Gap Analysis Report - Hills Shire Care Private Hospital

Date: 01 July 2024

1. Introduction

This gap analysis report assesses the cybersecurity and privacy compliance posture of Hills Shire Care Private Hospital against a set of established standards and frameworks. The analysis considers the hospital's provided policy documents and compares them to the requirements of ISO/IEC 27001, 27002, 27005, 27035, 27018, NIST CSF, the Cyber Security Act 2024, the 2023-2030 Australian Cyber Security Strategy, GDPR, Australian Privacy Principles (APPs), the Privacy Act, and other relevant Australian healthcare privacy regulations. This report identifies gaps where policy documents do not fully address the requirements of these standards, providing recommendations for remediation and improvement.

2. Scope

This analysis covers the following areas:

- **Information Security Management System (ISMS):** Based on ISO/IEC 27001:2022 requirements.
- **Risk Management:** Addressing ISO/IEC 27005:2018 and the hospital's Risk Management Policy.
- **Incident Management:** Considering ISO/IEC 27035:2016, Incident Response Policy and procedures.
- **Data Privacy:** Covering ISO/IEC 27018:2019, GDPR, APPs, the Privacy Act, and related Australian healthcare regulations, along with relevant hospital policies.
- **Physical Security:** Reviewing Facility Security Policy, Data Center Security Procedures, Visitor Management Policy.
- **Cybersecurity Controls:** Based on ISO/IEC 27002:2013, NIST CSF, and NIST SP 800-53 Rev. 4, and relevant hospital policies.
- **Compliance with Cyber Security Act 2024 and Australian Cyber Security Strategy 2023-2030.**

3. Methodology

The gap analysis was conducted by reviewing the provided policy documents and comparing them against the requirements of the specified standards and frameworks. Gaps were identified where policies were missing, incomplete, or insufficient to meet the requirements.

4. Findings

4.1 Information Security Management System (ISMS)

- **Gap:** While the Information Security Policy provides a high-level overview, it lacks the required detail for a fully implemented ISMS as per ISO 27001. Specifically, the policy does not define roles and responsibilities clearly, documentation requirements, or processes for internal audits and management review.
- **Recommendation:** Develop a dedicated ISMS manual outlining all aspects of the ISMS,

including roles, responsibilities, procedures, and documentation requirements. Define clear ownership of information assets and security responsibilities.

4.2 Risk Management

- **Gap:** The Risk Management Policy lacks specific details on risk assessment methodologies, risk appetite, and risk treatment processes. It doesn't adequately address the integration of risk management into the overall ISMS.
- **Recommendation:** Enhance the Risk Management Policy to include details on risk assessment methodologies (e.g., qualitative, quantitative), risk acceptance criteria, and procedures for risk treatment (e.g., mitigation, transfer, acceptance, avoidance). Define the frequency of risk assessments and how risk management activities are integrated into the change management process.

4.3 Incident Management

- **Gap:** The Incident Response Policy is high-level and lacks detailed procedures for incident identification, containment, eradication, recovery, and post-incident activity. It doesn't address specific incident types relevant to healthcare, such as ransomware or medical device compromise. The connection between incident response and business continuity/disaster recovery is unclear.
- **Recommendation:** Develop comprehensive incident management procedures, including playbooks for specific incident scenarios, escalation paths, communication protocols, and forensic analysis processes. Establish clear roles and responsibilities for the incident response team. Integrate incident management with business continuity and disaster recovery plans.

4.4 Data Privacy

- **Gap:** While the hospital has policies addressing Australian Privacy Principles (APPs), GDPR, and the Privacy Act, there is a lack of a unified data privacy policy that comprehensively addresses all relevant regulations. Specific gaps include inadequate procedures for data subject requests, limited detail on data retention and disposal practices specifically for different data types (e.g., medical records, financial information), and lack of clarity around cross-border data transfers. The Patient Data Privacy Policy should include explicit mentions of My Health Record system security and interoperability considerations.
- **Recommendation:** Create a consolidated data privacy policy encompassing all relevant regulations, including APPs, GDPR, Privacy Act, and My Health Record specific provisions. Implement procedures for handling data subject requests, data breach notifications, and cross-border data transfers. Detail data retention and destruction procedures in alignment with regulatory requirements, including secure disposal methods for physical and electronic records. Ensure specific considerations for sensitive health information are addressed. Review and update consent procedures related to telehealth services.

