Inconsistency Report for Hills Shire Care Private Hospital

Date: 01 July 2024

Subject: Cybersecurity and Privacy Compliance Inconsistency Report

This report details inconsistencies identified within Hills Shire Care Private Hospital's current policies and procedures compared against established standards and regulations, 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 other relevant Australian healthcare privacy regulations. These inconsistencies pose potential risks to the hospital's security posture and compliance efforts.

I. Data Retention and Destruction

- **Inconsistency:** The `Data Retention and Destruction Policy.pdf` states data will be retained for 7 years, while the `Patient Data Privacy Policy.pdf` mentions a 10-year retention period. This contradicts the Australian My Health Records Act 2012 which does not stipulate a time.
- **Impact:** Conflicting retention periods can lead to legal and compliance issues if audits reveal discrepancies.
- **Recommendation:** Harmonize data retention periods across all policies to align with legal requirements and industry best practices. Consult legal counsel to determine appropriate retention durations for different data types, considering the My Health Records Act and other relevant regulations. Document the rationale behind the chosen retention periods.

II. Data Breach Response

- **Inconsistency:** The `Data Breach Response Policy.pdf` lacks specific procedures for notifying individuals affected by a data breach, which is a mandatory requirement under the Notifiable Data Breaches (NDB) scheme of the Privacy Act 1988. The `GDPR Compliance Policy.pdf` mentions a 72-hour notification window which might not be feasible in all situations.
- **Impact:** Failure to promptly notify affected individuals and the Office of the Australian Information Commissioner (OAIC) can result in significant penalties.
- **Recommendation:** Revise the Data Breach Response Policy to include detailed procedures for identifying affected individuals, determining the severity of the breach, preparing notification content, and delivering notifications within legally mandated timeframes as per the NDB scheme. Establish clear communication channels and escalation paths.

III. Access Control

- **Inconsistency:** The `Access Control Policy.pdf` allows staff access to patient data based on their “department,” but the `Patient Data Privacy Policy.pdf` mentions access should be granted based on “need-to-know.” The `Ambulance Patient Data Handling Policy.pdf` doesn't clarify access controls for paramedics.
- **Impact:** Granting excessive access rights violates the principle of least privilege and increases the risk of unauthorized data access or modification.

- **Recommendation:** Implement a robust role-based access control (RBAC) system. Define roles with specific permissions based on job responsibilities and data sensitivity. Restrict access to patient data to only those individuals requiring it to perform their duties. Ensure the Ambulance Patient Data Handling Policy aligns with overall access control principles and addresses data access for paramedics, including secure authentication and authorization mechanisms.

IV. Security Awareness Training

- **Inconsistency:** `Security Awareness Training Policy.pdf` mandates annual training, but the `Role-Based Security Training Procedure Incident Management Procedures.pdf` doesn't clearly define the frequency for role-specific training. The hospital's IT team and Staff members are undertrained in new technologies and the use of social media apps. There is no policy to manage the use of employees personal mobile devices BYOD.
- **Impact:** Inconsistent training frequency can create gaps in employee knowledge about cybersecurity threats and best practices.
- **Recommendation:** Implement a comprehensive security awareness training program that includes annual general awareness training and more frequent role-based training, particularly for roles with high-risk access. The training should cover relevant topics such as phishing, malware, social engineering, data privacy, and compliance requirements. Introduce role based access control for each level of employee. Introduce BYOD Bring Your Own Device policy to ensure mobile device data is encrypted and protected. Provide specific training in regards to GDPR compliance and APP policies. Introduce specific training to comply with new technologies as they are rolled out. Introduce training to use social media apps safely, to protect patient and hospital information.

V. Third-Party Risk Management

- **Inconsistency:** `Third-Party Risk Management Policy.pdf` addresses vendor risk assessments but does not specify the frequency of these assessments or procedures for ongoing monitoring. The hospital doesn't not conduct background checks on security and IT staff before employment. There is no mention of any whistleblowing policy for staff.
- **Impact:** Inadequate third-party risk management can expose the hospital to vulnerabilities introduced by external vendors.
- **Recommendation:** Implement a formalized third-party risk management program. Define clear criteria and procedures for conducting risk assessments on all third-party vendors with access to sensitive data. Establish a regular schedule for assessments (e.g., annually or based on risk level) and incorporate ongoing monitoring activities to track vendor performance and compliance. Conduct background checks on security and IT staff before employment. Implement and Communicate a whistleblowing policy to all staff.

VI. Incident Response

- **Inconsistency:** The `Incident Response Policy.pdf` and `Incident Reporting Procedures.pdf` have conflicting descriptions of the incident reporting process, creating confusion for staff. `Telehealth Security Policy.pdf` does not specify incident response procedures related to telehealth services.
- **Impact:** A poorly defined incident reporting process can hinder timely and effective incident response, leading to greater damage.

- **Recommendation:** Clarify and streamline the incident reporting process. Establish a single point of contact for reporting security incidents. Develop a standardized incident reporting form capturing essential details. Clearly define roles and responsibilities during incident response. Integrate incident response procedures into the Telehealth Security Policy, addressing specific scenarios related to telehealth, such as data breaches during virtual consultations or unauthorized access to telehealth platforms.

