Hills Shire Care Private Hospital Cybersecurity and Privacy Compliance Improvements Report

Date: 01 July 2024

1. Introduction

This report outlines the results of a cybersecurity and privacy compliance audit conducted at Hills Shire Care Private Hospital. The audit assessed the hospital's compliance with relevant standards, including 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 all Australian healthcare-related privacy regulations. The report identifies areas for improvement in the hospital's policy documents and provides recommendations for enhancing compliance and quality.

2. Executive Summary

The audit revealed that while Hills Shire Care Private Hospital has a foundation of policies and procedures in place, several areas require improvement to achieve full compliance with the identified standards. Key areas for improvement include:

- **Specificity and Detail:** Many policies lack the necessary detail and specificity to provide actionable guidance.
- **Implementation Guidance:** Policies often fail to clearly outline implementation steps and responsibilities.
- **Alignment with Standards:** Several policies need updating to align with the latest versions of relevant standards, especially regarding incident response, data breach notification, and third-party risk management.
- **Training and Awareness:** The Security Awareness Training policy needs bolstering to address contemporary threats like phishing and social engineering.
- **Monitoring and Auditing:** The Audit and Monitoring policy should include more specific metrics and reporting requirements.

3. Detailed Improvement Recommendations

3.1 Acceptable Use Policy

- **Improvement:** Include specific examples of unacceptable use, such as accessing unauthorized websites, downloading illegal software, or using hospital resources for personal gain.
- **Reasoning:** Clarity reduces ambiguity and ensures staff understand the boundaries of acceptable behavior.

3.2 Access Control Policy

- **Improvement:** Define a clear process for granting, modifying, and revoking access privileges, incorporating the principle of least privilege.
- **Reasoning:** Formalized processes enhance control and reduce the risk of unauthorized access.

3.3 Ambulance Patient Data Handling Policy

- **Improvement:** Specify secure data transfer mechanisms between ambulances and the hospital system, addressing data encryption in transit and at rest.
- **Reasoning:** Ensures patient data confidentiality during transport.

3.4 Asset Management Policy

- **Improvement:** Include a comprehensive inventory process and define lifecycle management for all IT assets, including hardware and software.
- **Reasoning:** A clear asset lifecycle enhances security and reduces unnecessary costs.

3.5 Audit and Monitoring Policy

- **Improvement:** Specify audit frequency, the types of events to be audited, and reporting procedures. Include metrics for evaluating the effectiveness of security controls.
- **Reasoning:** Provides a structured approach to auditing and monitoring, enabling proactive identification of security issues.

3.6 Australian Privacy Principles (APPs) Policy

- **Improvement:** Map each APP to specific procedures within the hospital's operations. Provide practical examples of how the hospital complies with each principle.
- **Reasoning:** Demonstrates a clear understanding and implementation of the APPs.

3.7 Backup and Recovery Policy

- **Improvement:** Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical systems. Include detailed recovery procedures and regular testing requirements.
- **Reasoning:** Ensures business continuity in case of system failures.

3.8 Business Continuity and Disaster Recovery Policy

- **Improvement:** Expand the policy to include a broader range of disaster scenarios, including cyberattacks and pandemics. Define roles and responsibilities in a crisis.
- **Reasoning:** Prepares the hospital for a wider array of potential disruptions.

3.9 Change Management Policy

- **Improvement:** Detail the change approval process, including roles and responsibilities and procedures for rollback in case of failure.
- **Reasoning:** Reduces the risk of introducing vulnerabilities during system changes.

3.10 Compliance Management Policy

- **Improvement:** Develop a compliance monitoring and reporting framework, including key performance indicators (KPIs) and regular reporting to management.
- **Reasoning:** Provides a structured approach to managing and demonstrating compliance.

3.11 Data Breach Response Policy

- **Improvement:** Update the policy to align with the Notifiable Data Breaches (NDB) scheme and GDPR requirements. Include specific procedures for notification,

investigation, and remediation. Define clear timelines for action.
- **Reasoning:** Ensures a timely and effective response to data breaches.

3.12 Data Center Security Procedures

- **Improvement:** Enhance physical security measures, such as access control, surveillance, and environmental controls. Address data center redundancy and failover mechanisms.
- **Reasoning:** Protects critical infrastructure and data from unauthorized access and environmental threats.

3.13 Data Classification Policy

- **Improvement:** Develop a clear data classification scheme and implement labeling procedures. Link data classification to access control and data handling procedures.
- **Reasoning:** Facilitates appropriate handling and protection of sensitive data based on its classification.

