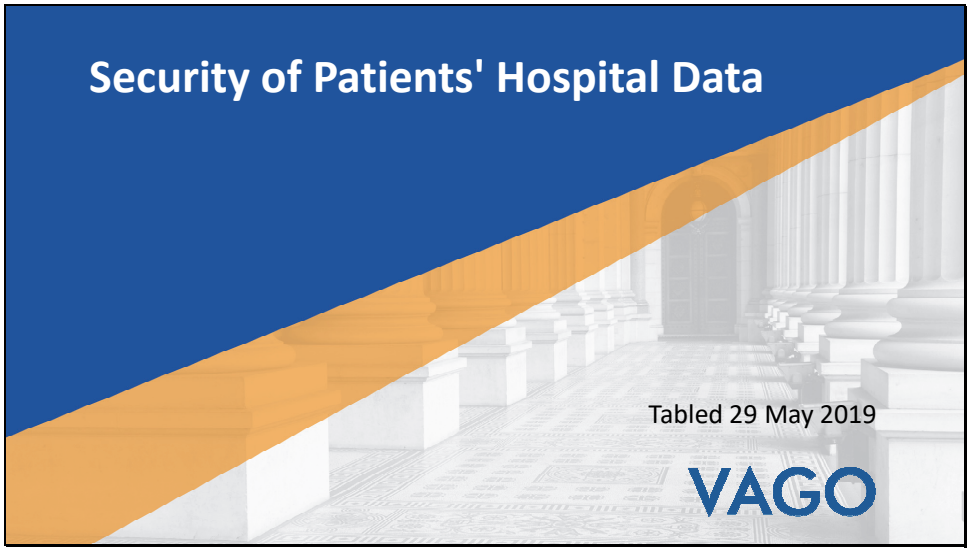
Slide 1



This presentation provides an overview of the Victorian Auditor-General's report *Security of Patients' Hospital Data.*

Slide 2

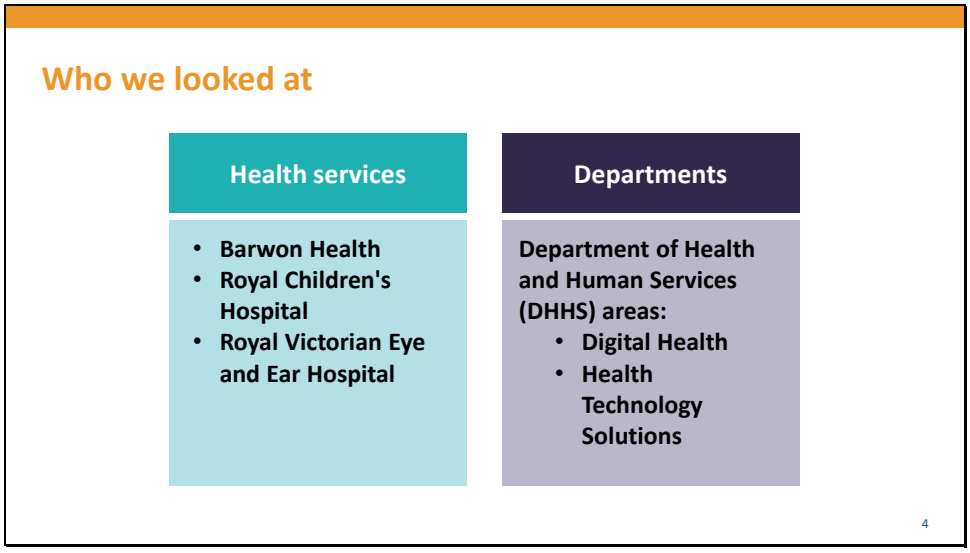
Public hospitals are increasingly using information and communications technology (ICT) to deliver healthcare and to capture and store patient information.

Digital records are valuable in improving patient care, however, health services need to manage the risk of a cybersecurity breach, which could steal patient information and disable health services' ICT systems, preventing staff from accessing patient information.

Slide 3

In this audit, we assessed whether health services are taking effective steps to protect patient data.

