Hills Shire Care Private Hospital Cybersecurity & Privacy Audit Action Plan

Date: 01 July 2024

Version: 1.0

Prepared by: [Your Name/Team Name]

1. Introduction

This action plan outlines the audit procedures for Hills Shire Care Private Hospital's cybersecurity and privacy compliance, aligning with 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.

2. Audit Scope

The audit will cover the following areas:

- **Information Security Policies and Procedures:** Review and evaluate the effectiveness of existing policies and procedures.
- **Data Governance:** Assess data classification, access control, retention, and destruction practices.
- **Incident Response:** Evaluate the incident reporting and response mechanisms.
- **Physical Security:** Assess physical security controls for facilities, data centers, and equipment.
- **Network Security:** Evaluate firewall management, network segmentation, and intrusion detection/prevention systems.
- **Endpoint Security:** Assess malware protection, vulnerability management, and mobile device management.
- **Third-Party Risk Management:** Review the security posture of third-party vendors and partners.
- **Compliance with Relevant Regulations:** Verify compliance with all applicable laws and regulations.
- **Security Awareness Training:** Evaluate the effectiveness of security awareness training programs.

3. Audit Methodology

The audit will utilize a combination of the following methods:

- **Document Review:** Examination of policies, procedures, and other relevant documentation.
- **Interviews:** Gathering information from key personnel across different departments.
- **Technical Assessments:** Vulnerability scanning, penetration testing, and security configuration reviews.
- **Observations:** On-site observation of security practices and procedures.

4. Audit Schedule

Activity	Start Date	End Date	Team Member(s)
Planning and Preparation	08 July 2024	12 July 2024	[Team Member A]
Document Review	15 July 2024	19 July 2024	[Team Member B]
Interviews	22 July 2024	26 July 2024	[Team Member C]
Technical Assessments	29 July 2024	02 Aug 2024	[Team Member D]
Observations	05 Aug 2024	09 Aug 2024	[Team Member E]
Report Drafting	12 Aug 2024	16 Aug 2024	[Team Member A]
Report Review and Finalization	19 Aug 2024	23 Aug 2024	[Team Lead]

5. Detailed Audit Plan

5.1. Information Security Policies and Procedures

- **Objective:** Verify the completeness, adequacy, and implementation of information security policies and procedures.
- **Activities:**
    - ○ Review all relevant policies and procedures provided (Acceptable Use, Access Control, etc.).
    - ○ Compare policies with industry best practices (ISO 27001, NIST CSF).
    - ○ Verify policy dissemination and acknowledgement by staff.
- **Deliverables:** Gap analysis report, recommendations for policy improvements.

5.2. Data Governance

- **Objective:** Assess the effectiveness of data governance practices.
- **Activities:**
    - ○ Review Data Classification Policy and its implementation.
    - ○ Evaluate access controls to patient data.
    - ○ Assess data retention and destruction procedures.
    - ○ Verify compliance with APPs and GDPR regarding data subject rights.
- **Deliverables:** Data governance assessment report, recommendations for improvement.

5.3. Incident Response

- **Objective:** Evaluate the incident reporting and response capabilities.
- **Activities:**
    - ○ Review Incident Response Policy and Procedures.
    - ○ Conduct a tabletop exercise to simulate a data breach scenario.
    - ○ Evaluate the effectiveness of communication and escalation procedures.
- **Deliverables:** Incident response assessment report, recommendations for improvement.

5.4. Physical Security

- **Objective:** Assess physical security controls.
- **Activities:**
    - ○ Inspect physical access controls to data centers and other sensitive areas.

    - ○ Review surveillance systems and procedures.
    - ○ Evaluate environmental controls (fire suppression, power backup).

- **Deliverables:** Physical security assessment report, recommendations for improvement.

5.5. Network Security

- **Objective:** Evaluate network security posture.
- **Activities:**
    - ○ Review Firewall Management Policy and configurations.
    - ○ Assess network segmentation and access controls.
    - ○ Evaluate intrusion detection/prevention system effectiveness.
- **Deliverables:** Network security assessment report, recommendations for improvement.

5.6. Endpoint Security

- **Objective:** Assess endpoint security controls.
- **Activities:**
    - ○ Review Malware Protection Policy and software deployment.
    - ○ Conduct vulnerability scanning and penetration testing.
    - ○ Evaluate Mobile Device Management Policy and its implementation.
- **Deliverables:** Endpoint security assessment report, recommendations for improvement.

5.7. Third-Party Risk Management

- **Objective:** Evaluate the management of third-party security risks.
- **Activities:**
    - ○ Review Third-Party Risk Management Policy.
    - ○ Assess the security posture of key third-party vendors.
    - ○ Review contracts and service level agreements for security requirements.
- **Deliverables:** Third-party risk assessment report, recommendations for improvement.

5.8. Compliance with Relevant Regulations

- **Objective:** Verify compliance with applicable laws and regulations.
- **Activities:**
    - ○ Review compliance documentation and evidence.
    - ○ Assess adherence to Australian Privacy Principles, GDPR, Cyber Security Act 2024, and other relevant regulations.
- **Deliverables:** Compliance assessment report, recommendations for remediation.

5.9. Security Awareness Training

- **Objective:** Evaluate the effectiveness of security awareness training programs.
- **Activities:**
    - ○ Review Security Awareness Training Policy and materials.
    - ○ Assess staff knowledge of security policies and procedures.

    - Evaluate the frequency and effectiveness of training programs.

- **Deliverables:** Security awareness training assessment report, recommendations for improvement.

6. Reporting

A comprehensive audit report will be prepared, detailing the findings, risks, and recommendations. The report will be submitted to the Hospital Director, Head of IT, COO, Cybersecurity Head, and Compliance Officer by 23 August 2024. The report will follow a standard format including an executive summary, detailed findings for each audit area, a risk assessment for identified vulnerabilities, and prioritized remediation actions.

7. Communication

Regular communication will be maintained with the hospital management throughout the audit process. Weekly progress reports will be provided, and any critical findings will be communicated immediately.

8. Resources

The audit team will have access to all necessary resources, including policy documents, system access, and personnel interviews. The hospital's IT department will provide technical support as needed.

9. Follow-up

After the audit report is submitted, a follow-up meeting will be scheduled to discuss the findings and agree on remediation actions. The hospital management will be responsible for implementing the recommended actions, and a follow-up audit may be conducted to verify implementation.