Legacy® IPC Device

Cybersecurity Policy

Published by: Stephen Ingram - Data Protection Officer

Date: 08th June 2023

Company: IG Technology Ltd

Introduction

The purpose of Cybersecurity is to ensure that information can be used when required in the conduct of business with confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorised disclosure, damage or loss.

IG Technology Ltd recognises the importance of Cybersecurity and is committed to ensuring that information is defended against Cybersecurity threats.

All Users of the Legacy® IPC device should be aware of this policy, their responsibilities and obligations. All Users are required to comply with the policy and should observe applicable statutory legislation.

Policy brief and purpose

The purpose of this policy is to outline Cybersecurity measures and guidelines put in place to ensure the secure usage of the Legacy® IPC wireless medical device and associated Mobile Application (APP). This policy is designed to protect the confidentiality, integrity, and availability of patient data, prevent unauthorised access, and mitigate potential Cybersecurity risks associated with the device and system.

Scope

This policy applies to all medical staff, Users and others specifically authorised to access information associated, owned, operated, controlled, or managed by IG Technology Ltd.

Policy elements - confidential data

All approved hardware and software used within the Legacy® IPC system will have the following protocols (where applicable):

Access Control

• IG Technology Ltd will assign unique user accounts and credentials to authorised personnel who will operate or access the device.

• Strong password policies will be implemented, including minimum length, complexity, and regular password updates.

• Multi-factor authentication (MFA) will be utilised for device access whenever possible to enhance security.

Device Configuration:

- The Legacy® IPC device is configured with the latest firmware and security patches provided by IG Technology Ltd.
- The Legacy® IPC system has enabled security features, such as encryption and authentication mechanisms on the device to protect data transmission and device access.
- The Legacy® IPC system will disable unnecessary services or features that is not essential for the device's functionality to minimise attack surfaces.

To maintain Network security, the user should ensure the following:

- Disablement of wireless visibility when the Legacy® IPC not in use to prevent unauthorised connections (i.e. turn the device off when not in use).
- Regularly review and update the list of devices connected to any routers/access points, removing any unauthorised or obsolete entries.
- Ensure that the Mobile device running the Legacy® IPC APP is connected to a secure and segregated wireless network that utilizes encryption (e.g., WPA2 or higher).
- Regular updates of wireless network access credentials and change default passwords to maintain confidentiality.
- Implement network segmentation to isolate the device from other critical systems and establish strict firewall rules to control network traffic.

Data Protection and Privacy

IG Technology Ltd will provide the following:

Data Encryption:

- Implementation of strong encryption algorithms to protect patient data both during transmission and storage.
- Ensure data encryption keys are securely managed and regularly rotated.

Data Backup and Recovery:

- Regularly back up of patient's data to a secure location.
- Test data restoration procedures to ensure data can be recovered effectively in the event of data loss or system failure.

Privacy and Confidentiality:

- Compliance with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA).
- Establish procedures for handling and disposing of patient data in a secure manner.
- Limit access to patient data to authorised personnel only and maintain an audit trail of data access and modifications.

Incident Response and Reporting:

- Develop an incident response plan that outlines procedures for identifying, responding to, and mitigating Cybersecurity incidents.
- Clearly define roles and responsibilities of personnel involved in an incident response.

Reporting Security Incidents:

- Establish clear reporting channels for users or employees to report any potential Cybersecurity incidents or vulnerabilities promptly.
- Maintain a process for incident documentation, including gathering evidence, containment measures, and reporting to relevant authorities if required.

Data Destruction - Policy Statement

This policy establishes guidelines and procedures for the secure and proper destruction of sensitive data to mitigate the risk of unauthorized access or data breaches. It is the responsibility of all employees and authorised individuals to adhere to this policy when disposing of data-bearing assets.

1. Definitions: a. Sensitive Data: Any information that, if accessed by unauthorised individuals, could cause harm to individuals, the organisation, or violate applicable laws and regulations. b. Data-Bearing Assets: Any physical or electronic media, including but not limited to hard drives, solid-state drives, USB drives, CDs/DVDs, tapes, or any other storage devices containing sensitive data.
2. Classification of Data: a. The organisation shall classify data based on its sensitivity and define data retention periods. This classification will determine the appropriate destruction methods.
3. Destruction Methods: a. Physical Destruction: Data-bearing assets that are no longer required shall be physically destroyed using approved methods, such as shredding, crushing, or incineration, to render the data irrecoverable. b. Secure Wiping: For electronic storage media, approved secure wiping methods, such as data erasure software using industry-recognised standards, shall be employed to ensure complete and irreversible removal of data. c. Degaussing: Magnetic storage media, such as tapes or hard drives, shall undergo degaussing using approved equipment to erase all data.
4. Data Destruction Procedures: a. Employees or authorised individuals responsible for data destruction shall follow documented procedures that outline the steps to be taken for each destruction method. b. The destruction process shall be logged, including details such as the date, type of media, destruction method used, and the individual performing the destruction. c. Destruction procedures shall include verification steps to ensure successful data destruction and proper disposal of the destroyed media.
5. Disposal of Destroyed Media: a. Disposal of destroyed media shall be carried out in a secure manner to prevent any possibility of data recovery. b. The organisation shall maintain relationships with authorised recycling or disposal vendors to ensure compliance with environmental regulations and secure disposal practices.

