it found that most health services have taken effective steps to protect their systems from internet-based attacks. Our testing complemented DHHS's work by focusing primarily on the following scenarios:

- An attacker attempts to gain access to an ICT system by physically connecting a rogue device to the network or exploiting an unlocked workstation.
- An attack could come from an 'insider' such as a staff member or an attacker that has already breached internet security controls, like firewalls. Once inside the ICT environment, the attacker then tries to access and remove patient data.

Figure 3A summarises the results of our penetration testing. We were able to access the applications used to store patient data at all the audited health services through social engineering techniques or by gaining physical access.

Figure 3A
Penetration testing overview


Access to patient data
Successful social engineering
Access to hardcopy patient records
Accessing the network using a rogue device
Cracking administrative user passwords

Source: VAGO.

The testing identified common weaknesses across all four audited agencies that hackers could exploit to gain access to ICT systems and patient data, including insufficient port security, weak user passwords, limited network segmentation and low staff awareness of data security.

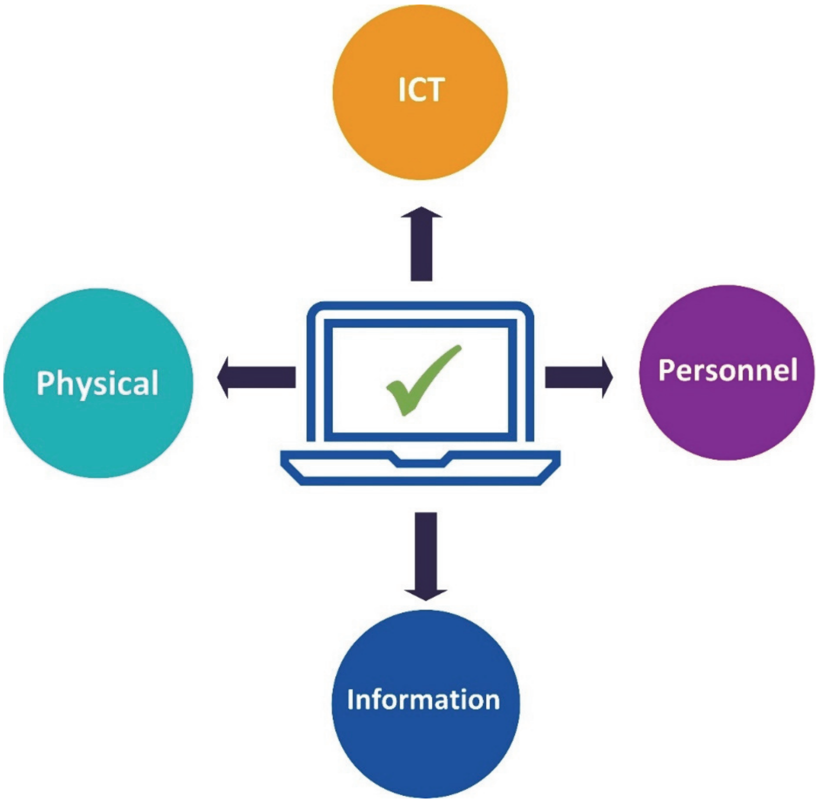
In the following sections we discuss these findings in relation to the key data security domains of governance, ICT security, personnel security and physical security.

3.3 Governance

Protecting patient confidentiality is a core principle of clinical care; however, health services have only recently begun to consider the privacy risks of digital technologies. Figure 3B summarises the audited agencies' data security policies. These policies are discussed further in Sections 3.5 and 3.6.

While we found that three of the four audited agencies have detailed policies, none of the audited health services had an integrated approach to managing data security across both hardcopy and digital records, and the data security domains. Better practice recommends that organisations identify the people, processes and IT systems managing sensitive information and develop policies and procedures across each security domain.

Figure 3B
Important elements of a data security policy



Source: VAGO.

3.4 ICT security

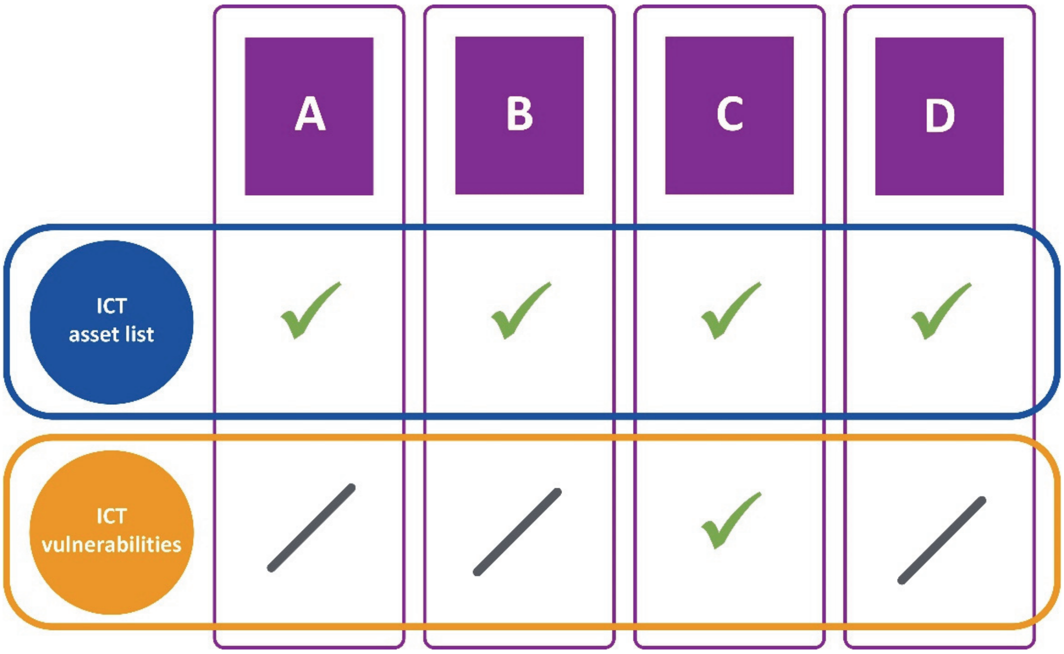
ICT security is fundamental to the ability of health services to protect patient data. However, all audited agencies had weaknesses in aspects of their ICT security. Common weaknesses include inconsistent patching practices, ineffective user access controls and incomplete knowledge of ICT assets.

We also found that while all audited agencies have undertaken security testing of key systems in the past, three completed them on an ad hoc basis. As per NIST's *Technical Guide to Information Security Testing and Assessment*, health services need to develop a policy that outlines when and how often they will test their ICT, personnel, and physical security controls. Without this, health services do not know whether they effectively protect patient data.

ICT asset identification

Without a comprehensive record of the number and type of ICT devices within a hospital, health services cannot fully understand the security risks they face or protect their devices. Figure 3C outlines whether health services maintain an ICT asset list and identify asset risks.

Figure 3C
ICT asset identification



	A	B	C	D
ICT asset list	✓	✓	✓	✓
ICT vulnerabilities	/	/	✓	/

Note: Audited agencies include three health services and HTS and have been de-identified above as 'A–D'.
Note: **/** indicates we assessed the agency as 'partial' as the program used to identify ICT vulnerabilities was not comprehensive
Source: VAGO.

While all audited agencies had documented their individual ICT assets and vulnerabilities in some way, only one of the audited health services utilised a program to scan the network to identify all ICT assets connected to the network, and associated vulnerabilities.

During the testing, we found that hospitals without an asset identification program had vulnerabilities, such as an unprotected program, server or computer, that could be exploited to gain access to patient data once inside the hospital.

Antivirus and patch management

Digital Health's controls require health services to review and implement all operating system patches within one month of release, and within three months for application patches. Of the audited agencies, one reports that it has fully implemented the control and two report partial implementation.

A **patch** is a set of computer code released by a software manufacturer to change or update existing programs. Organisations need to apply patches to their systems to ensure their software has the most up-to-date features, including security protections.

In three of the audited agencies we found devices that did not have adequate patching or antivirus protection, and unsecured network ports. Health services need to secure network ports to prevent attackers using open ports to connect unauthorised devices to their networks.

All health services have documented antivirus and patch management in their ICT policies and procedures. This highlights the need for health services to regularly test their controls to ensure their policies and procedures are effective.

Network monitoring and segmentation

Digital Health's controls require health services to effectively segment their ICT networks so that a successful security attack on one segment is unable to spread to other critical systems. All the audited health services have made progress towards implementing this control. Three report partial implementation, and one reports full implementation.

Network monitoring uses a program to constantly monitor a computer network for issues and alert staff to problems in real time.

Health services also need to effectively monitor their networks to detect possible attacks in real time. Although we did not test the ability of audited agencies to detect unusual network activity, we did identify weaknesses in their internal network monitoring. Digital Health is in the process of procuring a tool that monitors networks in real time and gives health services alerts when it detects unusual activity.

User access management

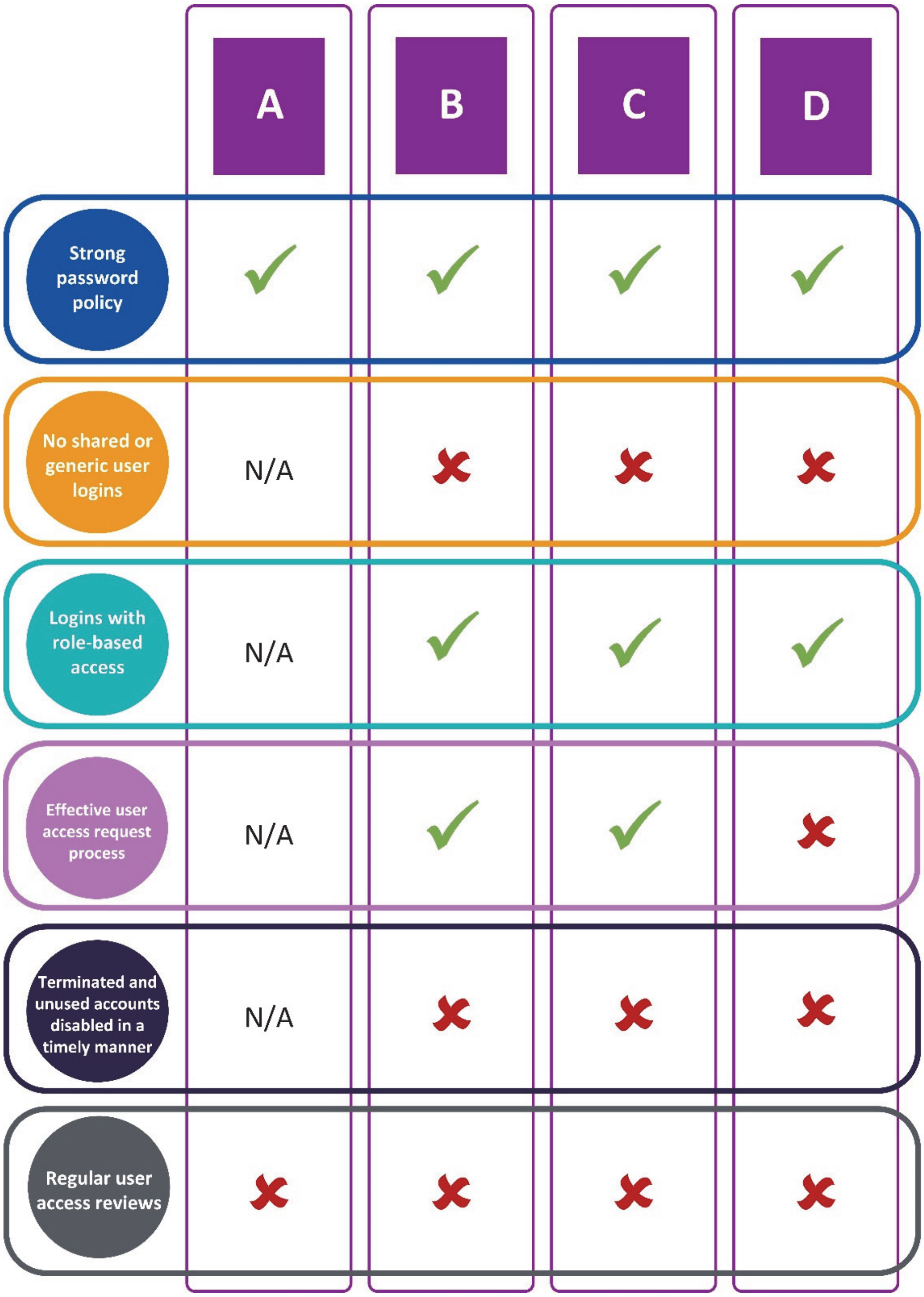
Health services need effective controls to ensure that only authorised staff can access the ICT applications used to store patient data. We found that all the audited health services can improve the way they manage user access.

