Hills Shire Care Private Hospital - Cybersecurity & Privacy FAQ

Date: 01 July 2024

This FAQ document provides guidance for all staff at Hills Shire Care Private Hospital on cybersecurity and privacy compliance in their daily work. It is designed to help you understand and adhere to the hospital's policies and procedures, which are aligned with standards such as ISO 27001/27002/27005/27018/27035, 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.

General Cybersecurity

Q1: What is cybersecurity, and why is it important in a hospital setting?

A: Cybersecurity refers to the practices that protect our computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. In a hospital, cybersecurity is crucial for protecting sensitive patient information, maintaining the integrity of medical records, ensuring the availability of critical systems, and upholding patient trust.

Q2: What is my role in maintaining cybersecurity at the hospital?

A: Every staff member plays a vital role in cybersecurity. You are responsible for following hospital policies and procedures, reporting any suspicious activity, protecting your login credentials, and completing mandatory security awareness training.

Q3: What should I do if I suspect a cybersecurity incident (e.g., phishing email, malware infection, unauthorized access)?

A: Immediately report the incident to the IT department or your designated cybersecurity contact as per the Incident Reporting Procedures. Do not attempt to resolve the issue yourself. Provide as much detail as possible about the incident.

Q4: What is the hospital's Acceptable Use Policy, and how does it apply to me?

A: The Acceptable Use Policy outlines the appropriate use of hospital IT resources, including computers, networks, email, and internet access. It prohibits activities such as accessing unauthorized websites, downloading illegal software, and sharing confidential information without authorization. Familiarize yourself with this policy and adhere to its guidelines.

Q5: How often should I change my password?

A: Follow the Password Management Policy, which dictates password complexity requirements and the frequency of changes. Never share your password with anyone, and avoid using easily guessable passwords.

Q6: Can I access hospital systems remotely?

A: Remote access is governed by the Remote Access Policy. If you require remote access,

follow the proper procedures for authorization and utilize approved security measures such as VPNs and multi-factor authentication.

Q7: How is the hospital protected against malware?

A: The hospital employs robust malware protection measures as outlined in the Malware Protection Policy. This includes antivirus software, regular system scans, and security updates. Never disable these protections or install unauthorized software.

Q8: What are the rules regarding the use of mobile devices at the hospital?

A: The Mobile Device Management Policy governs the use of personal and hospital-owned mobile devices. It addresses security requirements, data storage, and acceptable use guidelines. Ensure your mobile device is secured with a strong password or PIN.

Patient Data Privacy

Q9: What are the Australian Privacy Principles (APPs), and how do they apply to my work?

A: The APPs are 13 principles that govern the handling of personal information in Australia. They cover aspects such as collection, use, disclosure, storage, and access to personal information. As hospital staff, we must comply with the APPs when dealing with patient data. Refer to the Australian Privacy Principles (APPs) Policy for details.

Q10: What constitutes "personal information" in a healthcare context?

A: Personal information includes any information that can identify an individual, such as name, address, medical history, test results, Medicare number, and contact details. Even seemingly insignificant details can contribute to identifying a patient, so treat all patient data with utmost confidentiality.

Q11: How can I ensure patient data confidentiality?

A: Adhere to the hospital's Patient Data Privacy Policy and relevant procedures. This includes only accessing patient data necessary for your role, securing physical copies of records, properly disposing of confidential information, and never discussing patient details outside of authorized contexts.

Q12: What is the process for obtaining patient consent for the collection and use of their information?

A: Follow the Patient Consent and Communication Policy. Obtain explicit consent from patients before collecting, using, or disclosing their information for any purpose beyond their immediate care. Ensure patients understand how their information will be used and their right to access and correct it.

Q13: How long should patient records be kept?

A: The Data Retention and Destruction Policy outlines the retention periods for different types of patient data. Follow this policy for storing and securely destroying records after the required retention period has expired.

Q14: What should I do if a patient requests access to their medical records?

A: Follow the established procedures for handling patient requests for access to their records. Verify the patient's identity and provide them with the requested information within a reasonable timeframe, subject to any legal or ethical limitations. Refer to the APPs policy and the Privacy Act for guidance.

Q15: What is a data breach, and what should I do if I become aware of one?

A: A data breach is any unauthorized access, use, disclosure, loss, or modification of personal information. If you become aware of a potential data breach, immediately report it to the designated contact as outlined in the Data Breach Response Policy.

Q16: How does the GDPR impact the hospital's handling of patient data, even though we are in Australia?

A: While the GDPR is a European regulation, it can apply to the hospital if we process the personal data of individuals located in the European Economic Area. The GDPR Compliance Policy outlines the necessary procedures for handling such data.

Specific Procedures and Policies

Q17: What is the policy on accessing patient booking information?

A: The Patient Booking System Security Policy governs access to the patient booking system. Only authorized personnel can access this system, and access is limited to information required for their specific role.

Q18: What are the security requirements for telehealth consultations?

A: The Telehealth Security Policy outlines the specific security requirements for conducting telehealth consultations. This includes using secure communication platforms, protecting patient privacy during virtual consultations, and ensuring the confidentiality of telehealth records.

