1. Consider an implanted medical device that monitors and records data about a patient's health and stores the information locally. To access the data, authorized personnel must transmit a personal identification number to the implanted device and once authorized, electronically request specific portions of the data. Give examples of Confidentiality, integrity and availability requirements associated with the system and in each case, indicate the degree of importance of the requirement.

The CIA Triad is a fundamental model in cybersecurity that represents three key principles:

1. Confidentiality - Protecting information from unauthorized access
2. Integrity - Ensuring data is accurate and unaltered.
3. Availability - Ensuring authorized users have access to data when needed.

1. Confidentiality [High Importance]

Requirement: The patient's health data must be protected from unauthorized access. Only authorized

personnel. with the correct PIN should be able to access the data.

Implementation:

Encryption: The stored and transmitted data should be encrypted using strong encryption algorithms.
eg: AES-256.

Authentication + Access Control: Only Authoried medical professionals should be able to retreive the data using multi-factor authentication (MFA) or secure PIN-based access.

Secure Commenication: Communication between the device and the external system must use TLS/SSL to prevent eavesdropping.

Importance: Critical - If unauthorized users access sensitive health data, if could lead to privacy violations, identity theft or even manipulation of medical records.

2. Integrity [High Importance]

Requirement: The health data recorded and Trasmitted must remain unaltered to ensure accurate medical decisions.

Extremely Critical: If the device fails or becomes inaccessible, medical personnel may not receive crucial health data in time, potentially leading to life threatening situations.

Encryption Algorithms:

(a) Symmetric Encryption (For Data Storage & Fast Communication).

- AES-256 (Advanced Encryption Standard - 256-bit).
- AES is widely used for encrypting stored data in medical devices.
- Fast and efficient on embedded devices with limited computational power.

(b) Hashing [For Integrity Verification]

- SHA - 256 (Secure Hash Algorithm - 256 bit).
- used to generate a unique fingerprint of stored / transmitted data.
- prevents data tampering and ensures medical records remain unaltered.

eg: If a hacker alters a patient's health data, SHA-256 will generate a different hash value, detecting tampering.

Digital signatures : use cryptographic hash functions to ensure data integrity and detect tampering.

Error Detection Mechanisms: Implemunt checksum or redundancy mechanisms to detect and correct transmission errors.

Tamper-Resistant Storage: The device should prevent unauthorized modification to stored data.

Importance: If integrity is compromised, incorrect or manipulated health data could lead to incorrect medical treatments, endangering the patient's life.

Availability

Requirement: The system must be accessible when needed, especially in emergencies.

Implementation.

- Ensure multiple secure ways to retrieve data
- The device should have efficient power management to remain operational for extended periods.
- Dos: Implemunt rate limiting and anomaly detection to prevent attackers from blocking access to the device.