User provisioning is the process of setting up accounts that provide individuals with access to ICT systems. Organisations should have documented processes for staff to request access, and to cancel access when it is no longer needed.

The key control for user access is a clear policy that outlines the process for user provisioning and de-provisioning. Health services should only grant users access to patient systems based on documented approval from the relevant manager. To confirm whether the user access controls are effective, health services should review their user accounts annually to check whether any terminated staff still have system access.

Figure 3D summarises our assessment of health services' user access controls.

Figure 3D
Results of user access controls testing



	A	B	C	D
Strong password policy	✓	✓	✓	✓
No shared or generic user logins	N/A	✗	✗	✗
Logins with role-based access	N/A	✓	✓	✓
Effective user access request process	N/A	✓	✓	✗
Terminated and unused accounts disabled in a timely manner	N/A	✗	✗	✗
Regular user access reviews	✗	✗	✗	✗

Note: Audited agencies include three health services and HTS and have been de-identified above as ‘A–D’.
Note: N/A indicates where we could not make an assessment due to the agency not having sufficient information.
Source: VAGO.

We found a range of weaknesses in how health services manage user access, including:

- unused and terminated employee accounts still enabled
- failure to keep individual user access approval forms as a record that a relevant manager approved access
- a lack of any formal, regular user access review to ensure only staff who need access have it.

We also found that one of the audited health services has generic user logins for one of its patient data applications. The use of generic and shared logins without strong mitigating controls increases the risk that unauthorised access of patient systems cannot be traced to one employee.

We were unable to test user access controls at one audited agency as its systems were not set up to extract user access data without payment to its third-party provider. This arrangement poses a significant risk as it prevents the health service from testing the effectiveness of its user access controls.

Passwords

We found that health services are not enforcing the use of long passwords, which are more difficult for cyberattackers to crack. We found examples where both clinical and ICT staff were using weak passwords to access their user accounts. We also identified administrator accounts with weak passwords, which is a risk because administrator accounts provide unrestricted access to health services' networks.

Crucially, we found examples where servers and other ICT equipment still had default account names and passwords. This is a significant risk because lists of default credentials exist on the internet. In one audited health service, we accessed a third-party system that was protected with only a default username and password.

Digital Health recommends health services align their password policies with the NIST standard. In 2018 NIST released Special Publication 800-63B on *Digital Identity Guidelines*, which recommends a move away from the traditional approach of using passwords that are changed frequently and require special characters to longer passphrases. It argues that traditional passwords are hard for individuals to remember—which can encourage people to write their passwords down—but paradoxically easy for cybercriminals to hack using algorithms. The new guidelines recommend that individuals use passwords that:

- are a minimum of eight and a maximum of 64 characters
- do not require the use of special characters (e.g. #,!)
- restrict sequential and repetitive characters (i.e. ABC, AAA)
- restrict context-specific words (e.g. the name of the organisation where the individual works)
- restrict common weak passwords, such as 'password1'
- restrict the use of passwords that are known to have been used in past breaches.

In contrast, ASD's *Information Security Manual* recommends that organisations use passwords that are a minimum of 13 alphabet characters, or a minimum of 10 characters, including characters from at least three of the following categories:

- lowercase alphabet characters
- uppercase alphabet characters
- numbers
- special characters.

While most audited agencies use eight-character passwords, as NIST recommends, we were still able to crack administrator passwords within a short timeframe. Recent international research found that hackers can crack any eight-character password within two and a half hours. To better manage the risk of cyberattack, health services should adopt passwords that are a minimum of 13 characters.

Multi-factor authentication

Digital Health follows ASD guidelines by recommending MFA for remote access to administrator accounts. MFA is a method of granting access to a computer system that requires users to provide more than one form of evidence, such as users providing a password as well as a special code generated by an application on their phone. MFA guards against attacks that rely on discovering or cracking user passwords because legitimate users need to provide an extra form of authentication.

We found limited use of MFA. One audited health service has optional swipe cards as a form of MFA for patient databases. Another audited health service advised that MFA for clinical staff would be too onerous and could potentially endanger patients if a clinician did not have their swipe card or access token with them. However, given the password weaknesses we identified, health services should consider the benefits of MFA for all users.

3.5 Personnel security

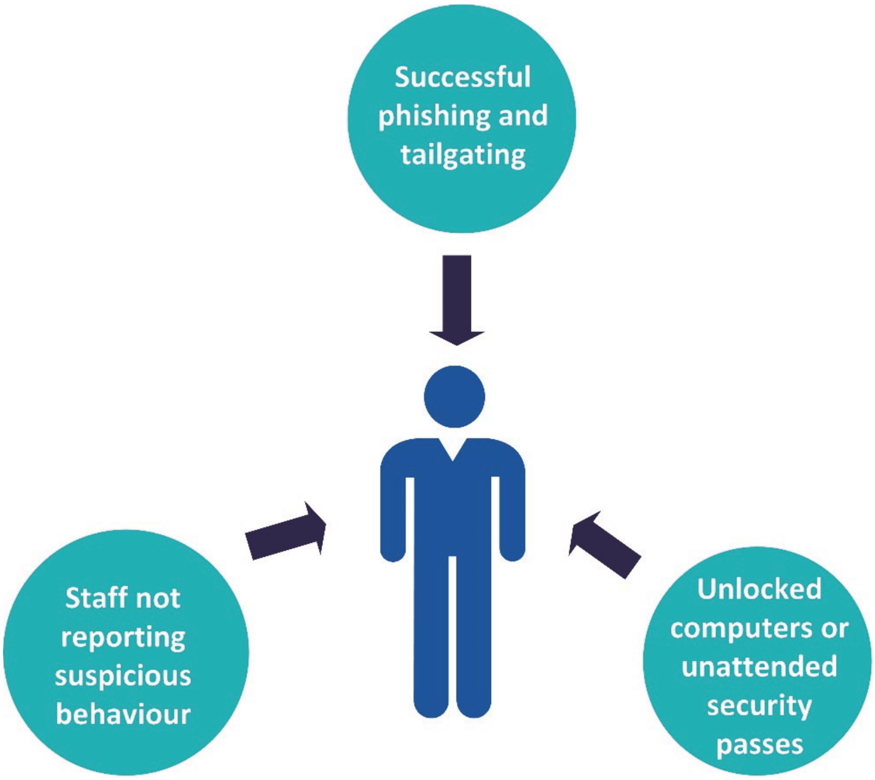
An organisation may have strong ICT controls, but staff action can undermine them. Health services are especially vulnerable to social engineering techniques that exploit staff because hospitals are busy, and open to the public. We found the audited health services do not train personnel to recognise suspicious behaviour, or to practice basic security such as locking computers, not clicking on suspicious links, or protecting their security access passes. We also found unattended hardcopy documents with patient information at all three health services, particularly on printers.

Social engineering is the practice of manipulating behaviour to access confidential information or physical areas. Examples include phishing, where someone is persuaded to provide their account password or click on an unsafe link, or baiting, where an attacker drops a USB stick hoping someone will plug it into a computer.

We found that hospital staff are more likely to be accommodating rather than sceptical. In one scenario, a hospital staff member gave us unsupervised access to their computer following a request to print a document. In another, we placed a rogue device in a printer room in front of a staff member, who did not question us or contact management.

Figure 3E outlines the weaknesses we identified in health services' personnel security.

Figure 3E
Personnel security test results


Successful phishing and tailgating
Staff not reporting suspicious behaviour
Unlocked computers or unattended security passes

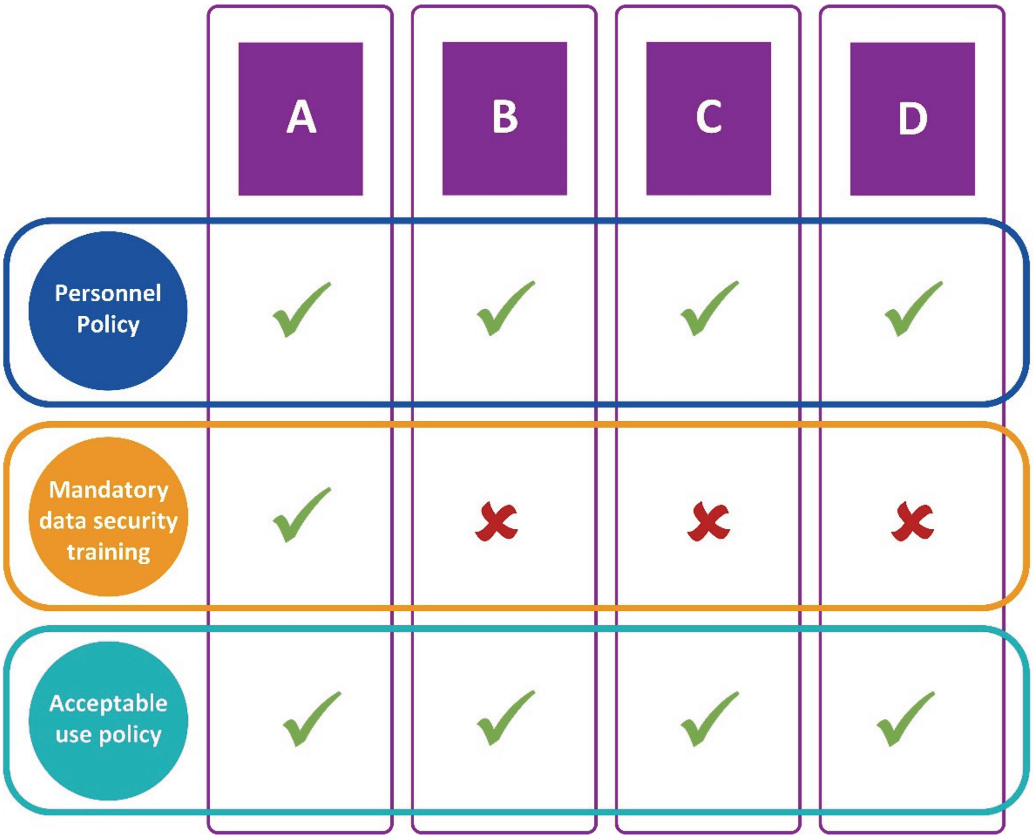
Source: VAGO.

Staff onboarding and training

Health services need to provide staff with guidance on how to use their ICT systems and training on how to manage security risks. In addition, health services must ensure that ICT staff receive regular training in cybersecurity because the tools and techniques used by cybercriminals constantly evolve.

As outlined in Figure 3F, we found that all audited hospitals had documented their procedures related to onboarding and offboarding, and had acceptable use policies, which outlines health services' expectations for how staff should use the internet and other ICT equipment. Despite this, we found patient data stored in unsecured shared files on all health services' networks, which staff had downloaded from clinical applications, but not secured appropriately.