6. Employee Training and Awareness: a. Regular training and awareness programs shall be conducted to educate employees and authorised individuals on the data destruction policy, procedures, and the importance of proper data disposal. b. Employees shall be made aware of the consequences of non-compliance with this policy, including disciplinary actions and potential legal repercussions.
7. Audit and Compliance: a. Regular audits shall be conducted to ensure compliance with the data destruction policy. b. Compliance with this policy shall be monitored, and any deviations or non-compliance shall be addressed promptly.
8. Policy Review: a. This policy shall be reviewed periodically to ensure its relevance and effectiveness in addressing emerging threats and changes in data protection regulations. b. Any necessary updates or revisions to this policy shall be communicated to all employees and authorized individuals.
9. Policy Violations: a. Violations of this policy shall be reported to the appropriate authority for investigation and may result in disciplinary action, up to and including termination of employment or legal consequences.
10. Policy Distribution: a. This policy shall be communicated to all employees and authorised individuals and made readily accessible through appropriate channels, such as the organisation's intranet or employee handbook.

Secure Data Transfer Policy

Policy Statement: This policy establishes guidelines and procedures for securely transferring data within and outside the organization to ensure the confidentiality, integrity, and availability of sensitive information. All employees and authorised individuals are responsible for adhering to this policy when transferring data.

1. Data Classification: a. Data shall be classified based on its sensitivity level and criticality to determine the appropriate security measures during transfer. b. The organisation shall define and maintain a data classification framework that outlines the requirements and controls for each classification level.
2. Secure Transfer Methods: a. Encryption: Confidential and sensitive data shall be encrypted during transit using industry-recognised encryption algorithms and protocols, such as TLS (Transport Layer Security) or VPN (Virtual Private Network). b. Secure File Transfer Protocols: Data transfers shall be conducted through secure file transfer protocols, such as SFTP (SSH File Transfer Protocol) or HTTPS, to ensure data integrity and protection against unauthorised access. c. Data Loss Prevention (DLP) Solutions: The organisation shall employ DLP solutions to monitor and prevent the transfer of sensitive data through unauthorised channels or methods.
3. Access Control and Authentication: a. Only authorised individuals with a legitimate need to access and transfer data shall be granted appropriate privileges. b. Multi-factor authentication (MFA) shall be enforced for accessing systems or platforms used for data transfer to enhance security.
4. Secure Email and Messaging: a. For data transfers via email or messaging platforms, sensitive information shall be encrypted before transmission. b. Employees shall be educated on the risks associated with transmitting sensitive data via email and encouraged to use secure file transfer methods whenever possible.

5. Third-Party Transfers: a. When transferring data to third parties, such as vendors, partners, or contractors, appropriate data protection agreements (DPAs) or contracts shall be in place. b. The organisation shall assess the third party's security practices and ensure they meet the required standards before initiating data transfers.
6. Data Transfer Logging and Monitoring: a. Logs of data transfers, including source, destination, timestamp, and relevant details, shall be maintained for audit and monitoring purposes. b. Regular monitoring of data transfers shall be conducted to detect and respond to any suspicious or unauthorised activities.
7. Employee Training and Awareness: a. Regular training programs shall be conducted to educate employees and authorised individuals on secure data transfer practices, the proper use of encryption, and the risks associated with insecure transfer methods. b. Employees shall be made aware of the consequences of non-compliance with this policy, including disciplinary actions and potential legal repercussions.
8. Policy Review: a. This policy shall be reviewed periodically to ensure its relevance and effectiveness in addressing emerging threats and changes in data protection regulations. b. Any necessary updates or revisions to this policy shall be communicated to all employees and authorized individuals.
9. Policy Violations: a. Violations of this policy shall be reported to the appropriate authority for investigation and may result in disciplinary action, up to and including termination of employment or legal consequences.
10. Policy Distribution: a. This policy shall be communicated to all employees and authorised individuals and made readily accessible through appropriate channels, such as the organisation's intranet or employee handbook.

By adhering to this Cybersecurity policy, the organisation aims to protect sensitive information, minimise the risk of data breaches, and ensure compliance with applicable laws and regulations.