3.14 Data Protection Policy

- **Improvement:** Consolidate data protection principles from various policies into a single, comprehensive document. Clearly define data protection responsibilities.
- **Reasoning:** Streamlines data protection efforts and clarifies responsibilities.

3.15 Data Retention and Destruction Policy

- **Improvement:** Specify retention periods for different data types based on legal and regulatory requirements. Detail secure data destruction methods for both physical and electronic media. Implement a robust data lifecycle management program.
- **Reasoning:** Ensures compliance with data retention requirements and prevents unauthorized access to disposed data.

3.16 Employee Onboarding and Offboarding Policy

- **Improvement:** Include specific security awareness training requirements for new employees and clear procedures for revoking access upon termination.
- **Reasoning:** Addresses security risks associated with employee lifecycle management.

3.17 Encryption Policy

- **Improvement:** Specify approved encryption algorithms and key management procedures for data at rest and in transit. Define requirements for encryption of mobile devices and removable media.
- **Reasoning:** Strengthens data protection by enforcing robust encryption practices.

3.18 Equipment Disposal Policy

- **Improvement:** Clearly outline procedures for securely sanitizing or destroying data storage devices before disposal. Include a process for documenting disposal activities.
- **Reasoning:** Prevents data breaches from discarded equipment.

3.19 Facility Security Policy

- **Improvement:** Enhance procedures for visitor management, including logging visitor details and escort requirements. Strengthen physical security controls, such as CCTV monitoring and intrusion detection systems.

- **Reasoning:** Improves physical security and reduces the risk of unauthorized access.

3.20 Firewall Management Policy

- **Improvement:** Detail firewall rule review and update procedures. Implement intrusion detection/prevention systems (IDPS) to enhance network security.
- **Reasoning:** Ensures firewall effectiveness and strengthens network defenses.

3.21 GDPR Compliance Policy

- **Improvement:** Review and update the policy to reflect the latest GDPR interpretations and enforcement actions. Clarify procedures for handling data subject requests.
- **Reasoning:** Maintains GDPR compliance and strengthens data subject rights protection.

3.22 Incident Reporting Procedures

- **Improvement:** Develop a standardized incident reporting form. Clarify reporting channels and escalation paths.
- **Reasoning:** Facilitates consistent and timely incident reporting.

3.23 Incident Response Policy

- **Improvement:** Align the policy with ISO/IEC 27035:2016 and NIST SP 800-61. Incorporate procedures for cyber incident containment, eradication, and recovery. Include clear communication and reporting procedures during an incident.
- **Reasoning:** Improves incident response effectiveness and minimizes the impact of security incidents.

3.24 Information Security Policy

- **Improvement:** Clarify roles and responsibilities for information security. Include a statement of management commitment to information security.
- **Reasoning:** Reinforces the importance of information security throughout the organization.

3.25 Internet Usage Policy

- **Improvement:** Provide specific guidance on acceptable internet usage, including social media use, email communication, and web browsing.
- **Reasoning:** Reduces the risk of malware infections and other security incidents related to internet usage.

3.26 Log Management Policy

- **Improvement:** Specify log retention periods for different log types. Implement centralized log management and analysis capabilities.
- **Reasoning:** Supports security investigations and compliance reporting.

3.27 Malware Protection Policy

- **Improvement:** Define procedures for regular malware scanning and updates. Implement endpoint detection and response (EDR) solutions for enhanced protection.
- **Reasoning:** Strengthens defenses against malware and other cyber threats.

3.28 Mobile Device Management Policy

- **Improvement:** Implement strong authentication mechanisms for mobile devices. Define policies for data encryption and remote wiping of lost or stolen devices.
- **Reasoning:** Protects sensitive data stored on mobile devices.

3.29 Network Security Policy

- **Improvement:** Implement network segmentation to isolate critical systems. Strengthen network access controls and implement intrusion prevention systems.
- **Reasoning:** Enhances network security and limits the impact of security breaches.

3.30 Password Management Policy

- **Improvement:** Strengthen password complexity requirements. Implement multi-factor authentication (MFA) for all sensitive systems. Prohibit password reuse and implement strong password management practices.
- **Reasoning:** Improves account security and mitigates the risk of unauthorized access.

3.31 Patient Booking System Security Policy

- **Improvement:** Implement secure authentication and authorization controls for the patient booking system. Conduct regular security testing and vulnerability assessments of the system.
- **Reasoning:** Protects the integrity and confidentiality of patient booking data.