4.5 Physical Security

- **Gap:** The Facility Security Policy does not adequately address environmental controls within the data center or other sensitive areas (e.g., temperature, humidity). Visitor Management Policy needs more specifics on visitor access levels and escort requirements. Data Center Security Procedures lack detail on physical access logs, surveillance systems management, and maintenance activities.
- **Recommendation:** Include specific environmental control requirements in the Facility

Security Policy. Enhance the Visitor Management Policy with clear visitor categorization, access control measures, and escort procedures. Expand the Data Center Security Procedures to incorporate detailed logging practices for physical access, management of surveillance systems (including data retention), and secure maintenance procedures.

4.6 Cybersecurity Controls

- **Gap:** Several policies lack sufficient detail and alignment with best practices. Examples:
    - **Access Control Policy:** Does not adequately address role-based access control or privileged access management.
    - **Backup and Recovery Policy:** Lacks specifics on backup frequency, retention periods, and restoration testing. Consider different data types and criticality for backup strategies.
    - **Change Management Policy:** Does not address emergency changes and their approval process.
    - **Encryption Policy:** Lacks details on encryption standards and key management practices.
    - **Firewall Management Policy:** Requires more specifics on rule management, logging, and monitoring.
    - **Log Management Policy:** Lacks details on log retention, analysis, and correlation.
    - **Malware Protection Policy:** Does not cover specific requirements for medical devices or IoT systems.
    - **Mobile Device Management Policy:** Needs further detail on BYOD policies and security requirements for mobile devices accessing patient data.
    - **Network Security Policy:** Requires stronger segmentation strategies, intrusion detection/prevention systems (IDPS) requirements, and vulnerability scanning procedures.
    - **Password Management Policy:** Password complexity requirements are not stringent enough. Implement multi-factor authentication (MFA).
    - **Security Awareness Training Policy:** Lacks details on training frequency, content, and effectiveness measurement. Include phishing and social engineering awareness training.
    - **Security Events Monitoring Policy:** Lacks details on security information and event management (SIEM) implementation and alert thresholds.
    - **Third-Party Risk Management Policy:** Needs a defined process for due diligence, risk assessments of third-party vendors, and ongoing monitoring.
- **Recommendation:** Review and enhance all listed policies to align with best practices from ISO 27002, NIST CSF, and NIST SP 800-53. Ensure controls are specific, measurable, achievable, relevant, and time-bound. Special attention should be paid to protecting medical devices and IoT systems due to their criticality in healthcare.

4.7 Compliance with Cyber Security Act 2024 and Australian Cyber Security Strategy 2023-2030

- **Gap:** While the Regulatory Compliance Policy mentions a commitment to compliance, it lacks specific procedures and controls demonstrating adherence to the Cyber Security Act 2024 and the Australian Cyber Security Strategy. Specifically, it does not address mandatory incident reporting requirements or requirements for critical infrastructure protection, if applicable.
- **Recommendation:** Update the Regulatory Compliance Policy to include specific

clauses addressing the Cyber Security Act 2024 and Australian Cyber Security Strategy 2023-2030. Implement procedures for mandatory incident reporting and demonstrate compliance with critical infrastructure regulations. Establish a process for staying updated on evolving regulatory requirements.

5. Conclusion

Hills Shire Care Private Hospital has a foundation of security and privacy policies. However, significant gaps must be addressed to achieve full compliance with the target standards and frameworks. This report highlights those gaps and provides recommendations for remediation. Implementing these recommendations will strengthen the hospital's security posture, protect sensitive patient data, and ensure compliance with relevant regulations.

6. Next Steps

- **Prioritize Gaps:** Prioritize the identified gaps based on risk and potential impact.
- **Develop Remediation Plan:** Develop a detailed remediation plan with timelines and assigned responsibilities.
- **Implement and Monitor:** Implement the remediation plan and continuously monitor its effectiveness.
- **Regular Review:** Establish a regular review cycle for all policies and procedures to ensure they remain current and effective.

This report should be used as a guide to improve the hospital's cybersecurity and privacy program. Regular updates and ongoing diligence are crucial in today's dynamic threat landscape.