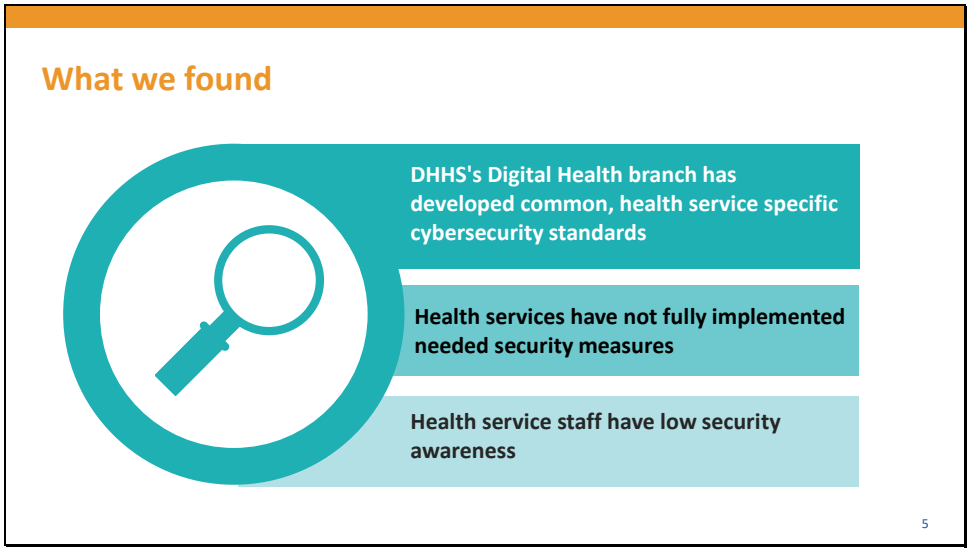
Slide 4



We audited Barwon Health, the Royal Children's Hospital and the Royal Victorian Eye and Ear Hospital.

We also examined two different areas of the Department of Health and Human Services (DHHS)—their Digital Health branch and Health Technology Solutions—and how they are supporting health services.

Slide 5

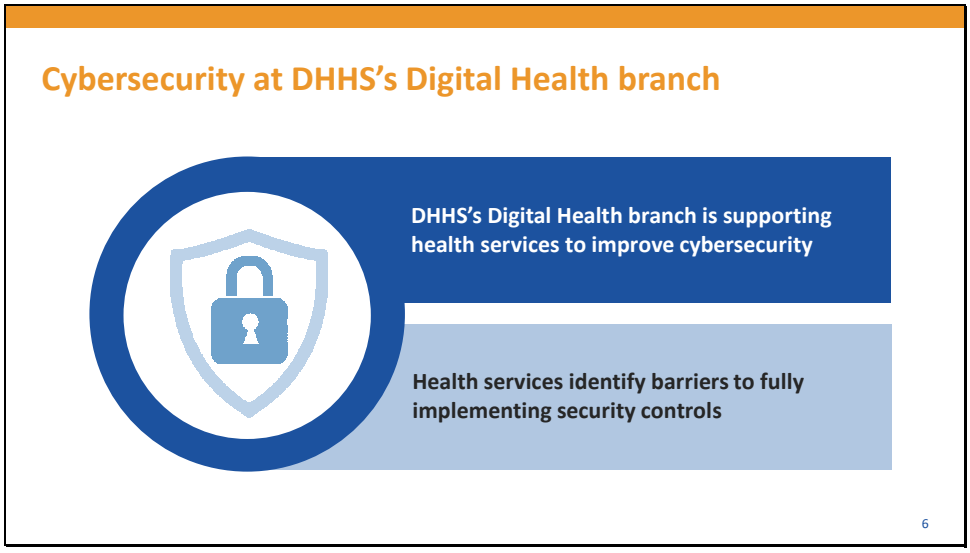


DHHS's Digital Health branch has filled an important gap in the sector by developing common, health service specific cybersecurity standards and acting as the central point for advice and support.

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.

Our testing identified key weaknesses in health services' approach to data security, particularly in relation to staff awareness and network monitoring.

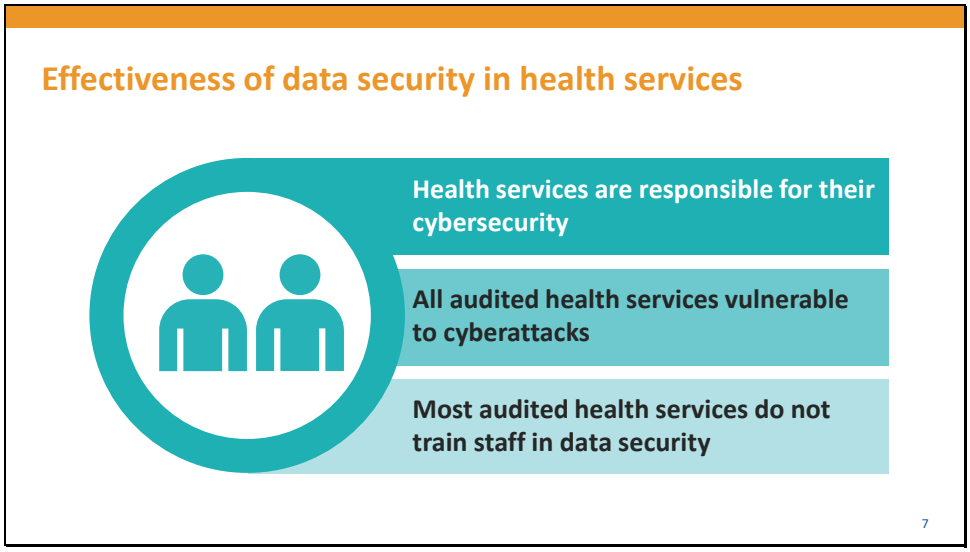
Slide 6



DHHS's Digital Health branch works to improve cybersecurity in the sector by developing guidance materials, running awareness and training sessions, and funding ICT infrastructure upgrades.