3.32 Patient Consent and Communication Policy

- **Improvement:** Clearly define procedures for obtaining and documenting patient consent for data collection and use. Specify communication channels and preferences for patient communication.
- **Reasoning:** Ensures patient autonomy and transparency regarding data handling practices.

3.33 Patient Data Privacy Policy

- **Improvement:** Integrate this policy into the overarching Data Protection Policy to avoid redundancy. Ensure alignment with relevant privacy legislation and regulations.
- **Reasoning:** Streamlines data protection efforts and ensures compliance with legal requirements.

3.34 Pharmacy Medication Security Policy

- **Improvement:** Enhance physical security controls for medication storage. Implement strict access control measures and inventory management procedures.
- **Reasoning:** Safeguards medications from theft or misuse.

3.35 Policy Review and Update Procedures

- **Improvement:** Establish a regular review cycle for all security and privacy policies, at least annually or more frequently as needed due to regulatory changes or significant events. Document review outcomes and update policies accordingly.
- **Reasoning:** Ensures policies remain current and relevant.

3.36 Privacy Policy

- **Improvement:** Provide more specific information about how the hospital collects, uses, and discloses patient data. Include information about data retention and destruction

practices. Clarify data subject rights, including the right to access, correct, and erase personal information.
- **Reasoning:** Enhances transparency and patient trust.

3.37 Regulatory Compliance Policy

- **Improvement:** Map specific regulatory requirements to relevant policies and procedures. Develop a compliance monitoring and reporting framework.
- **Reasoning:** Provides a structured approach to managing regulatory compliance.

3.38 Remote Access Policy

- **Improvement:** Mandate multi-factor authentication for all remote access connections. Implement strong encryption for remote access traffic. Implement logging and monitoring of remote access activity.
- **Reasoning:** Secures remote access connections and mitigates the risk of unauthorized access.

3.39 Risk Management Policy

- **Improvement:** Define a formal risk assessment methodology and implement a regular risk assessment schedule. Clearly define risk acceptance criteria and risk treatment procedures.
- **Reasoning:** Provides a structured approach to managing risks.

3.40 Role-Based Security Training Procedure & Incident Management Procedures

- **Improvement:** Develop role-specific security training modules that address the unique security responsibilities of different roles within the hospital. Incorporate simulated phishing exercises to strengthen awareness of social engineering attacks.
- **Reasoning:** Ensures staff receive relevant and effective security training.

3.41 Security Awareness Training Policy

- **Improvement:** Expand the training program to cover contemporary cyber threats such as phishing, ransomware, and social engineering. Implement regular security awareness campaigns and refresher training. Make security awareness training mandatory for all staff, including contractors and volunteers. Track and report on training completion rates.
- **Reasoning:** Raises awareness of cybersecurity risks and best practices.

3.42 Security Events Monitoring Policy

- **Improvement:** Define specific security events to be monitored, including access attempts, system changes, and malware detections. Implement automated security event monitoring and alerting. Integrate security event logs with SIEM (Security Information and Event Management) capabilities.
- **Reasoning:** Enables proactive detection and response to security incidents.

3.43 Telehealth Security Policy

- **Improvement:** Specify security requirements for telehealth platforms and devices. Implement end-to-end encryption for telehealth communication.
- **Reasoning:** Protects the confidentiality of patient data during telehealth sessions.

3.44 Third-Party Risk Management Policy

- **Improvement:** Implement a comprehensive third-party risk assessment process, including security questionnaires, on-site audits, and contract review. Implement ongoing monitoring of third-party security performance. Define clear exit strategies for third-party relationships.
- **Reasoning:** Mitigates risks associated with third-party access to sensitive data.

3.45 Vulnerability Management Policy & Compliance Reporting Procedures

- **Improvement:** Define procedures for regular vulnerability scanning and penetration testing. Establish a process for prioritizing and remediating identified vulnerabilities. Implement a vulnerability disclosure policy. Develop a standardized compliance reporting template.
- **Reasoning:** Identifies and addresses security vulnerabilities.

4. Conclusion

Implementing these improvements will significantly strengthen the cybersecurity and privacy compliance posture of Hills Shire Care Private Hospital. It is recommended that the hospital prioritize these recommendations and develop an implementation plan with clear timelines and responsibilities. Regular monitoring and review of the effectiveness of these improvements are essential for ongoing compliance and security posture enhancement.