Figure 3F
Summary of personnel security policies and procedures



	A	B	C	D
Personnel Policy	✓	✓	✓	✓
Mandatory data security training	✓	✗	✗	✗
Acceptable use policy	✓	✓	✓	✓

Note: Audited agencies include three health services and HTS, and have been de-identified above as 'A–D'.
Source: VAGO.

Only one audited health service provides mandatory data security training for all staff, which is through an e-learning course. While the other audited health services do conduct cyber-awareness activities, such as phishing and information campaigns, they do not provide staff training. Instead, as part of standard human resources' onboarding processes all the audited health services require staff to sign an acceptable ICT use policy. However, this approach does not provide any assurance to the hospital that staff understand security risks and the hospital's approach to data security.

One health service advised that it is considering developing cybersecurity training for all staff; however, it also noted that it would be unlikely that the training would be mandatory due to the amount of compulsory training clinical staff are already required to complete.

None of the audited health services has dedicated data security training for their ICT staff. However, all the audited health services send their staff to group training sessions organised by Digital Health and we did find examples where individual staff members attended security training as part of their professional development activities. There is a need for health services to improve the security capability of their ICT staff, given the lack of dedicated cybersecurity specialists in health services.

Managing inappropriate data access

In addition to training and acceptable use policies, health services need to monitor staff access to patient records to ensure they access only the information necessary for treatment, or information that is relevant to their role.

Health services operate on the principle that clinicians should have easy access to the patient information they require. One of the key advantages of digitising patient records is that clinicians no longer need to order and maintain hardcopy files, but can access patient data at the point of care. However, only one of the audited health services has a regular, documented process for identifying and managing inappropriate staff access to patient data.

This health service has an EMR that logs every time a user views or changes a patient record, which allows it to review whether staff are accessing records appropriately. Its EMR also includes a feature that protects sensitive patient records that include information about mental health or sexual abuse. When a staff member that is not directly treating a sensitive patient attempts to access their record, the system requires them to enter the reason why they wish to do so. The system will then allow the clinician to access the record, which means that patient treatment is not delayed. Health information services staff regularly review these cases to ensure that the reasons are legitimate and take disciplinary action if necessary.

The other health services investigate staff access to digital records only in response to a specific privacy complaint, or on an ad hoc basis, such as when treating high-profile patients. Without an audit process, health services cannot assure themselves that staff access patient data appropriately.

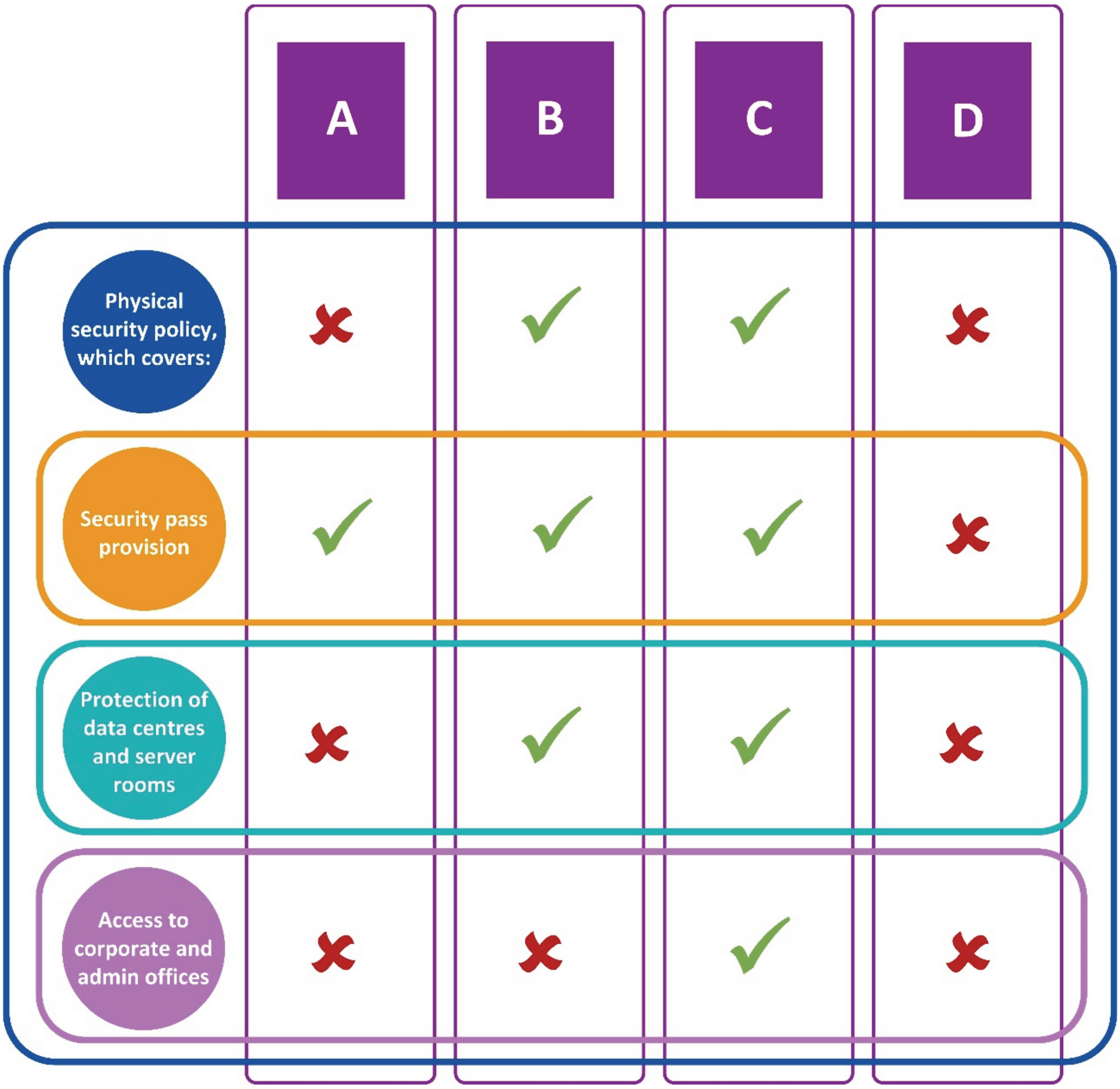
In contrast, we found that health services have well-developed processes for managing access to their hardcopy patient files. To effectively protect patient data in all its formats, health services need to integrate their information management practices, which were developed to protect hardcopy records, with ICT security and user access policies.

3.6 Physical security

Strong physical security measures are necessary to complement ICT and personnel controls. While an organisation may have strong external ICT controls—such as firewalls—poor physical security can override these. Although hospitals are designed to enable free movement, health services need to secure sensitive areas, such as server rooms and corporate offices.

Health services do not have comprehensive physical security policies, as outlined in Figure 3G. The audited health services have not documented their approach to physical security, such as defining restricted access areas where sensitive information (such as patient data records, or ICT servers) is stored, or door security and access pass policies for staff.

Figure 3G
Physical security policies



	A	B	C	D
Physical security policy, which covers:	✗	✓	✓	✗
Security pass provision	✓	✓	✓	✗
Protection of data centres and server rooms	✗	✓	✓	✗
Access to corporate and admin offices	✗	✗	✓	✗

Note: Audited agencies include three health services and HTS and have been de-identified above as 'A–D'.
Source: VAGO.

Digital Health directs health services to ensure that all servers, ICT infrastructure, and critical systems are stored in facilities with protection against physical access or tampering by unauthorised persons. We accessed critical ICT infrastructure at two of the audited health services due to weaknesses in their physical controls, allowing us to connect a rogue device to a network. We also found that corporate and administration offices had inadequate physical security. These spaces are vulnerable to social engineering techniques such as tailgating, where individuals without swipe card access follow authorised staff members to gain access to restricted areas. It is important that health services secure corporate areas because attackers can use these spaces to gain network access, such as through unsecured workstations or by finding an unattended swipe card.

4 Health Technology Solutions and vendor security

Health services typically store their patient data in applications hosted and secured by third-party vendors. However, health services remain responsible for protecting patient data and ensuring that vendors fulfil their security responsibilities.

HTS—a business unit within DHHS—is the key provider of outsourced ICT business systems to Victorian health services, including clinical and patient administration applications. Although it is optional to use HTS's services, 61 per cent of health services use at least one of the clinical and patient data applications hosted by HTS. In addition, some health services use shared ICT services provided by RHAs or directly engage third-party vendors.

4.1 Conclusion

Despite being part of DHHS, HTS has not fully implemented Digital Health's cybersecurity controls and has similar security weaknesses to Victorian health services. Given the volume of patient data stored on HTS's systems, it is vital that HTS improves its security practices.

While HTS has established a process to monitor vendor performance, it needs to ensure that its main third-party vendor complies with relevant security controls within an agreed timeframe. It is critical that HTS assures itself that the vendor is appropriately managing its staff's access to HTS systems, because the vendor is responsible for managing the infrastructure that stores patient data. HTS also needs to assure itself that the vendor has addressed past weaknesses in incident management.

We also found issues with vendor management at two of the audited health services. At one health service, we gained access to patient data by a system managed by a third-party vendor. At another health service—which is part of an RHA—we found confusion around responsibility for data security. While it is common practice for health services to outsource key parts of their ICT operations, they remain accountable for the security of their patient data and need to ensure that third-party vendors fulfil their security responsibilities.

4.2 HTS services

DHHS has provided ICT business applications for health services as part of the HealthSMART program since 2006. Initially, it was mandatory for Victorian public health services to participate in the HealthSMART program and use its patient data applications. Since the HealthSMART program ended in 2013, it has been optional for health services to use DHHS's systems, which are now provided by HTS.

Sixty-one per cent of Victorian health services currently use HTS's clinical or patient administration applications, as outlined in Figure 4A. A further 32 Victorian health services only use the HTS-hosted financial management system. This represents 99 per cent of Victorian health services. Figure 4A shows the number of health services and RHAs using the clinical system, patient management application or financial management system via HTS.

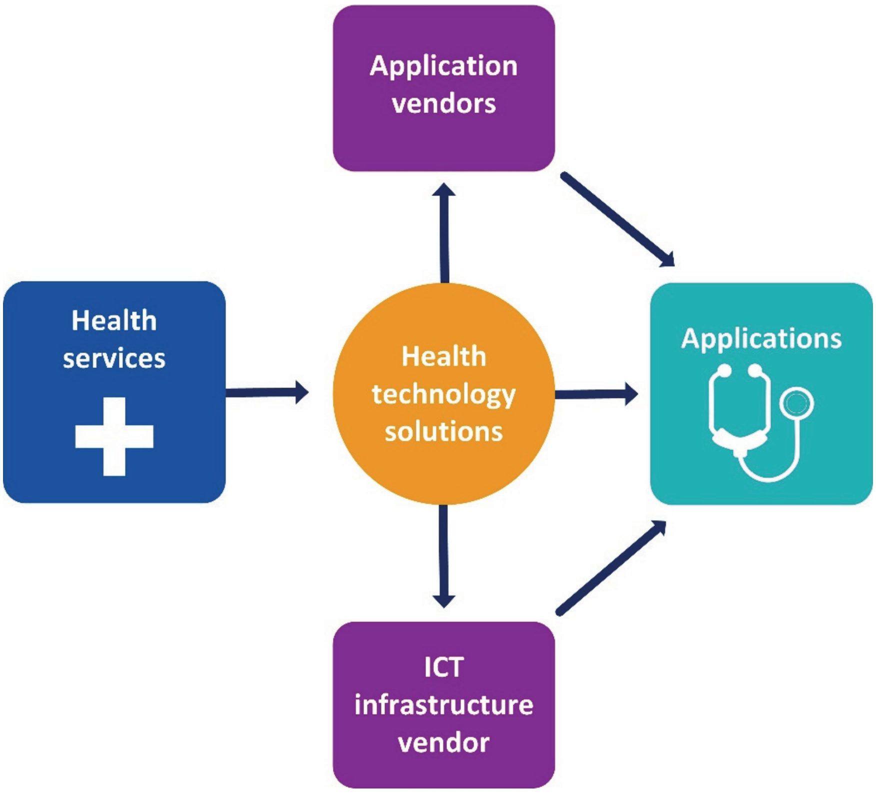
Figure 4A
Heath services and RHAs using HTS services in 2018–19

Type of service	Health services	RHAs
Clinical system	6	0
Patient management application	8	3 (39 health services)
Financial management system	7	5 (71 health services)

Source: VAGO, from HTS data.