VII. Physical Security

- **Inconsistency:** `Facility Security Policy.pdf` mentions the use of security cameras, but `Data Center Security Procedures.pdf` lacks details about specific physical security controls for the data center, such as access badges or biometric authentication. `Visitor Management Policy.pdf` does not have procedures for verifying visitor identities.
- **Impact:** Weak physical security controls can allow unauthorized physical access to sensitive areas and data.
- **Recommendation:** Strengthen physical security measures for the data center and other critical areas. Implement multi-factor authentication (e.g., access badges + biometric verification) for data center access. Ensure the Visitor Management Policy includes procedures for verifying visitor identities (e.g., checking photo IDs) and logging their entry and exit times. Conduct regular physical security assessments to identify vulnerabilities.

VIII. Policy Review and Updates

- **Inconsistency:** `Policy Review and Update Procedures.pdf` states policies should be reviewed annually. This is insufficient for some regulations, like GDPR, which may require more frequent updates due to evolving legal interpretations.
- **Impact:** Outdated policies can lead to non-compliance with current regulations.
- **Recommendation:** Establish a dynamic policy review schedule. While annual reviews are a minimum, some policies, particularly those related to privacy and data protection (e.g., GDPR Compliance Policy, Australian Privacy Principles Policy), should be reviewed more frequently to reflect changes in legislation, regulatory guidance, and industry best practices.

IX. Compliance with Standards

- **Inconsistency:** Many policies lack explicit mappings to specific controls within ISO 27001, 27002, NIST CSF, etc. For example, `Network Security Policy.pdf` mentions firewalls but lacks reference to relevant ISO 27001 Annex A controls or NIST CSF subcategories.
- **Impact:** Lack of mappings makes it difficult to demonstrate compliance with specific controls during audits.
- **Recommendation:** Map each policy to relevant controls within ISO 27001 Annex A, ISO 27002 clauses, NIST CSF subcategories, and other applicable standards. This mapping should be explicitly documented within each policy or in a separate compliance matrix. This will enhance transparency and facilitate compliance verification.

X. Data Classification

- **Inconsistency:** The `Data Classification Policy.pdf` does not provide clear

instructions on how to classify patient data according to its sensitivity level (e.g., confidential, restricted, public). The policy needs to align with APPs and State/Territory health data privacy legislation and relevant regulations.
- **Impact:** Inconsistencies in data classification can hinder proper data protection measures.
- **Recommendation:** Revise the Data Classification Policy to include detailed guidance on data classification levels and provide examples of how to classify different types of patient data. Develop procedures for labelling and handling data based on its classification. Integrate data classification procedures with access control and data retention/destruction policies to ensure consistent application.

XI. Encryption

- **Inconsistency:** `Encryption Policy.pdf` mandates encryption of data at rest and in transit but `Mobile Device Management Policy.pdf` does not address enforcement mechanisms for device encryption or encryption requirements for data stored on mobile devices.
- **Impact:** Failure to enforce encryption on mobile devices increases the risk of data breaches in case of device loss or theft.
- **Recommendation:** Strengthen the Mobile Device Management Policy to incorporate specific requirements for device encryption. Implement Mobile Device Management (MDM) software to enforce encryption settings and manage mobile device security. Define encryption standards for data storage and transmission from mobile devices.

XII. Asset Management

- **Inconsistency:** The `Asset Management Policy.pdf` doesn't define a process for managing software licenses, which can lead to non-compliance with software licensing agreements. `Equipment Disposal Policy.pdf` does not adequately address data sanitization procedures before disposal.
- **Impact:** Unmanaged software licenses can result in legal and financial risks. Improper data sanitization during equipment disposal can lead to data breaches.
- **Recommendation:** Enhance the Asset Management Policy to include procedures for managing software licenses, including tracking software installations, ensuring license compliance, and managing software updates. Revise the Equipment Disposal Policy to provide detailed instructions on data sanitization procedures for different types of equipment (e.g., hard drives, mobile devices), ensuring data is securely erased or destroyed before disposal in accordance with NIST SP 800-88 or other relevant standards.

XIII. Backup and Recovery

- **Inconsistency:** The `Backup and Recovery Policy.pdf` specifies a backup frequency, but the `Business Continuity and Disaster Recovery Policy.pdf` does not specify recovery time objectives (RTOs) or recovery point objectives (RPOs), which are crucial for ensuring business continuity.
- **Impact:** Lack of RTOs and RPOs can hinder the hospital's ability to restore critical systems and data within acceptable timeframes after a disaster.
- **Recommendation:** Define specific RTOs and RPOs for critical systems and data within the Business Continuity and Disaster Recovery Policy. Align backup and recovery procedures with these objectives. Regularly test the disaster recovery plan to ensure its effectiveness.

This report serves as a starting point for addressing the identified inconsistencies. A dedicated team should be tasked with implementing the recommended actions and regularly monitoring compliance with relevant standards and regulations. Regular updates and reviews of policies and procedures are essential to maintain a robust security posture and protect the confidential information of patients. Further detailed assessments and gap analyses may be necessary to address specific areas in greater depth.