

SECURITY

Solutions Partner for Security Designation

HEALTHCARE

Determine Industry Requirements

What Are We Assessing?

The first step is to identify which industries are ideal for our Security solution, which we have done using data available to us, as outlined in Lesson 2. We will now determine the specific requirements of these solutions by industry. We look at this from three perspectives – partner, customer and the results delivered.



What Is the Information Provided?

- **Partner oriented:** Provides information on the technical outcomes anticipated within this industry and outlines the required functionalities to achieve them.
- **Customer oriented:** Communicates with the customer about achievable outcomes in plain language, providing appropriate context messaging.
- **Outcome oriented:** Communicates to the customer the results or outcomes they will gain after transitioning to your new solution.

Why Is This Information Important to Understand and Use?

To create a successful solution, it is essential to understand the primary priorities of the industry, as they are crucial for meeting customer needs. This step clarifies our solution's goals, allowing us to identify the necessary technical components in our next lesson.

Partner Oriented



What are top 10 security priorities faced by the Healthcare industry in Australia. List the reason and requirement. Visualise in a table. Do not list numbers.



Top 10 Security Priorities in the Australian Healthcare Industry

Priority	Reason	Requirement
Data Encryption	Protect sensitive patient information from unauthorised access	Advanced encryption standards and protocols
Access Control	Ensure only authorised personnel can access patient data	Multi-factor authentication and role-based access controls
Network Security	Prevent cyber-attacks on healthcare networks	Firewalls, intrusion detection/prevention systems
Data Backup and Recovery	Safeguard patient data against data loss and disasters	Regular backups and robust disaster recovery plans
Endpoint Security	Protect devices connected to the healthcare network	Antivirus software, endpoint detection and response tools
Compliance Monitoring	Ensure adherence to healthcare regulations and standards	Continuous monitoring and auditing systems
Employee Training	Prevent security breaches due to human error	Regular cybersecurity awareness and training programs
Incident Response	Quickly address and mitigate security incidents	Comprehensive incident response plans and teams
Third-Party Risk Management	Assess and mitigate risks posed by third-party vendors	Vendor risk assessments and regular security reviews
Physical Security	Protect physical access to healthcare facilities and equipment	Surveillance systems, access controls, and security personnel

Customer Oriented



What are top 10 security priorities faced by the Healthcare industry in Australia. List the reason and requirement. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.



Top 10 Security Priorities in the Australian Healthcare Industry

Priority	Reason	Requirement
Data Privacy	To protect patients' personal and medical information	Strict data handling policies and secure storage methods
Cybersecurity	To prevent cyber-attacks and protect digital records	Regular software updates and strong passwords
Employee Training	To ensure staff know how to manage security threats	Regular training sessions on security awareness
Incident Response	To quickly deal with and reduce the impact of security incidents	Well-prepared incident response plans and teams
Third-Party Risk Management	To avoid risks from external vendors and partners	Vendor risk assessments and regular security reviews
Physical Security	To prevent unauthorised access to healthcare facilities and equipment	Surveillance systems, access controls, and security personnel
Network Security	To protect internal networks from unauthorised access	Firewalls and secure Wi-Fi connections
Application Security	To safeguard software applications used in healthcare	Regular application testing and secure coding practices
Access Control	To ensure only authorised personnel access sensitive information	Role-based access controls and user authentication
Patient Safety	To ensure the safety and well-being of patients	Protocols for emergency situations and secure patient handling procedures

Outcome Oriented



What are top 10 security priorities faced by the Healthcare industry in Australia. List the reason and security outcomes delivered. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.



Top 10 Security Priorities in the Australian Healthcare Industry

Priority	Reason	Security Outcomes
Patient Data Protection	To safeguard patient records and personal information	Enhanced privacy and compliance with regulatory standards
Cyber Attack Prevention	To prevent unauthorised access and data breaches	Increased security against malware and phishing
System Integrity	To ensure the reliability of healthcare systems	Continuous operation without disruptions or tampering
Access Control Management	To ensure only authorised personnel access sensitive information	Restricted access based on roles and authentication
Secure Communication	To protect communication channels among healthcare providers	Confidential and secure sharing of patient information
Device Security	To protect medical devices from cyber threats	Safe and secure operation of all medical equipment
Application Security	To safeguard software applications used in healthcare	Regular application testing and secure coding practices
Incident Response	To quickly address and mitigate security incidents	Effective handling of security breaches and minimised impact
Employee Training	To educate staff about security best practices	Enhanced awareness and reduced risk of human error
Patient Safety	To ensure the safety and well-being of patients	Protocols for emergency situations and secure patient handling procedures

Continue on your path to achieving a Microsoft Partner for Security designation.

Visit dickerdata.com.au/Microsoft or contact the Dicker Data Microsoft Team

(02) 8556 8061 Microsoft.Sales@DickerData.com.au