HTS hosts and supports ICT applications on behalf of its client health services. Health services engage HTS directly to access applications and HTS maintains a head contract with the relevant application vendors. HTS has service level agreements (SLA) with each participating hospital and vendor that specify the required performance levels. As the health services only have agreements with HTS, HTS manages all interaction with the application vendors, including escalating service requests and managing changes to systems. In addition, HTS servers—where patient data is stored—are managed by a third-party vendor. HTS also outsources some security functions to the same vendor. Figure 4B outlines the service relationships between HTS, health services and providers.

Figure 4B
Service relationships between HTS, health services and vendors



Source: VAGO.

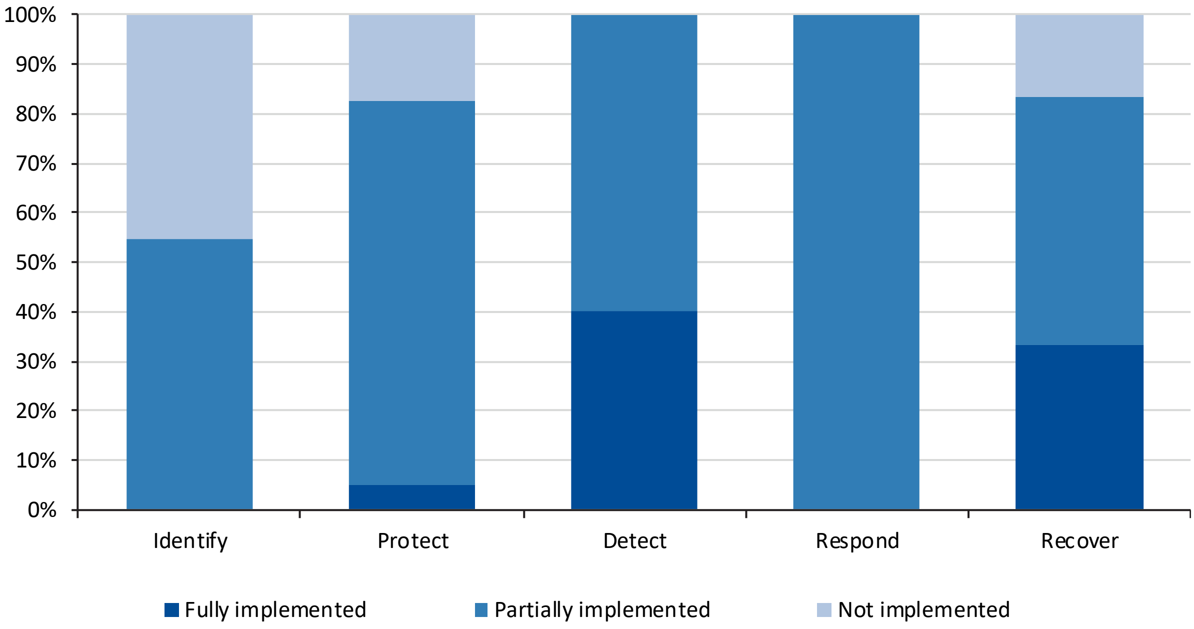
Data security

Under its agreements with its client health services, HTS must take all reasonable steps to protect patient data from unauthorised access or changes. However, we found similar weaknesses in HTS's security practices to those in health services, including weak passwords, incomplete user access controls, and insufficient patch management. Given that HTS is custodian of most of the patient information in the sector, it is vital that DHHS take steps to ensure that HTS has a best practice approach to data security.

HTS does not comply with the 72 controls designed by Digital Health, despite both units being part of DHHS. HTS has fully implemented two of the 38 foundation controls and has partially implemented 29. HTS has made no further progress in implementing the controls since Digital Health first introduced them in March 2017.

Figure 4C highlights HTS's progress implementing the 72 controls in March 2017 against the five core cybersecurity areas. Controls not implemented relate to blacklist management, device testing and user training.

Figure 4C
HTS progress implementing the DHHS cybersecurity controls



Source: VAGO, from DHHS data.

HTS has an extensive suite of policies that align with the standards promoted by the Information Technology Infrastructure Library (ITIL). ITIL aims to support organisations to design and deliver ICT services to their customers. While ITIL does include guidelines on security, they are an addition to its core focus on managing services and operations. In contrast, the ASD and VPDSS recommend that organisations need a holistic approach to security that not only focuses on ICT controls, but also identifies and manages risks across the other key security domains—information, personnel and physical security.

HTS has not developed a schedule for reviewing its ICT polices. On average, HTS reviews its policies every two years. One key policy—the Security Incident Management Standard—was only recently reviewed after eight and a half years. Organisations need a regular review schedule to ensure polices reflect current better practice.

Security assessments

Organisations can assess the security of their ICT systems by conducting vulnerability assessments and penetration testing. Vulnerability assessments often use automated scanning tools that search for known software weaknesses. While organisations can perform vulnerability scanning frequently and in-house, penetration testing is a more targeted exercise conducted by an independent service. In contrast to vulnerability assessments, penetration testing aims to discover unknown weaknesses that attackers could exploit.

HTS uses an automated vulnerability scanning tool every six months to assess its exposure to internet-based threats. HTS requires its third-party vendor to conduct six-monthly vulnerability scans on server infrastructure. However, advances in scanning tools mean that HTS could be scanning more regularly.

A **red team** test simulates an ICT attack to test an organisation's ability to defend itself. The aim is usually for testers to use 'any means necessary' to achieve the test goal.

HTS's Security Vulnerability Assessment Standard states that HTS will conduct penetrating testing 'from time to time', such as after a major security incident or when a new application is rolled-out. HTS engaged security experts in 2016 to conduct a 'red team' test—a more intrusive form of penetration testing—to assess whether patient data could be accessed. Our testing found that HTS has not yet remediated weaknesses identified in this test.

HTS last engaged ICT experts to security test its patient administration application in 2014 and clinical application in 2015. One of our audited health services advised that HTS did not conduct a penetration test or security risk assessment on a patient application it recently engaged HTS to provide. HTS advised that the application was tested when it was first implemented at another health service. While penetration testing may be expensive and can come with the risk of service disruption, it is an important way of managing the risk of cyberattacks. HTS should test applications after significant software updates and when it deploys an application in a new health service.

The lack of regular security testing makes it difficult for HTS to identify and manage risks effectively.

Supporting health services

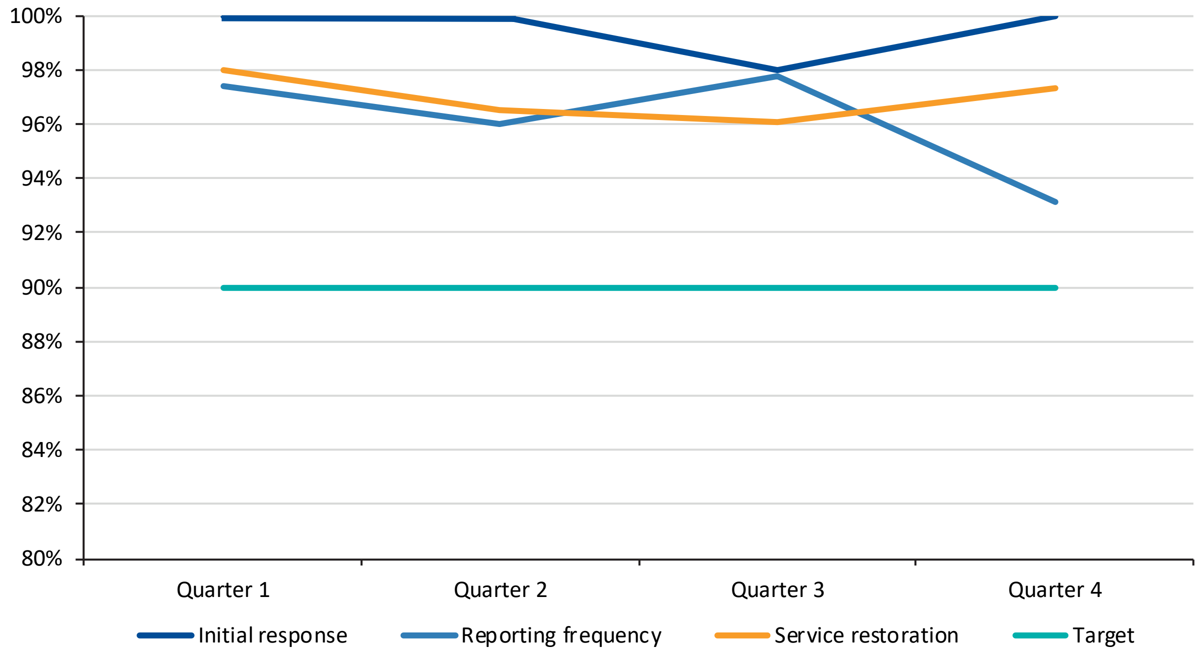
HTS operates a service desk that is the entry point for health services to raise issues that they have with their patient and clinical data applications. While HTS meets its overall SLAs with health services, we identified areas for improvement.

The service desk is the main pathway for health services to receive technical support from HTS. Under its SLAs, HTS has agreed to provide service desk support for individual hospitals. HTS uses its service desk application to track performance against the SLA, including:

- resolved date
- call priority
- problem description
- solution description.

Figure 4D shows HTS's average performance against the agreed service level targets in each quarter of 2018. Initial response and reporting frequency represent whether HTS responds and updates agencies within the agreed time frames. Service restoration tracks whether the business service involved in the incident is restored within agreed timeframes. In 2018, HTS reported that it failed its SLA targets 34 times, out of a total of 1 617 requests. This represents 2 per cent of requests made.

