Cybersecurity and Privacy Compliance Audit Report for Hills Shire Care Private Hospital

Date: 01 July 2024

1. Introduction

This report presents the findings of a cybersecurity and privacy compliance audit conducted for Hills Shire Care Private Hospital (HSCPH). The audit assessed the hospital's compliance with relevant standards and regulations, including 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 Australian healthcare-related privacy regulations. The audit was conducted by reviewing the provided policy and procedure documents and leveraging cybersecurity and privacy compliance expertise.

2. Executive Summary

HSCPH demonstrates a good foundation for cybersecurity and privacy compliance with a comprehensive set of policies covering many critical areas. However, gaps exist, requiring improvements to align fully with the specified standards and regulations. This report details these gaps and provides recommendations for remediation. A summary table of compliance levels against major standards is included in Section 8.

3. Scope

The audit scope encompasses the policies and procedures provided, focusing on their alignment with the identified standards and regulations. This includes evaluating the comprehensiveness, implementation, and effectiveness of these documents in addressing the requirements of each standard. The physical security assessment and technical configuration reviews were outside the scope of this document review-based audit.

4. Methodology

The audit methodology involved a thorough review of HSCPH's policies and procedures. Each document was analyzed against the control objectives and requirements of the relevant standards and regulations. The analysis considered the following aspects:

- **Coverage:** Does the policy address the specific requirements of the standard/ regulation?
- **Implementation:** Is there evidence that the policy is being implemented effectively? (This aspect relies on documentation and could not be fully validated in this desktop review.)
- **Effectiveness:** Are the controls defined in the policy likely to be effective in achieving the desired outcome? (Again, practical effectiveness could not be fully assessed in this review.)

5. Findings

The following sections detail the findings for each standard and regulation, providing a percentage of coverage and specific gaps identified. It's important to remember these

percentages are based on the *documented* policies and not observed practices.

5.1 ISO/IEC 27001:2022

- **Estimated Coverage:** 70%
- **Strengths:** HSCPH has established an Information Security Management System (ISMS) with documented policies addressing many of the mandatory clauses of ISO 27001. The policies on risk management, access control, incident response, and business continuity are particularly well-defined.
- **Gaps:** Further work is needed to document the risk assessment methodology and the selection of controls. The policy for addressing interested party requirements could be more explicitly defined. Evidence of management review and continuous improvement needs further documentation.

5.2 ISO/IEC 27002:2013

- **Estimated Coverage:** 65%
- **Strengths:** The provided policies cover many of the controls recommended in ISO 27002. The policies on asset management, access control, encryption, and human resources security are noteworthy.
- **Gaps:** Greater detail is required on physical security controls, environmental security, and communications security. More explicit procedures around data backups, system operations, and malware protection would strengthen compliance.

5.3 ISO/IEC 27005:2018

- **Estimated Coverage:** 60%
- **Strengths:** The Risk Management Policy provides a good starting point for risk assessment.
- **Gaps:** The policy lacks detailed processes for risk identification, analysis, and evaluation. It does not explicitly address risk treatment options or define risk acceptance criteria. Further documentation on the risk management framework and process is required.

5.4 ISO/IEC 27035:2016

- **Estimated Coverage:** 55%
- **Strengths:** The Incident Response Policy outlines a basic incident response process. The Incident Reporting Procedures supplement this policy.
- **Gaps:** The policies lack details on information gathering, evidence handling, and post-incident activities. The procedures could be improved by incorporating threat intelligence and threat modeling aspects.

5.5 ISO/IEC 27018:2019

- **Estimated Coverage:** 75%
- **Strengths:** The Data Protection Policy and the Australian Privacy Principles (APPs) Policy address many of the requirements of ISO 27018 regarding the protection of personally identifiable information (PII) in the cloud.
- **Gaps:** The policies should be more explicit about data subject rights and consent management. More details regarding data breach notification and transparency are needed.

5.6 NIST Cybersecurity Framework (CSF)

- **Estimated Coverage:** 60%
- **Strengths:** The policies address several aspects of the five NIST CSF functions: Identify, Protect, Detect, Respond, and Recover.
- **Gaps:** Mapping the existing policies to the NIST CSF subcategories would strengthen alignment. Additional policies and procedures are needed to address areas like vulnerability management, security awareness training, and communications planning.

5.7 Cyber Security Act 2024 and Australian Cyber Security Strategy 2023-2030

- **Estimated Coverage:** Difficult to quantify without specific requirements documented from the Acts.
- **Discussion:** The policies demonstrate a commitment to cybersecurity, aligning with the overall goals of these frameworks. However, further analysis and implementation of specific regulations within the Act and Strategy are required. This will likely involve updates to existing policies and potentially creating new ones.