Q19: How are medications secured within the pharmacy?

A: The Pharmacy Medication Security Policy dictates procedures for storing, handling, and dispensing medications. This includes physical security measures, access controls, and inventory management practices.

Q20: What security measures are in place for our data center?

A: The Data Center Security Procedures outline the physical and logical security measures protecting our data center, including access controls, environmental controls, and surveillance systems.

Q21: How does the hospital classify different types of data?

A: The Data Classification Policy describes how data is categorized (e.g., confidential, restricted, public) based on sensitivity and regulatory requirements. This helps ensure appropriate security controls are applied to different data types.

Q22: What is the hospital’s policy on handling data from ambulance services?

A: The Ambulance Patient Data Handling Policy outlines the procedures for receiving, processing, and protecting patient data transmitted by ambulance services. This ensures data

integrity and confidentiality while facilitating seamless patient care transitions.

Q23: How are visitors to the hospital managed to ensure security and patient privacy?

A: The Visitor Management Policy outlines procedures for managing visitors, including registration, identification, authorized access areas, and appropriate conduct within the hospital. This policy helps maintain a secure environment while respecting patient privacy.

Q24: What is the process for reporting security incidents?

A: The Incident Reporting Procedures detail how to report security incidents, including contact information, required information in the report, and follow-up procedures. Timely reporting is crucial for effective incident response.

Q25: What is the procedure for equipment disposal?

A: The Equipment Disposal Policy defines procedures for securely disposing of IT equipment, including data sanitization/destruction methods to prevent unauthorized data access.

Q26: What are the procedures for compliance reporting?

A: The Compliance Reporting Procedures describe the process for generating and submitting compliance reports to relevant authorities. This ensures transparency and accountability in maintaining adherence to legal and regulatory obligations.

Q27: How does the hospital manage third-party risks?

A: The Third-Party Risk Management Policy outlines procedures for assessing and managing risks associated with third-party vendors and service providers who have access to hospital systems or data. This ensures that third parties also adhere to appropriate security and privacy standards.

Q28: How are security vulnerabilities identified and addressed?

A: The Vulnerability Management Policy outlines procedures for regularly identifying, assessing, and remediating security vulnerabilities in hospital systems and applications. This includes vulnerability scanning, penetration testing, and timely patching.

Q29: How are facility security risks managed?

A: The Facility Security Policy details measures implemented to secure the physical premises of the hospital. This includes access control systems, surveillance systems, alarm systems, and emergency response procedures.

Q30: What is the process for managing changes to IT systems?

A: The Change Management Policy defines procedures for planning, implementing, and documenting changes to IT systems. This structured approach helps prevent disruptions and maintain system stability and security.

Q31: How are security events monitored?

A: The Security Events Monitoring Policy outlines the processes for monitoring security-related events, such as unauthorized access attempts, system errors, and suspicious activity. This enables timely detection and response to potential security threats.

Q32: How are security and privacy policies reviewed and updated?

A: The Policy Review and Update Procedures describe the process for regularly reviewing and updating security and privacy policies to ensure they remain relevant and effective.

Q33: What training is provided to staff on security awareness?

A: The Security Awareness Training Policy outlines the mandatory training programs provided to all staff on cybersecurity and privacy best practices. This training enhances your knowledge and skills to protect patient data and hospital systems.

Q34: What is the procedure for onboarding and offboarding employees related to security and access?

A: The Employee Onboarding and Offboarding Policy details the procedures for granting and revoking system access for new and departing employees, respectively. This ensures that only authorized personnel have access to hospital systems and data.

Q35: How is data protected during transmission and storage?

A: The Encryption Policy details the use of encryption techniques to protect data both in transit and at rest. This helps prevent unauthorized access to confidential information.

Q36: How are system logs managed?

A: The Log Management Policy outlines procedures for collecting, storing, and analyzing system logs. Log management is critical for security auditing, incident investigation, and compliance reporting.

Q37: How does the hospital address threat intelligence and threat modeling?

A: The Threat Intelligence and Threat Modeling Policy guides the hospital in proactively identifying, analyzing, and mitigating potential cyber threats. Threat intelligence gathers information about current and emerging threats, while threat modeling analyzes system vulnerabilities to anticipate potential attack vectors.

Q38: What are the principles guiding the hospital's overall Information Security program?

A: The Information Security Policy establishes the overarching principles and goals for protecting the hospital's information assets. It provides a framework for all other security policies and procedures.

Q39: What is the policy regarding internet usage?

A: The Internet Usage Policy details acceptable use guidelines for accessing the internet from hospital systems. This policy helps prevent security risks and ensures productive use of internet resources.

Q40: Where can I find copies of these policies and procedures?

A: All policies and procedures are available on the hospital intranet or from your department manager. Familiarize yourself with the relevant policies for your role.

This FAQ is a living document and will be updated regularly. If you have any further questions, please contact the IT department, your supervisor, or the Compliance Officer. Your

cooperation in upholding these standards is essential for protecting our patients and the hospital.