Figure 4D
Reported performance against SLA in 2018 (percentage)

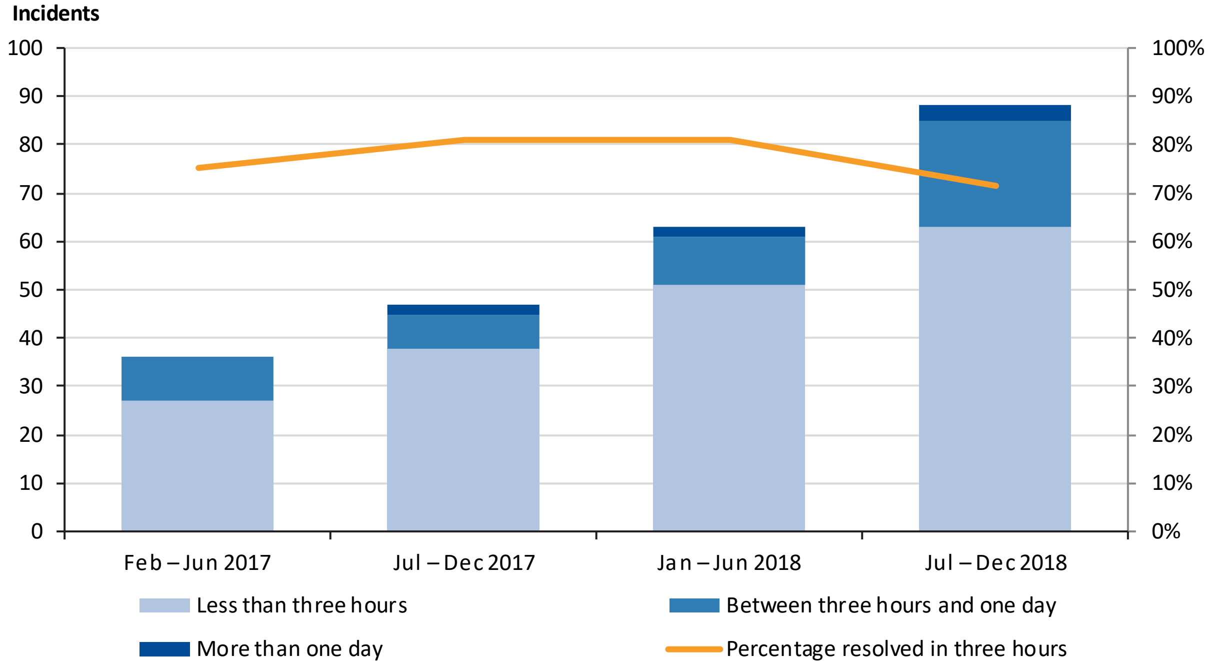


Note: The percentage is an average of all incidents reported to the HTS service desk in the quarter.
Source: VAGO, based on HTS performance reporting.

HTS tracks requests from client health services for enhancement requests, known errors, problems, incidents and major incidents, which HTS defines as having a 'high impact' on any of their client health services. Major incidents include issues that could also occur because of a cyberattack, such as reports of performance issues with key clinical applications, multiple users being locked out of the application, and outages at data centres.

Figure 4E shows how long HTS took to resolve clinical application and patient management system major incidents from January 2017 to December 2018. The sample included two major incidents that HTS defined as security incidents. The longest time a major incident was open was 13 days, however, HTS resolved 76 per cent of major incidents within three hours.

Figure 4E
Resolution of incidents classified as 'major incidents' for clinical application and patient management system



Source: VAGO, from HTS data.

4.3 Vendor management

While it is common practice for organisations to outsource aspects of their ICT services to third-party vendors, health services remain accountable for managing the security of their systems. While HTS has established a process to monitor the security practices of its main vendor, none of the audited health services are assuring themselves that vendors are complying with necessary security controls.

Digital Health has recognised the security risks associated with third-party vendors and is in the process of conducting a risk assessment of vendor security practices on behalf of the sector. This should be a useful resource for health services. However, health services need to actively manage their agreements with third-party vendors.

HTS vendors

HTS uses a third-party vendor to manage the infrastructure used to store patient data. In 2018, HTS entered into a new contract with the vendor it had used from 2015–18.

The new contract requires HTS to develop a vendor cybersecurity policy, and requires the vendor to provide coverage for cybersecurity services.

The contract also specifies that the vendor will ensure that the services it provides to HTS comply with all relevant state and federal government cybersecurity guidelines. The vendor has self-assessed its compliance with the 72 controls and identified gaps. HTS needs to ensure that the vendor takes steps to comply with the controls within an agreed timeframe.

HTS advised that in the past there have been weaknesses in incident management. In one example, a health service alerted HTS to a possible attack, but the vendor did not have staff available to run a vulnerability scan within the required time. While major incidents occur rarely, it is vital that HTS assures itself that its main vendor can respond appropriately.

Rural Health Alliances

RHAs are groups of small regional and rural health services that deliver core ICT services to their members, governed by a joint-venture agreement. DHHS established five RHAs across Victoria in 1997 to improve the ICT capability of small rural hospitals. DHHS made it mandatory for rural hospitals to participate in RHAs in 2008.

RHAs typically use third-party vendors to provide ICT services to their members and require clear governance arrangements to ensure that participants and vendors understand their security responsibilities. While each RHA varies according to the needs of participating health services, they typically manage the core ICT services for members, including internet access, telephony, shared applications, and ICT infrastructure. RHAs typically also engage HTS to provide patient data applications.

One of our audited health services is part of an RHA. While the health service manages its own patient applications, its infrastructure is managed by the RHA, which then outsources key services to third-party vendors. We found significant weaknesses in how the RHA and the audited health service manage data security. The RHA's joint-venture agreement lacks clear SLAs, does not specify how the RHA will manage security, and does not outline how the RHA and member health services should comply with Digital Health's 72 controls. The case study in Figure 4F demonstrates how this confusion impacted the way the RHA and the health service managed a cybersecurity incident.

Figure 4F
Case study

One of the audited health services belongs to an RHA that manages its ICT infrastructure and telecommunications services. The RHA outsources some services to a supplier, who then purchases services from another third-party vendor. In a recent incident, the third-party vendor used by RHA's internet supplier detected an attempted DDOS attack and suspended the internet service. However, the vendor did not communicate effectively with the supplier or the RHA to explain the reason for the service interruption. The health service experienced an internet service outage and reported this to the RHA, but the RHA did not know why it took place.

Digital Health assisted the RHA and the audited health service by hosting a post-incident review. The review found inadequacies in the RHA's incident management process and poor communication with both its member health services and third-party vendors.

Source: VAGO, based on information provided by an audited health service.

DHHS is currently reviewing the joint-venture agreements for RHAs. As part of this, it is essential that RHAs and their members develop clear expectations around data security.

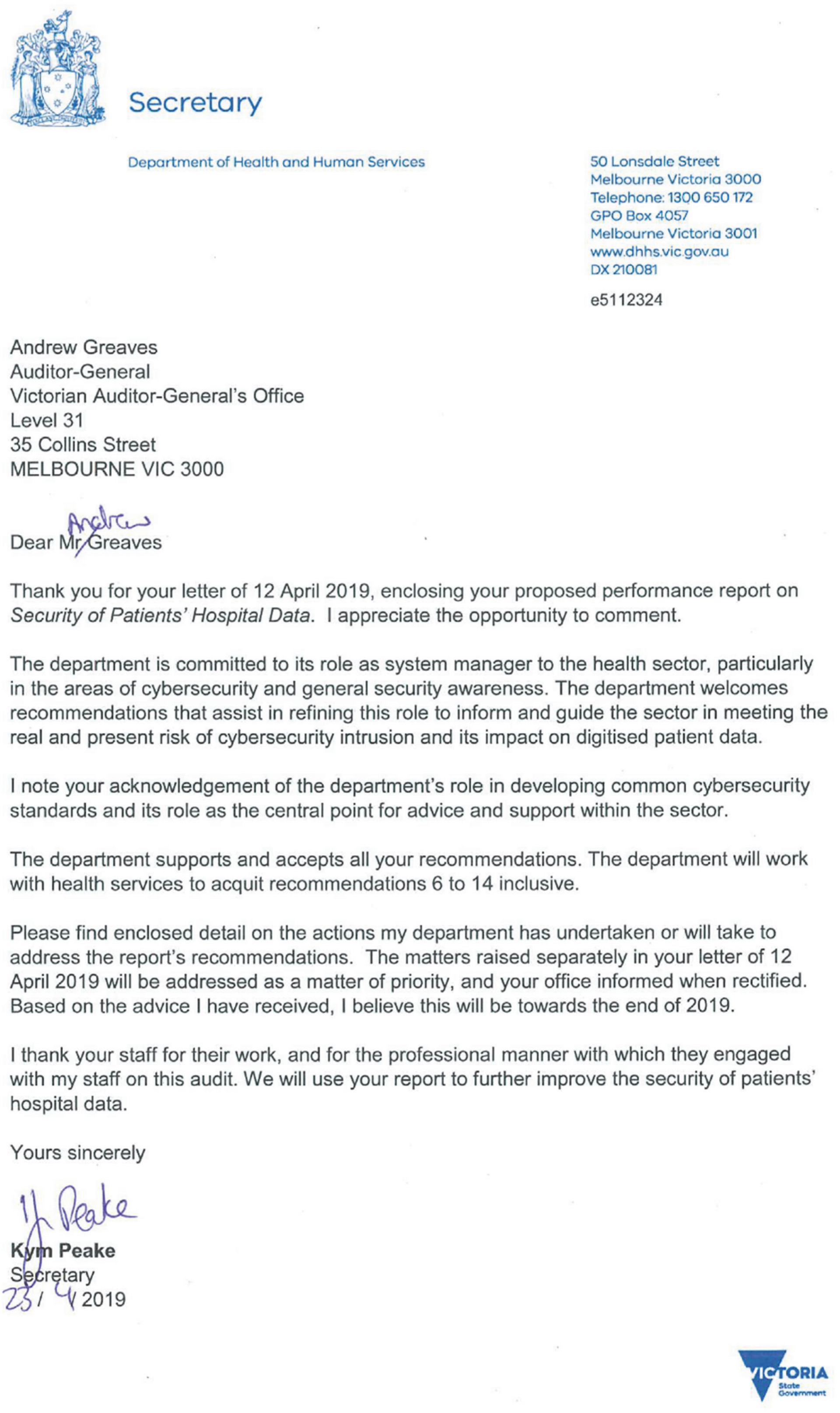
Appendix A *Audit Act 1994* section 16—submissions and comments

We have consulted with DHHS, BH, RCH and RVEEH, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments. We also provided a copy of the report to the Department of Premier and Cabinet.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

RESPONSE provided by the Secretary, DHHS



Secretary

Department of Health and Human Services

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 650 172
GPO Box 4057
Melbourne Victoria 3001
www.dhhs.vic.gov.au
DX 210081

e5112324

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31
35 Collins Street
MELBOURNE VIC 3000

Andrew
Dear ~~Mr~~ Greaves

Thank you for your letter of 12 April 2019, enclosing your proposed performance report on *Security of Patients' Hospital Data*. I appreciate the opportunity to comment.

The department is committed to its role as system manager to the health sector, particularly in the areas of cybersecurity and general security awareness. The department welcomes recommendations that assist in refining this role to inform and guide the sector in meeting the real and present risk of cybersecurity intrusion and its impact on digitised patient data.

I note your acknowledgement of the department's role in developing common cybersecurity standards and its role as the central point for advice and support within the sector.

The department supports and accepts all your recommendations. The department will work with health services to acquit recommendations 6 to 14 inclusive.

Please find enclosed detail on the actions my department has undertaken or will take to address the report's recommendations. The matters raised separately in your letter of 12 April 2019 will be addressed as a matter of priority, and your office informed when rectified. Based on the advice I have received, I believe this will be towards the end of 2019.

I thank your staff for their work, and for the professional manner with which they engaged with my staff on this audit. We will use your report to further improve the security of patients' hospital data.