5.8 GDPR and Australian Privacy Principles (APPs), Privacy Act

- **Estimated Coverage:** 70% for APPs, 60% for GDPR, similar for the related Privacy Act.
- **Strengths:** The GDPR Compliance Policy, Australian Privacy Principles (APPs) Policy, Data Protection Policy, and Privacy Policy address data subject rights, data breach notification, and data minimization. The inclusion of a Patient Consent and Communication Policy indicates attention to data use transparency.
- **Gaps:** Policies should include clear guidance on cross-border data transfers, especially in the context of GDPR. Mechanisms for data subject access requests, consent withdrawal, and data portability need to be documented and implemented. Further clarity is needed on data retention and destruction practices to comply with both frameworks. APP and GDPR principles need to be explicitly addressed, not just mentioned generally.

6. Recommendations

- **Gap Analysis and Remediation:** Conduct a detailed gap analysis against each standard and regulation. Develop and implement corrective actions to address identified gaps.
- **Policy Review and Updates:** Review and update all policies to ensure they are current, comprehensive, and aligned with the latest versions of the standards and regulations. Specifically, ensure GDPR articles and APP principles are mapped to policy implementation.
- **Implementation Evidence:** Document the implementation of policies and procedures. This can include records of training, risk assessments, incident response activities, and policy reviews.
- **Awareness Training:** Conduct regular security awareness training for all staff, including specific training on healthcare privacy regulations. Consider role-based security training as outlined in your provided procedure document, tailoring it to each department's data access needs.
- **Monitoring and Measurement:** Establish key performance indicators (KPIs) and metrics to measure the effectiveness of the ISMS. Conduct regular audits and reviews to monitor compliance and identify areas for improvement.
- **Dedicated Resource:** Consider appointing a dedicated Data Protection Officer (DPO) to oversee privacy compliance, especially given the sensitivity of patient health information.
- **Third-Party Risk Management:** Implement robust third-party risk management processes to ensure that all vendors and partners comply with the same security and

privacy standards as the hospital. Review and update the Third-Party Risk Management Policy, particularly focusing on data sharing agreements and due diligence processes.
- **Incident Response Plan Enhancement:** Develop a detailed incident response plan that incorporates threat intelligence, forensic analysis capabilities, and communication protocols for various stakeholders.

7. Conclusion

HSCPH has a commendable starting point for robust cybersecurity and privacy compliance. However, targeted improvements are required to achieve full compliance with the identified standards and regulations. Implementing the recommendations outlined in this report will significantly enhance the hospital's security posture and strengthen its ability to protect sensitive patient information. Regular monitoring, reviews, and updates are crucial to maintain ongoing compliance and adapt to the evolving threat landscape.

8. Compliance Summary Table

Standard/ Regulation	Estimated Coverage	Key Strengths	Key Gaps
ISO/IEC 27001:2022	70%	Documented ISMS, Risk Management, Access Control, Incident Response, BC/DR	Risk assessment methodology, interested party requirements, evidence of management review
ISO/IEC 27002:2013	65%	Asset management, Access Control, Encryption, Human Resources Security	Physical and environmental security, communications security, data backups, system operations
ISO/IEC 27005:2018	60%	Basic risk management policy exists	Risk identification, analysis, and evaluation; risk treatment options; risk acceptance criteria
ISO/IEC 27035:2016	55%	Basic incident response process and reporting procedures	Information gathering, evidence handling, post-incident activities, threat intelligence integration
ISO/IEC 27018:2019	75%	Data protection and APPs policies address many cloud PII protection requirements	Data subject rights, consent management, data breach notification, transparency
NIST CSF	60%	Policies address aspects of all five NIST CSF functions	Mapping to NIST CSF subcategories, vulnerability management, security awareness, communications planning
Cyber Security Act 2024/Australian Cyber Security Strategy	N/A (Difficult to quantify)	General alignment with cybersecurity principles	Implementation of specific regulations within these frameworks

GDPR/APPs/ Privacy Act	70% (APPs), 60% (GDPR/ Privacy Act)	Data subject rights, data breach notification, data minimization, patient consent policy	Cross-border data transfers, data subject access requests, data portability, data retention and destruction

This report serves as a snapshot of the current state of compliance based on the documentation provided. Ongoing monitoring and improvement are vital to maintain a strong security and privacy posture.