Hills Shire Care Private Hospital Cybersecurity & Privacy Compliance Training

Date: 01 July 2024

Version: 1.0

Introduction

This training program is designed to equip all staff at Hills Shire Care Private Hospital with the knowledge and skills necessary to maintain cybersecurity and privacy compliance in their daily work. This training aligns with international standards like 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 relevant Australian healthcare privacy regulations.

Training Objectives

Upon completion of this training, staff will be able to:

- Understand the importance of cybersecurity and privacy in healthcare.
- Identify key cybersecurity and privacy risks.
- Apply hospital policies and procedures related to data protection.
- Recognize and report security incidents.
- Use hospital systems and devices securely.
- Maintain patient confidentiality.

Module 1: Understanding Cybersecurity and Privacy in Healthcare

Why Cybersecurity and Privacy Matter

- **Protecting Patient Information:** Patient data is highly sensitive and confidential. Unauthorized access or disclosure can have severe consequences for patients, including identity theft, financial loss, and reputational damage.
- **Maintaining Hospital Operations:** Cybersecurity incidents can disrupt hospital operations, impacting patient care and potentially leading to life-threatening situations.
- **Meeting Legal and Regulatory Requirements:** Hospitals are required to comply with various laws and regulations related to cybersecurity and privacy. Failure to comply can result in significant fines and penalties.
- **Building Trust and Reputation:** Maintaining strong cybersecurity and privacy practices builds trust with patients and the community, enhancing the hospital's reputation.

Key Cybersecurity and Privacy Risks

- **Phishing:** Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.
- **Malware:** Malicious software designed to damage or disable computer systems.
- **Ransomware:** A type of malware that encrypts data and demands a ransom for its release.
- **Insider Threats:** Security risks posed by individuals within the hospital, whether intentional or unintentional.
- **Data Breaches:** Unauthorized access or disclosure of sensitive data.
- **Physical Security Breaches:** Unauthorized physical access to hospital facilities or equipment.

Module 2: Hospital Policies and Procedures

Key Policies

This section will cover the key hospital policies related to cybersecurity and privacy, including:

- **Acceptable Use Policy:** Defines acceptable use of hospital IT resources.
- **Access Control Policy:** Governs access to sensitive information and systems.
- **Data Classification Policy:** Categorizes data based on sensitivity and dictates handling procedures.
- **Data Protection Policy:** Outlines measures to protect patient data.
- **Data Retention and Destruction Policy:** Specifies how long data is retained and how it is securely destroyed.
- **Privacy Policy:** Details the hospital's commitment to patient privacy.
- **Incident Response Policy:** Describes the process for responding to security incidents.
- **Mobile Device Management Policy:** Governs the use of mobile devices on the hospital network.
- **Password Management Policy:** Sets requirements for creating and managing strong passwords.
- **Remote Access Policy:** Defines procedures for accessing hospital systems remotely.

Procedures

This section will detail procedures related to:

- **Incident Reporting:** How to report suspected security incidents.
- **Data Breach Response:** Steps taken in the event of a data breach.
- **Policy Review and Update:** How policies are reviewed and updated to reflect current best practices.

Module 3: Recognizing and Reporting Security Incidents

What is a Security Incident?

A security incident is any event that compromises the confidentiality, integrity, or availability of hospital information systems or data. Examples include:

- Suspicious emails or attachments.
- Unauthorized access attempts.
- Malware infections.

- Loss or theft of devices.
- Physical security breaches.

How to Report a Security Incident

If you suspect a security incident, immediately report it to the IT Help Desk or your supervisor. Provide as much detail as possible, including:

- Date and time of the incident.
- Description of the incident.
- Any affected systems or data.
- Any individuals involved.

Module 4: Secure Use of Hospital Systems and Devices

Password Security

- Use strong, unique passwords for all hospital accounts.
- Do not share passwords with anyone.
- Change passwords regularly.

Email Security

- Be cautious of suspicious emails.
- Do not click on links or open attachments from unknown senders.
- Report phishing emails to the IT Help Desk.

Device Security

- Keep devices locked when not in use.
- Install and maintain anti-virus software.
- Do not connect unauthorized devices to the hospital network.

Physical Security

- Secure physical access to hospital facilities and equipment.
- Report any suspicious activity to security personnel.

Module 5: Maintaining Patient Confidentiality

HIPAA and Australian Privacy Principles

- Understand the requirements of the Australian Privacy Principles (APPs) and other relevant Australian legislation.
- Only access patient information when necessary for your job duties.
- Do not discuss patient information with unauthorized individuals.
- Protect patient information from unauthorized access or disclosure.

Module 6: Specific Compliance Requirements

ISO 27001/27002: Information Security Management

- Understand the key principles of information security management.
- Follow established procedures for protecting information assets.

ISO 27005: Information Security Risk Management

- Understand the process of risk assessment and risk treatment.
- Identify and report potential security risks.

ISO 27018: Protection of Personally Identifiable Information (PII) in the Cloud

- Understand the specific requirements for protecting PII in cloud environments.
- Follow procedures for securely storing and processing patient data in the cloud.

ISO 27035: Information Security Incident Management

- Understand the incident management lifecycle.
- Follow procedures for responding to and managing security incidents.

NIST Cybersecurity Framework (CSF)

- Understand the five core functions of the NIST CSF: Identify, Protect, Detect, Respond, and Recover.
- Apply the framework to improve the hospital's cybersecurity posture.

Cyber Security Act 2024 & Australian Cyber Security Strategy 2023-2030

- Be aware of the key provisions of the Cyber Security Act 2024 and the Australian Cyber Security Strategy 2023-2030.
- Understand the hospital's obligations under these regulations.

GDPR and Australian Privacy Principles (APPs)

- Understand the key principles of GDPR and APPs.
- Follow procedures for obtaining patient consent and managing data subject requests.

Assessment and Evaluation

- Successful completion of this training requires achieving a passing score on a post-training assessment.
- The assessment will cover the key concepts discussed in this training material.

Further Information and Resources

- Contact the IT Help Desk for any questions or concerns related to cybersecurity and privacy.
- Refer to the hospital's intranet for access to all relevant policies and procedures.

Acknowledgement

By completing this training, you acknowledge that you have read, understood, and agree to abide by the hospital's cybersecurity and privacy policies and procedures.

This concludes the Hills Shire Care Private Hospital Cybersecurity & Privacy Compliance Training. Thank you for your participation.