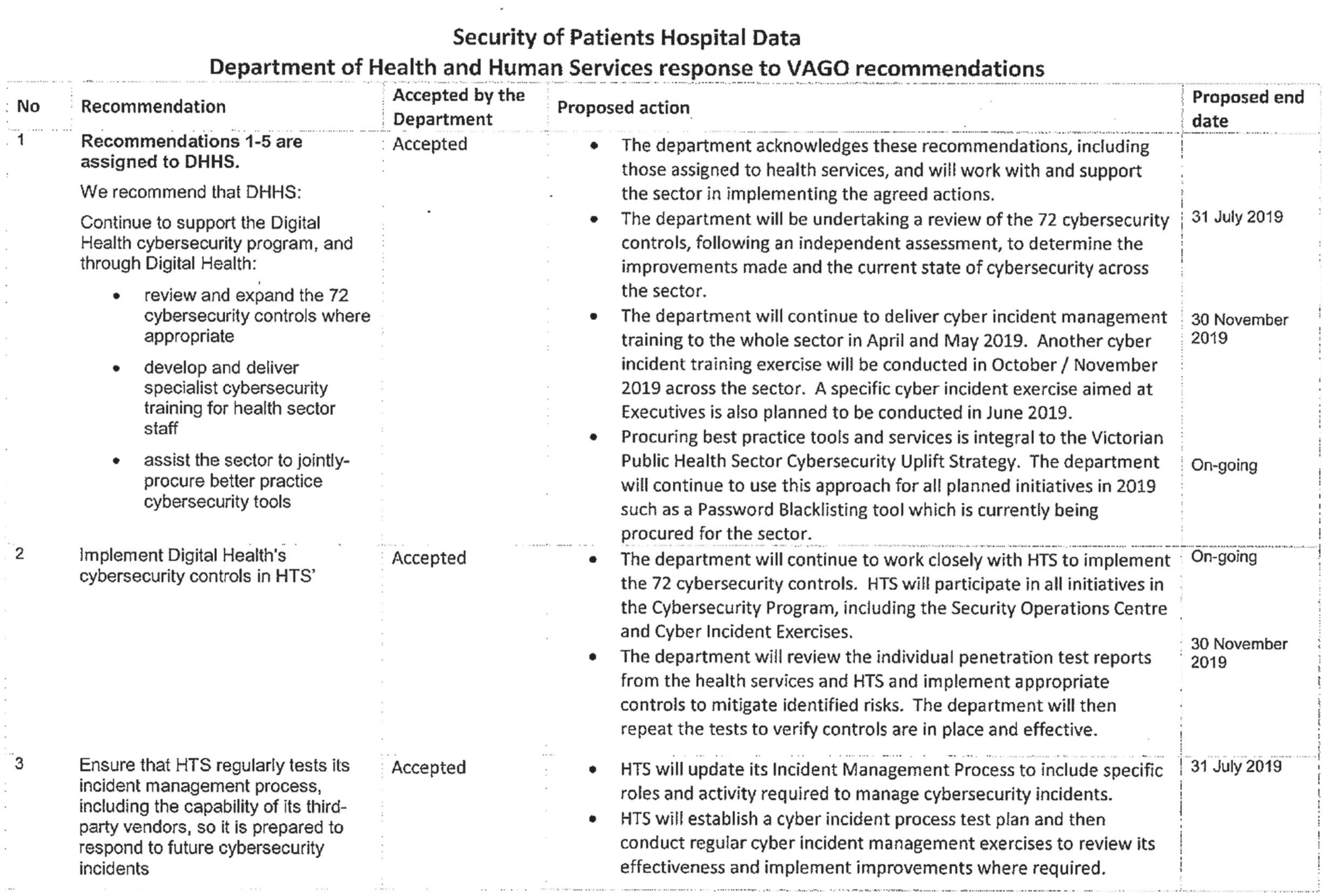
Yours sincerely

K Peake

Kym Peake
Secretary
23/ 4 2019

VICTORIA
State Government

RESPONSE provided by the Secretary, DHHS—continued

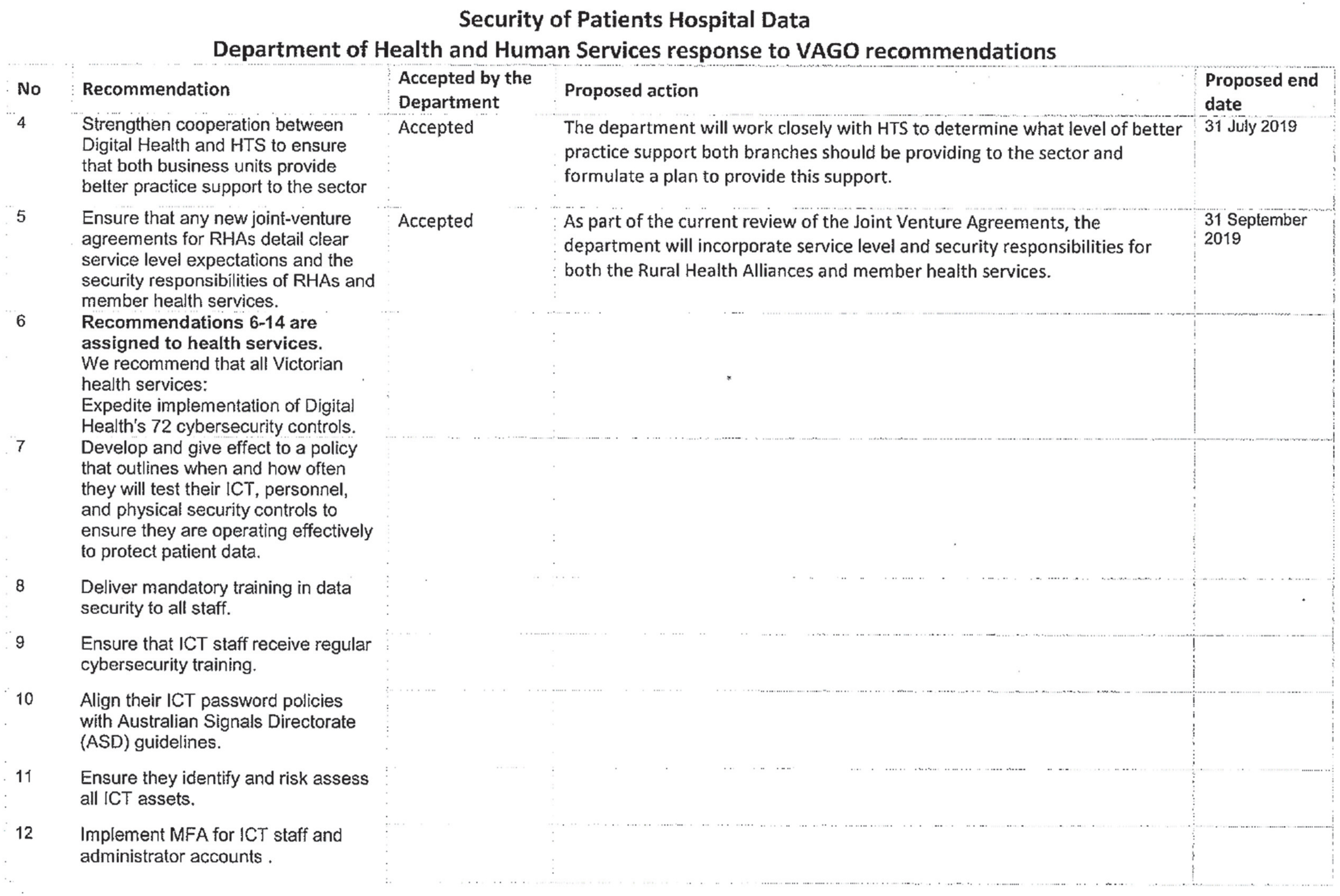


Security of Patients Hospital Data

Department of Health and Human Services response to VAGO recommendations

No	Recommendation	Accepted by the Department	Proposed action	Proposed end date
1	**Recommendations 1-5 are assigned to DHHS.** We recommend that DHHS: Continue to support the Digital Health cybersecurity program, and through Digital Health: • review and expand the 72 cybersecurity controls where appropriate • develop and deliver specialist cybersecurity training for health sector staff • assist the sector to jointly-procure better practice cybersecurity tools	Accepted	• The department acknowledges these recommendations, including those assigned to health services, and will work with and support the sector in implementing the agreed actions.	
			• The department will be undertaking a review of the 72 cybersecurity controls, following an independent assessment, to determine the improvements made and the current state of cybersecurity across the sector.	31 July 2019
			• The department will continue to deliver cyber incident management training to the whole sector in April and May 2019. Another cyber incident training exercise will be conducted in October / November 2019 across the sector. A specific cyber incident exercise aimed at Executives is also planned to be conducted in June 2019.	30 November 2019
			• Procuring best practice tools and services is integral to the Victorian Public Health Sector Cybersecurity Uplift Strategy. The department will continue to use this approach for all planned initiatives in 2019 such as a Password Blacklisting tool which is currently being procured for the sector.	On-going
2	Implement Digital Health's cybersecurity controls in HTS'	Accepted	• The department will continue to work closely with HTS to implement the 72 cybersecurity controls. HTS will participate in all initiatives in the Cybersecurity Program, including the Security Operations Centre and Cyber Incident Exercises.	On-going
			• The department will review the individual penetration test reports from the health services and HTS and implement appropriate controls to mitigate identified risks. The department will then repeat the tests to verify controls are in place and effective.	30 November 2019
3	Ensure that HTS regularly tests its incident management process, including the capability of its third-party vendors, so it is prepared to respond to future cybersecurity incidents	Accepted	• HTS will update its Incident Management Process to include specific roles and activity required to manage cybersecurity incidents. • HTS will establish a cyber incident process test plan and then conduct regular cyber incident management exercises to review its effectiveness and implement improvements where required.	31 July 2019

RESPONSE provided by the Secretary, DHHS—continued

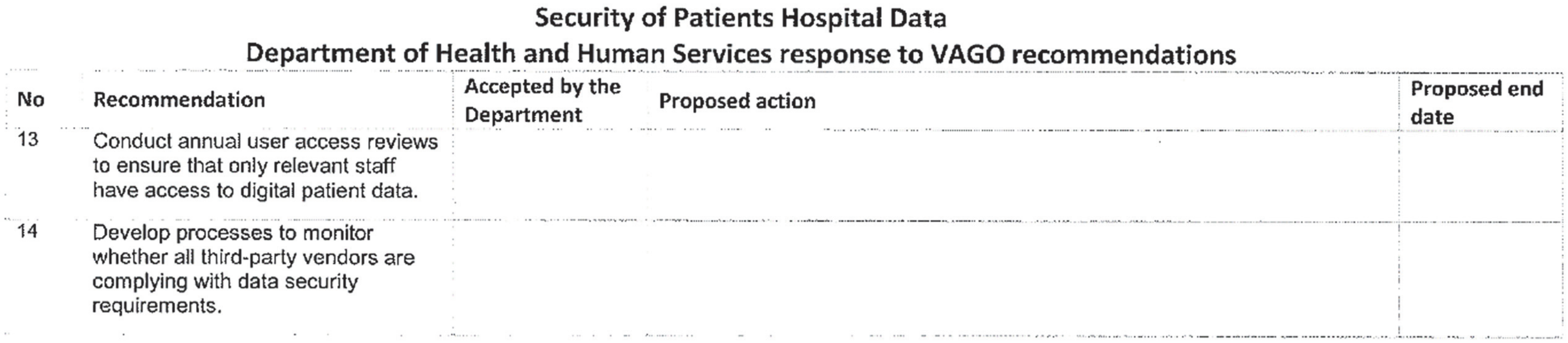


Security of Patients Hospital Data

Department of Health and Human Services response to VAGO recommendations

No	Recommendation	Accepted by the Department	Proposed action	Proposed end date
4	Strengthen cooperation between Digital Health and HTS to ensure that both business units provide belter practice support to the sector	Accepted	The department will work closely with HTS to determine what level of better practice support both branches should be providing to the sector and formulate a plan to provide this support.	31 July 2019
5	Ensure that any new joint-venture agreements for RHAs detail clear service level expectations and the security responsibilities of RHAs and member health services.	Accepted	As part of the current review of the Joint Venture Agreements, the department will incorporate service level and security responsibilities for both the Rural Health Alliances and member health services.	31 September 2019
6	**Recommendations 6-14 are assigned to health services.** We recommend that all Victorian health services: Expedite implementation of Digital Health's 72 cybersecurity controls.			
7	Develop and give effect to a policy that outlines when and how often they will test their ICT, personnel, and physical security controls to ensure they are operating effectively to protect patient data.			
8	Deliver mandatory training in data security to all staff.			
9	Ensure that ICT staff receive regular cybersecurity training.			
10	Align their ICT password policies with Australian Signals Directorate (ASD) guidelines.			
11	Ensure they identify and risk assess all ICT assets.			
12	Implement MFA for ICT staff and administrator accounts .			

