Hills Shire Care Private Hospital - Cybersecurity & Privacy Audit Checklist

Date: 01 July 2024

Version: 1.0

Scope: This checklist covers the cybersecurity and privacy compliance of Hills Shire Care Private Hospital, referencing ISO/IEC 27001, 27002, 27005, 27035, 27018, NIST CSF, Cyber Security Act 2024, 2023-2030 Australian Cyber Security Strategy, GDPR, Australian Privacy Principles (APPs), Privacy Act, and other relevant Australian healthcare privacy regulations.

I. Governance and Risk Management

- **1.1 Information Security Policy:**
  - ○ Is a comprehensive Information Security Policy in place, reviewed, and approved at least annually?
  - ○ Does the policy align with the hospital's overall business strategy and objectives?
  - ○ Is the policy communicated effectively to all staff, contractors, and third parties?
  - ○ Does the policy define roles and responsibilities related to information security?
- **1.2 Risk Management:**
  - ○ Is a formal risk management process implemented based on ISO 27005?
  - ○ Are regular risk assessments conducted to identify, analyze, and evaluate security risks?
  - ○ Are risk treatments (acceptance, mitigation, transfer, avoidance) documented and implemented?
  - ○ Is risk ownership assigned and accountability enforced?
  - ○ Are residual risks documented and accepted by management?
- **1.3 Regulatory Compliance:**
  - ○ Is there a documented process to identify and comply with applicable laws and regulations (e.g., Cyber Security Act 2024, Australian Cyber Security Strategy, GDPR, Privacy Act, APPs, My Health Records Act)?
  - ○ Is compliance monitored and reported regularly to management?
  - ○ Are compliance gaps identified and addressed promptly?
- **1.4 Governance Structure:**
  - ○ Is there a clear governance structure for cybersecurity and privacy?
  - ○ Are roles and responsibilities clearly defined and understood?
  - ○ Is there adequate management oversight of cybersecurity and privacy risks?

II. Security Controls

- **2.1 Access Control:**

  - ○ Is a robust access control policy implemented, based on the principle of least privilege?
  - ○ Are user access rights regularly reviewed and revoked when no longer required?
  - ○ Is multi-factor authentication (MFA) implemented for all sensitive systems and data?
  - ○ Are strong password policies enforced (e.g., password complexity, length, rotation)?

- **2.2 Data Security and Privacy:**

  - ○ Is data classified according to sensitivity levels?
  - ○ Are appropriate security controls implemented for each data classification level (e.g., encryption, access restrictions)?
  - ○ Is data encryption in transit and at rest implemented, as per the Encryption Policy?
  - ○ Are data retention and destruction policies in place and adhered to?
  - ○ Are data backups performed regularly and tested for restorability?
  - ○ Are there procedures in place to handle data breaches, including notification requirements?

- **2.3 Physical Security:**

  - ○ Are physical security controls implemented to protect IT infrastructure and sensitive areas (e.g., data centers, server rooms)?
  - ○ Are access controls in place to restrict physical access to these areas?
  - ○ Are surveillance systems (e.g., CCTV) used and monitored?
  - ○ Are visitor management procedures in place and enforced?

- **2.4 Network Security:**

  - ○ Are firewalls configured and managed effectively to control network traffic?
  - ○ Is intrusion detection/prevention systems (IDS/IPS) implemented and monitored?
  - ○ Are network segmentation strategies in place to isolate sensitive systems?
  - ○ Are secure network protocols used (e.g., HTTPS, VPNs)?

- **2.5 Endpoint Security:**

  - ○ Is anti-malware software installed and updated on all endpoints?
  - ○ Are endpoint security configurations managed centrally?
  - ○ Are regular vulnerability scans conducted on endpoints?
  - ○ Is a mobile device management (MDM) solution implemented for mobile devices accessing hospital systems?

- **2.6 System Security:**

  - ○ Are operating systems and applications patched regularly?
  - ○ Are secure configurations applied to systems and applications?
  - ○ Are vulnerability scans conducted regularly on systems and applications?
  - ○ Are secure coding practices followed for in-house developed applications?

- **2.7 Third-Party Security:**

  - ○ Are third-party security risks assessed and managed?
  - ○ Are security requirements included in contracts with third-party vendors?

○ Is third-party access to hospital systems monitored and controlled?

III. Security Operations

- **3.1 Security Monitoring:**

  ○ Are security events logged and monitored?
  ○ Are security alerts investigated and responded to promptly?
  ○ Is a Security Information and Event Management (SIEM) system used?

- **3.2 Incident Management:**

  ○ Is an incident response plan in place and tested regularly?
  ○ Are incident response procedures documented and followed?
  ○ Is incident response training provided to staff?

- **3.3 Change Management:**

  ○ Is a change management process in place to control changes to IT systems?
  ○ Are changes reviewed and approved before implementation?
  ○ Are changes tested before being deployed to production?

- **3.4 Business Continuity and Disaster Recovery:**

  ○ Are business continuity and disaster recovery plans in place and tested regularly?
  ○ Do these plans cover critical systems and data?
  ○ Are backup and recovery procedures documented and tested?

IV. Awareness and Training

- **4.1 Security Awareness Training:**

  ○ Is regular security awareness training provided to all staff, contractors, and third parties?
  ○ Does the training cover relevant security policies and procedures?
  ○ Does the training address current cybersecurity threats and best practices?
  ○ Is the effectiveness of the training measured and evaluated?

- **4.2 Role-Based Training:**

  ○ Is specialized security training provided to staff with specific security responsibilities (e.g., system administrators, security analysts)?

V. Compliance with Specific Regulations

- **5.1 GDPR:**

  ○ If processing personal data of EU residents, are GDPR requirements met (e.g., data subject rights, data protection impact assessments)?

- **5.2 Australian Privacy Principles (APPs):**

  ○ Are all 13 APPs adhered to? Focus on collection, use, disclosure, quality, security, and access/correction of personal information.

- **5.3 My Health Records Act 2012:**
    - ○ Are specific requirements regarding My Health Records access and security followed?
- **5.4 Cyber Security Act 2024:**
    - ○ Are the hospital's systems designated as critical infrastructure, and if so, are the relevant obligations under the Act fulfilled?
- **5.5 Australian Cyber Security Strategy 2023-2030:**
    - ○ Are the hospital's cybersecurity practices aligned with the goals and objectives of the Strategy?

VI. Hospital-Specific Considerations

- **6.1 Patient Booking System:**
    - ○ Is the Patient Booking System secure and compliant with relevant regulations?
    - ○ Are access controls implemented to protect patient data within the system?
- **6.2 Ambulance Patient Data Handling:**
    - ○ Are secure procedures in place for handling patient data received from ambulances?
- **6.3 Pharmacy Medication Security:**
    - ○ Are security controls implemented to protect medication information and prevent unauthorized access?
- **6.4 Telehealth Security:**
    - ○ Are telehealth consultations conducted securely, protecting patient privacy and confidentiality?

VII. Audit Evidence and Reporting

- Documentation review of policies, procedures, risk assessments, incident reports, training records, and system configurations.
- Interviews with staff responsible for cybersecurity and privacy.
- Observation of security practices.
- Technical testing of security controls (e.g., vulnerability scanning, penetration testing).

This checklist should be used as a guide for the audit team. Each item should be thoroughly investigated, and evidence should be gathered to support the audit findings. Any identified gaps or weaknesses should be documented and reported to management, along with recommendations for remediation. The audit report should provide a clear and concise summary of the hospital's cybersecurity and privacy posture, including its level of compliance with relevant regulations and standards.