

# Case Study – Health Care Sector

April 2024



## WRC Case study brief: Health Care Sector:

### Topic: Strengthening cyber security in Queensland's healthcare network with the Essential Eight Audit

#### Health care sector overview

Cyber security threats are escalating in healthcare organisations, due to the valuable nature of patient data and integrated technology systems. The Australian Signals Directorate's (ASD) industry.

#### Case study

A regional healthcare network in Queensland, Australia, with over 50,000 patients across multiple hospitals and clinics, faced mounting challenges in cyber security, particularly in protecting patient data and complying with the Australian Privacy Act 1988.


#### Challenge

The network's dated IT infrastructure, siloed operations, and limited cyber security expertise left it exposed to modern cyber threats. The surge in ransomware attacks within the sector highlighted the need for proactive defence measures.

#### Solution

In response, the Regional Healthcare Network partnered with White Rook Cyber to conduct a tailored Essential Eight audit. This audit was pivotal in the network's cyber security improvement efforts, focusing on:

- **Application hardening:** Evaluating and reinforcing critical healthcare applications (EMR, billing systems).
- **Patch management:** Implementing a robust process for timely software updates.
- **Multi-factor authentication (MFA):** Enabling MFA across all patient data access points.
- **Application whitelisting:** Restricting device operations to pre-approved software devices.
- **Endpoint protection:** Deploying sophisticated solutions to detect and prevent malware.
- **Data backup and recovery:** Regularly backing up patient data and ensuring effective recovery strategies.
- **User awareness training:** Educating staff on cyber security best practices and threat detection.

- 
- **Incident response planning:** Developing a comprehensive plan for containment and resolution of incidents.

### **Outcomes**

- The audit resulted in a significant reduction in the network's vulnerability to attacks.
- Compliance with data protection laws improved, ensuring adherence to the Australian Privacy Act.
- The introduction of MFA strengthened defences against unauthorised access attempts.
- Employee training programs enhanced the overall cyber security awareness within the network.

### **Key Findings**

- Tailoring the Essential Eight framework to the unique requirements of healthcare data security is essential for optimal effectiveness.
- Regular audits and staff training form a comprehensive defence against cyber threats.
- Continuous monitoring and improvements are essential to maintain a resilient cyber security posture.

### **Future Initiatives**

- The Healthcare Network plans to integrate real-time threat intelligence into its cyber security strategy.
- Continual vulnerability assessments and penetration testing will be employed to reinforce system defences.
- The success of the Essential Eight audit has motivated the healthcare network to evaluate additional cyber security frameworks.

### **Conclusion**

This case study validates the applicability of the Essential Eight framework in enhancing healthcare cyber security. By prioritising the protection of patient data and implementing a culture of cyber security awareness, the network has significantly reduced its risks profile and strengthened its cyber security infrastructure.