RESPONSE provided by the Secretary, DHHS—continued

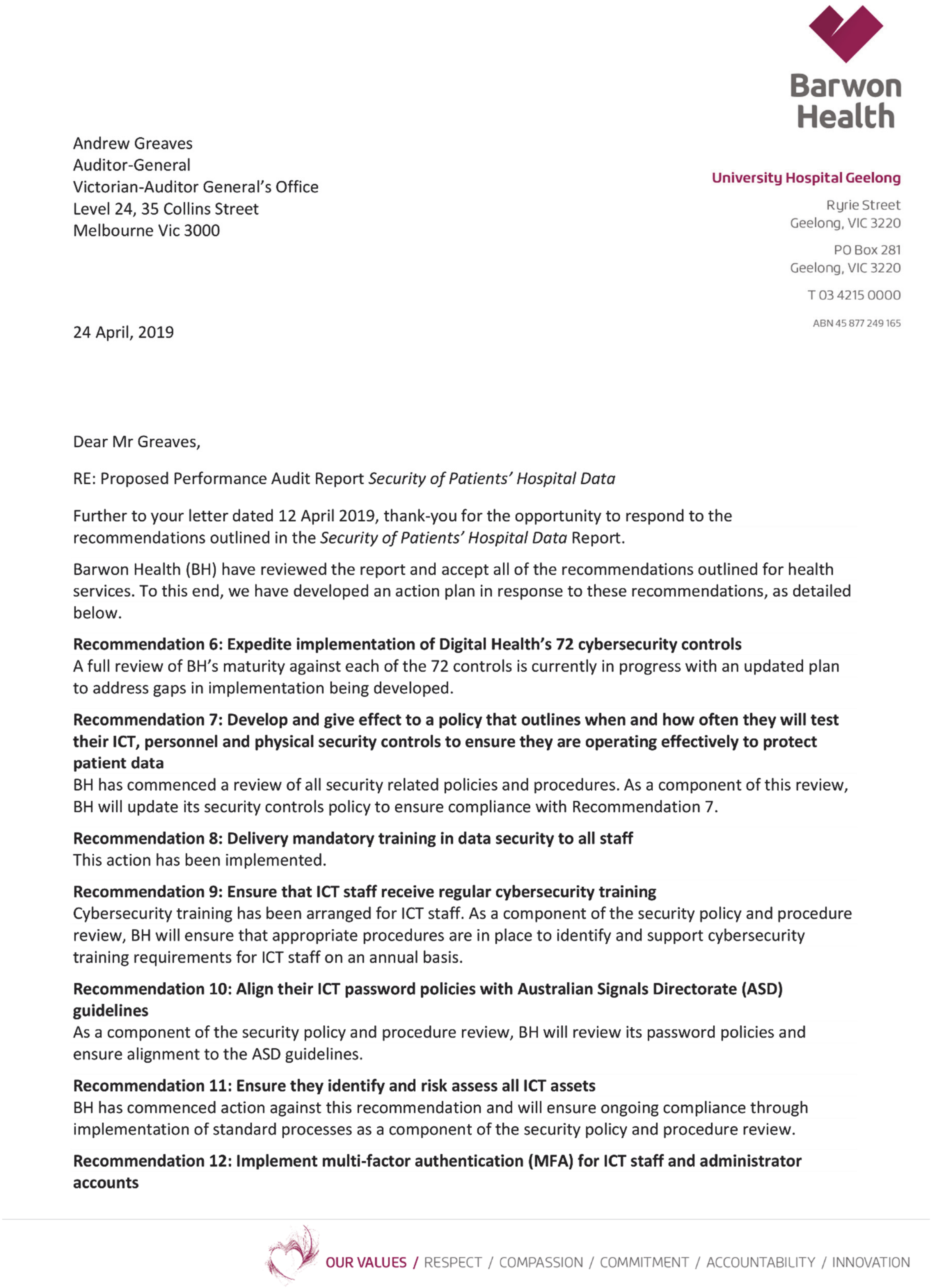


Security of Patients Hospital Data

Department of Health and Human Services response to VAGO recommendations

No	Recommendation	Accepted by the Department	Proposed action	Proposed end date
13	Conduct annual user access reviews to ensure that only relevant staff have access to digital patient data.			
14	Develop processes to monitor whether all third-party vendors are complying with data security requirements.			

RESPONSE provided by the Chair, BH



Barwon
Health

University Hospital Geelong

Ryrie Street
Geelong, VIC 3220

PO Box 281
Geelong, VIC 3220

T 03 4215 0000

ABN 45 877 249 165

Andrew Greaves
Auditor-General
Victorian-Auditor General's Office
Level 24, 35 Collins Street
Melbourne Vic 3000

24 April, 2019

Dear Mr Greaves,

RE: Proposed Performance Audit Report *Security of Patients' Hospital Data*

Further to your letter dated 12 April 2019, thank-you for the opportunity to respond to the recommendations outlined in the *Security of Patients' Hospital Data* Report.

Barwon Health (BH) have reviewed the report and accept all of the recommendations outlined for health services. To this end, we have developed an action plan in response to these recommendations, as detailed below.

Recommendation 6: Expedite implementation of Digital Health's 72 cybersecurity controls
A full review of BH's maturity against each of the 72 controls is currently in progress with an updated plan to address gaps in implementation being developed.

Recommendation 7: Develop and give effect to a policy that outlines when and how often they will test their ICT, personnel and physical security controls to ensure they are operating effectively to protect patient data
BH has commenced a review of all security related policies and procedures. As a component of this review, BH will update its security controls policy to ensure compliance with Recommendation 7.

Recommendation 8: Delivery mandatory training in data security to all staff
This action has been implemented.

Recommendation 9: Ensure that ICT staff receive regular cybersecurity training
Cybersecurity training has been arranged for ICT staff. As a component of the security policy and procedure review, BH will ensure that appropriate procedures are in place to identify and support cybersecurity training requirements for ICT staff on an annual basis.

Recommendation 10: Align their ICT password policies with Australian Signals Directorate (ASD) guidelines
As a component of the security policy and procedure review, BH will review its password policies and ensure alignment to the ASD guidelines.

Recommendation 11: Ensure they identify and risk assess all ICT assets
BH has commenced action against this recommendation and will ensure ongoing compliance through implementation of standard processes as a component of the security policy and procedure review.

Recommendation 12: Implement multi-factor authentication (MFA) for ICT staff and administrator accounts

OUR VALUES / RESPECT / COMPASSION / COMMITMENT / ACCOUNTABILITY / INNOVATION

RESPONSE provided by the Chair, BH—continued

BH is currently reviewing their identity access and management policies, procedures and tools and will ensure that capability for MFA for ICT staff and administrator accounts is a core component of the future roadmap.

Recommendation 13: Conduct annual user access reviews to ensure that only relevant staff have access to digital patient data
As a component of the review of identity access and management policies, procedures and tools, BH will implement robust processes to review appropriateness of access to digital patient data.

Recommendation 14: Develop processes to monitor whether all third-party vendors are complying with data security requirements
As a component of the security policy and procedure review, BH are currently implementing processes to monitor third-party vendor compliance with data security requirements.

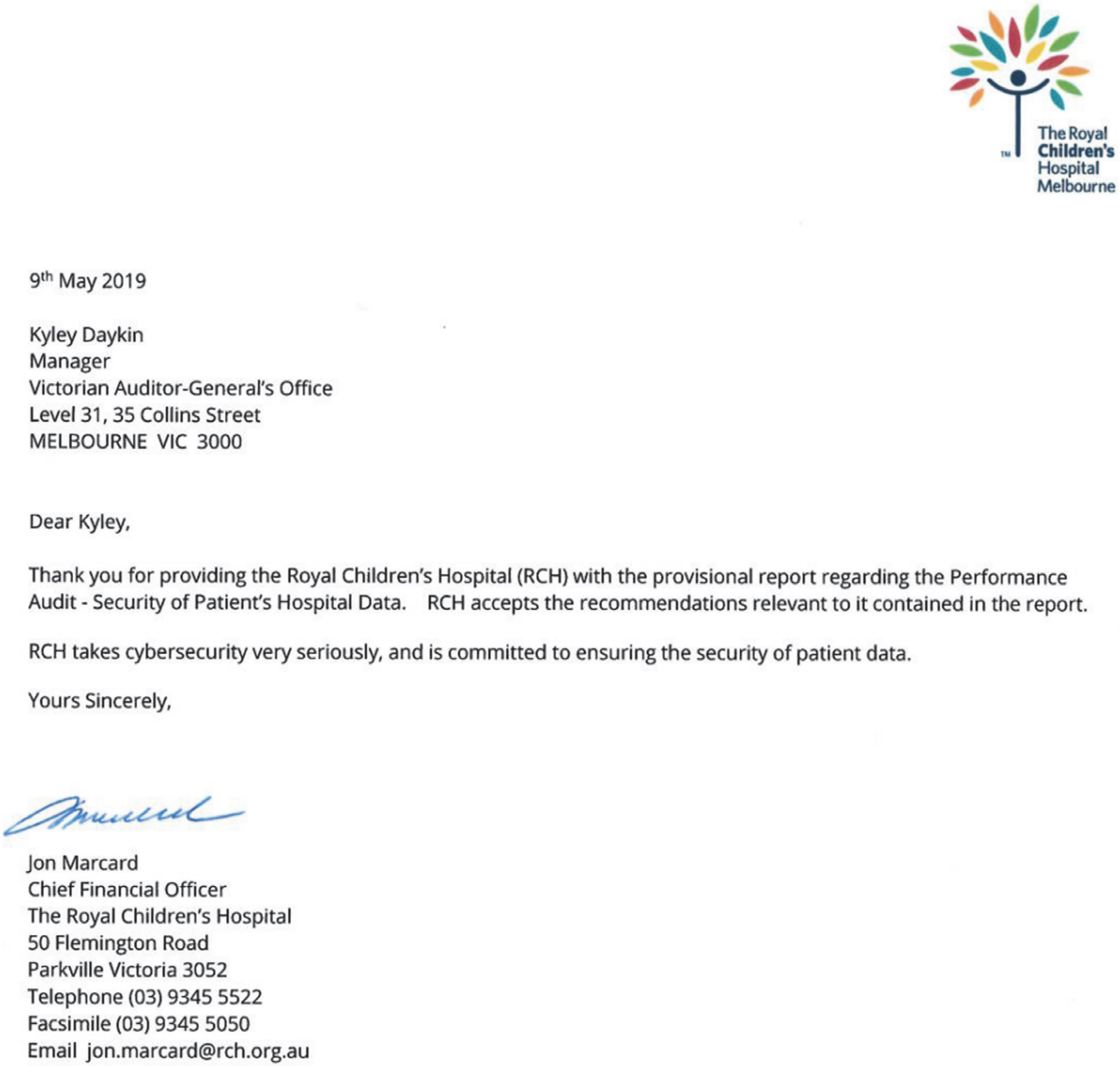
Barwon Health is committed to ensuring the security of the data and information that we hold. Progress against each of these recommendations will be supported and regularly monitored by the Barwon Health Board, and the Board's Audit and Risk Sub-Committee.

Kind Regards,

Brian Cook.