We found that DHHS's Digital Health branch has completed an effective program of work to improve health services' approach to data security. However, health services identify key barriers to fully implementing the controls, such as lack of cybersecurity staff and insufficient resources for ICT projects.

Slide 7



While DHHS has developed a clear roadmap to improve cybersecurity, ultimately it is the responsibility of health services to implement those improvements.

We conducted scenario-based penetration testing at the audited health services and found that all were vulnerable to attacks that could steal or alter patient data. Key weaknesses include inadequate user access controls, weak passwords and limited monitoring to detect suspicious behavior on their ICT network.

Additionally, we found that most audited health services do not train staff to recognise suspicious behaviour, or to practice basic security such as locking computers, not clicking on suspicious links, or protecting their security access passes.

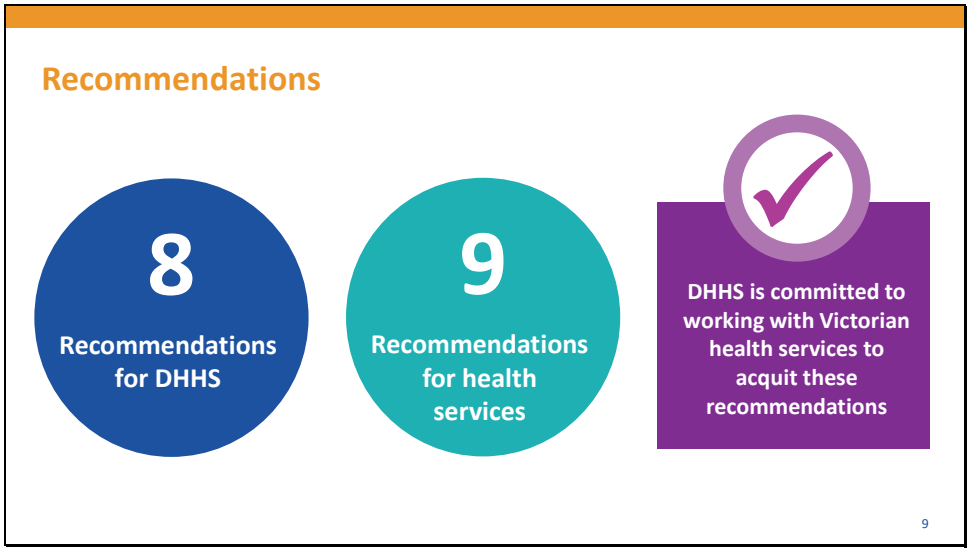
Slide 8

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. Health Technology Solutions is the key provider of outsourced ICT business systems to Victorian health services.

Despite being part of DHHS, Health Technology Solutions has made no progress in implementing Digital Health's cybersecurity controls since they were introduced in March 2017 and has similar security weaknesses to Victorian health services.

We also found issues with vendor management at two audited health services. At one health service, we gained access to patient data in a system managed by a third-party vendor. At another, we found confusion around whether the responsibility for data security sat with the third party or the hospital.

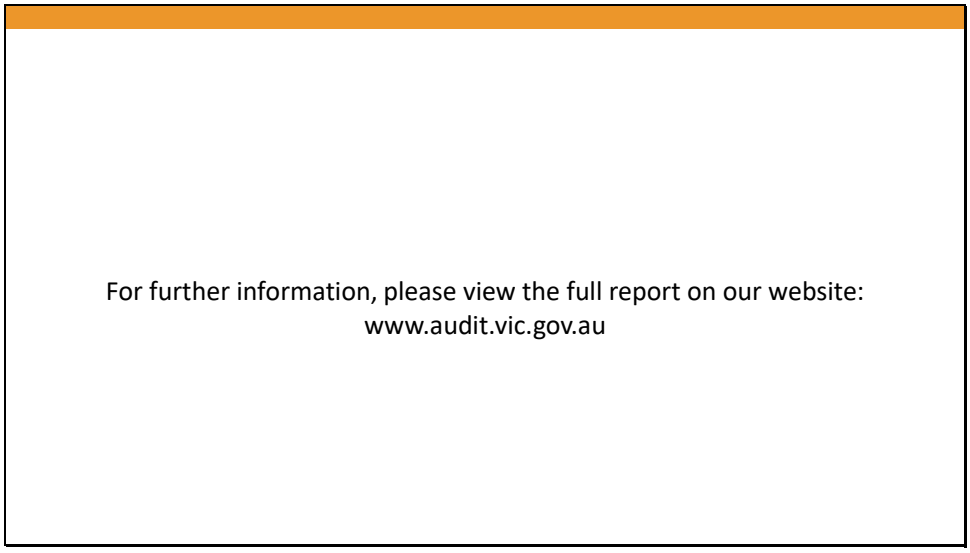
Slide 9



We made eight recommendations for DHHS around continuing support for the Digital Health cybersecurity program and nine recommendations for health services.

DHHS has committed to working with Victorian health services to acquit these recommendations.

Slide 10



For further information, please see the full report of this audit on our website, www.audit.vic.gov.au.