Information Assurance Principles

Information assurance (IA) makes sure that information systems are safe from attacks that harm the availability, confidentiality, integrity, authentication, and non-repudiation of data.

a. Confidentiality, Integrity, Availability (CIA Triad)

Confidentiality making sure that sensitive information is only accessible by those who are allowed is known as confidentiality. This safeguards patient medical records in a healthcare facility from unauthorized access, including hackers and non-medical staff.

Integrity the correctness and reliability of data are referred to as consistency. Any modifications to a patient's medical record, such as a change in diagnosis or prescription, must be made by a qualified professional and cannot be made accidentally or deliberately in a hospital.

Availability guarantees that systems and data are available when required. In order to provide fast and precise treatment, healthcare systems, including electronic health data, must always be accessible, particularly during crises.

b. Authentication and Non-repudiation

Authentication process of confirming a user's identity. To verify that a user is authentic, hospitals employ biometric scans, ID cards, or passwords.

The inability to retract one's conduct is guaranteed by Non-repudiation. The system records a nurse's time and user ID when they update a record or give medication, demonstrating accountability for any ensuing audits or disputes.

c. Real-world example in healthcare

Maintaining confidentiality in a hospital setting guarantees that patient data is only accessed by authorized staff. To prevent unintentional changes to prescriptions or test findings, integrity is essential. Availability is essential for accessing real-time patient data in an emergency.

Authentication regulates system access, and non-repudiation keeps track of user behavior to ensure accountability, both of which are critical for patient safety and compliance.

Risk Management Table

ASSET	THREAT	VULNERABILITY	RISK LEVEL	TREAT WITH JUSTIFICATION
Patient Records Server	Ransomware attack	Weak encryption	High	Use role-based access control, timely system updates, and end-to-end encryption. Maintains integrity and confidentiality.
External Backup Drive	Theft or loss	No encryption or stored only 0n-site	Medium	Encrypt backup data and use cloud or off-site storage. Ensures availability and confidentiality in case of physical damage or theft.
Staff Workstations	Phishing email Malware infections	Weak passwords No antivirus software	High	Install antivirus software, train staff, and enforce strict password regulations. supports data integrity and authentication.

Reflection Questions

The suggested solutions support IA principles for any specific threats in regard to confidentiality, integrity, availability, authentication, and non-repudiation. Keeping the confidentiality of patient records through encryption and maintaining integrity and authentication through firewalls and virus. It ensures availability of data and systems by offsite backup and system update. I chose mitigation as the first choice for risk treatment because healthcare systems takes care of sensitive and life-critical data. Risk acceptance is not acceptable. When the risks are mitigated the chances of a breach, system downtimes, or getting unauthorized access are reduced as well. As a result, the legal, financial, or even life-threatening repercussions of this non-compliance will also reduce. Taking risks here would be reckless but mitigating risks is consistent with maintaining safe and trusted healthcare operations. To ensure compliance as well as patients' trust and the reliability of operations, organizations must deal with vulnerabilities proactively. However mitigation is the best and most ethical option.

Reference

Whitman, Michael E., and Herbert J. Mattord. Principles of Information Security. 6th ed., Cengage Learning, 2018.

Stallings, William, and Lawrie Brown. Computer Security: Principles and Practice. 4th ed., Pearson, 2018.

National Institute of Standards and Technology (NIST). An Introduction to Information Security (NIST SP 800-12 Rev. 1). U.S. Department of Commerce, 2017, doi:10.6028/NIST.SP.800-12r1.

Pfleeger, Charles P., Shari Lawrence Pfleeger, and Jonathan Margulies. Security in Computing. 5th ed., Prentice Hall, 2015.