Mr Brian Cook
Chair
Barwon Health Board of Directors

RESPONSE provided by the Chief Financial Officer, RCH



The Royal
Children's
Hospital
Melbourne

9th May 2019

Kyley Daykin
Manager
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear Kyley,

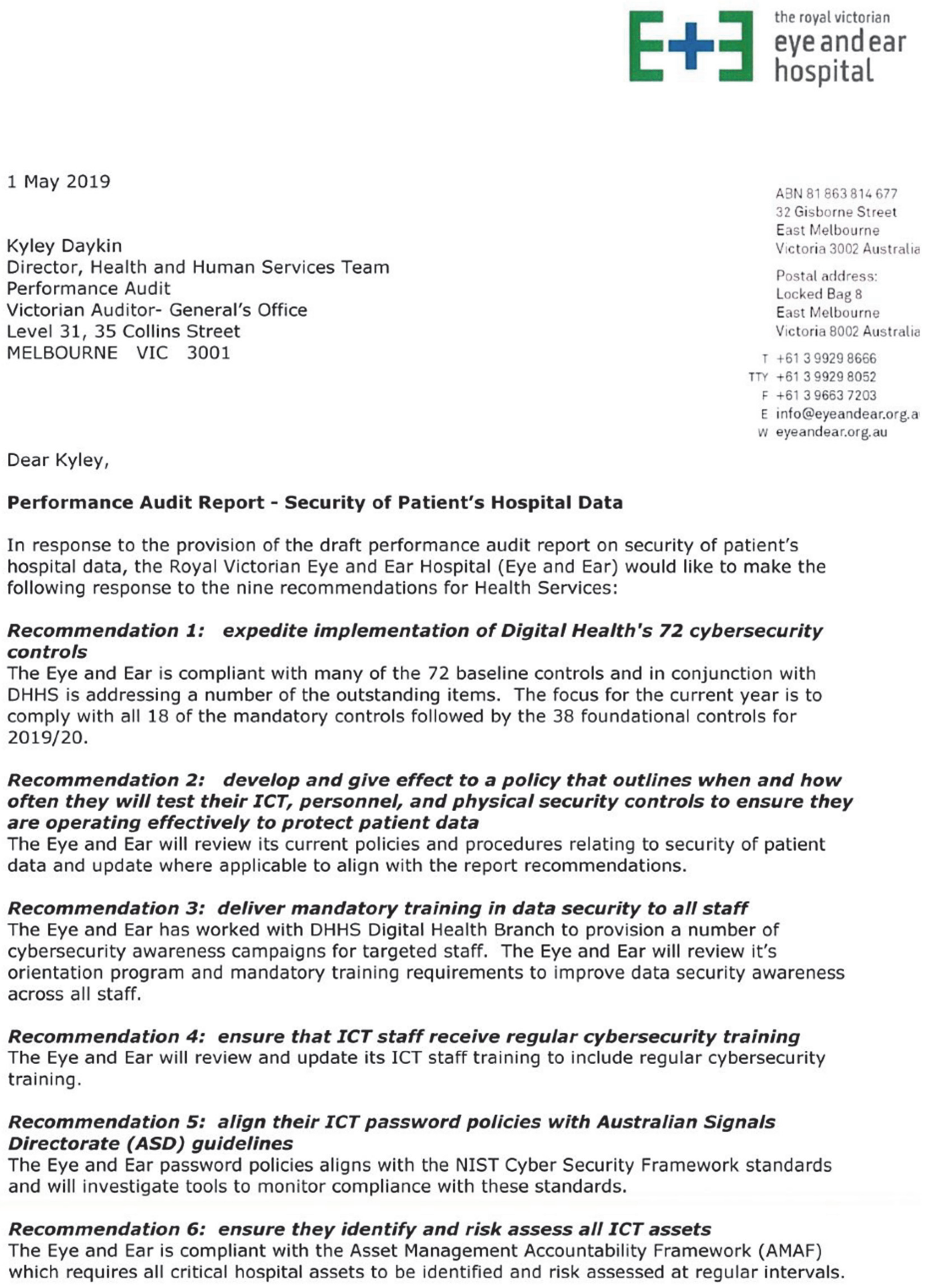
Thank you for providing the Royal Children's Hospital (RCH) with the provisional report regarding the Performance Audit - Security of Patient's Hospital Data. RCH accepts the recommendations relevant to it contained in the report.

RCH takes cybersecurity very seriously, and is committed to ensuring the security of patient data.

Yours Sincerely,

Jon Marcard
Chief Financial Officer
The Royal Children's Hospital
50 Flemington Road
Parkville Victoria 3052
Telephone (03) 9345 5522
Facsimile (03) 9345 5050
Email jon.marcard@rch.org.au

RESPONSE provided by the Chief Executive Officer, RVEEH



the royal victorian
eye and ear
hospital

1 May 2019

ABN 81 863 814 677
32 Gisborne Street
East Melbourne
Victoria 3002 Australia

Postal address:
Locked Bag 8
East Melbourne
Victoria 8002 Australia

T +61 3 9929 8666
TTY +61 3 9929 8052
F +61 3 9663 7203
E info@eyeandear.org.a
W eyeandear.org.au

Kyley Daykin
Director, Health and Human Services Team
Performance Audit
Victorian Auditor- General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3001

Dear Kyley,

Performance Audit Report - Security of Patient's Hospital Data

In response to the provision of the draft performance audit report on security of patient's hospital data, the Royal Victorian Eye and Ear Hospital (Eye and Ear) would like to make the following response to the nine recommendations for Health Services:

Recommendation 1: expedite implementation of Digital Health's 72 cybersecurity controls
The Eye and Ear is compliant with many of the 72 baseline controls and in conjunction with DHHS is addressing a number of the outstanding items. The focus for the current year is to comply with all 18 of the mandatory controls followed by the 38 foundational controls for 2019/20.

Recommendation 2: develop and give effect to a policy that outlines when and how often they will test their ICT, personnel, and physical security controls to ensure they are operating effectively to protect patient data
The Eye and Ear will review its current policies and procedures relating to security of patient data and update where applicable to align with the report recommendations.

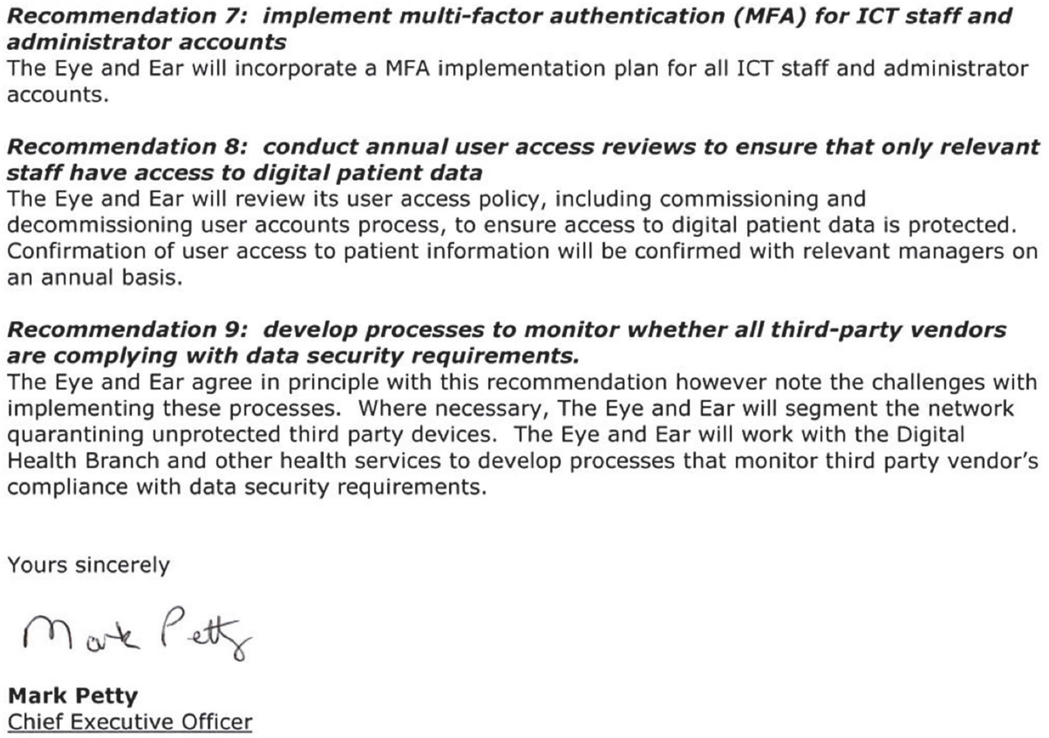
Recommendation 3: deliver mandatory training in data security to all staff
The Eye and Ear has worked with DHHS Digital Health Branch to provision a number of cybersecurity awareness campaigns for targeted staff. The Eye and Ear will review it's orientation program and mandatory training requirements to improve data security awareness across all staff.

Recommendation 4: ensure that ICT staff receive regular cybersecurity training
The Eye and Ear will review and update its ICT staff training to include regular cybersecurity training.

Recommendation 5: align their ICT password policies with Australian Signals Directorate (ASD) guidelines
The Eye and Ear password policies aligns with the NIST Cyber Security Framework standards and will investigate tools to monitor compliance with these standards.

Recommendation 6: ensure they identify and risk assess all ICT assets
The Eye and Ear is compliant with the Asset Management Accountability Framework (AMAF) which requires all critical hospital assets to be identified and risk assessed at regular intervals.

RESPONSE provided by the Chief Executive Officer, RVEEH—continued



Recommendation 7: implement multi-factor authentication (MFA) for ICT staff and administrator accounts
The Eye and Ear will incorporate a MFA implementation plan for all ICT staff and administrator accounts.

Recommendation 8: conduct annual user access reviews to ensure that only relevant staff have access to digital patient data
The Eye and Ear will review its user access policy, including commissioning and decommissioning user accounts process, to ensure access to digital patient data is protected. Confirmation of user access to patient information will be confirmed with relevant managers on an annual basis.

Recommendation 9: develop processes to monitor whether all third-party vendors are complying with data security requirements.
The Eye and Ear agree in principle with this recommendation however note the challenges with implementing these processes. Where necessary, The Eye and Ear will segment the network quarantining unprotected third party devices. The Eye and Ear will work with the Digital Health Branch and other health services to develop processes that monitor third party vendor's compliance with data security requirements.

Yours sincerely

Mark Petty

Mark Petty
Chief Executive Officer

Auditor-General's reports tabled during 2018–19

Report title	Date tabled
Local Government Insurance Risks (2018–19:1)	July 2018
Managing the Municipal and Industrial Landfill Levy (2018–19:2)	July 2018
School Councils in Government Schools (2018–19:3)	July 2018
Managing Rehabilitation Services in Youth Detention (2018–19:4)	August 2018
Police Management of Property and Exhibits (2018–19:5)	September 2018
Crime Data (2018–19:6)	September 2018
Follow up of Oversight and Accountability of Committees of Management (2018–19:7)	September 2018
Delivering Local Government Services (2018–19:8)	September 2018
Security and Privacy of Surveillance Technologies in Public Places (2018–19:9)	September 2018
Managing the Environmental Impacts of Domestic Wastewater (2018–19:10)	September 2018
Contract Management Capability in DHHS: Service Agreements (2018–19:11)	September 2018
State Purchase Contracts (2018–19:12)	September 2018
Auditor-General's Report on the Annual Financial Report of the State of Victoria: 2017–18 (2018–19:13)	October 2018
Results of 2017–18 Audits: Local Government (2018–19:14)	December 2018
Professional Learning for School Teachers (2018–19:15)	February 2019
Access to Mental Health Services (2018–19:16)	March 2019
Outcomes of Investing in Regional Victoria (2018–19:17)	May 2019
Reporting on Local Government Performance (2018–19:18)	May 2019
Local Government Assets: Asset Management and Compliance (2018–19:19)	May 2019
Compliance with the Asset Management Accountability Framework (2018–19:20)	May 2019
Security of Government Buildings (2018–19:21)	May 2019
Security of Water Infrastructure Control Systems (2018–19:22)	May 2019

VAGO

Victorian Auditor-General's Office

All reports are available for download in PDF and HTML format on our website www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au