1. Information Assurance Principles

A. CIA Triad

- Confidentiality meaning only authorized people have access to confidential information. Requiring an account number or routing number while banking online is a good example of a technique for safeguarding confidential information and protecting sensitive data. Another popular technique for maintaining confidentiality is data encryption. For instance, social networking platforms require user IDs and passwords as part of a routine practice. Additionally, two-factor authentication (2FA) is spreading throughout the financial services and healthcare sectors.
- Integrity ensures data is accurate and unmodified except by authorization. Organizations typically have some way to identify data changes brought on by non-human-caused events, including server crashes or electromagnetic pulses.
- Availability means that the data must be accessible when needed. Keeping up with all system upgrades is also crucial. Other crucial strategies include avoiding bottlenecks and providing sufficient transmission capacity. When hardware problems do arise, redundancy, failover, redundant array of independent disks (RAID), and even high availability clusters might help to avoid major repercussions.

B. Authentication and Non-repudiation

- Authorization. The practice of verifying that someone or something is who or what they claim to be is known as authentication. By verifying that a user's credentials match those in a database of authorized users or a data authentication server, authentication technology gives systems access control. By doing this, authentication guarantees the security of company data, systems, and procedures.
- Non-repudiation is the guarantee that a party to a transaction or communication cannot later contest the legitimacy of their signature or the message they sent. Put another way, non-repudiation ensures that the integrity and source of data can be established, making it difficult for someone to deny sending or receiving a particular piece of information.

C. Real-world example

- A hospital in a health care institution which is limited to electronic health records (EHR) must be confidential (read restricted), updated correctly (integrity), available at the time of need (availability), logged in securely (authentication), and actions must be traceable (non-repudiation).

2. Risk Management Table

Asset	**Threats**	**Vulnerabilities**	**Risk Level**	**Treatment with Justification**
Patient Records Server	Malware, Ransomware	Outdated antivirus, no network segmentation	High	Mitigate – Install updated antivirus, segment network to contain breaches (protects confidentiality and availability).
	Insider Threat	Weak user access controls	High	Mitigate – Implement role-based access control (RBAC) and audit trails (integrity, confidentiality).
External Backup Drive	Theft, Physical Damage	Unencrypted storage, no redundancy	Medium	Mitigate – Encrypt drive and maintain cloud-based redundant backup (confidentiality, availability).
	Malware Infection	Plugged into infected machines	Medium	Mitigate – Scan devices before connection; implement endpoint security (integrity, availability).
Staff Workstations	Phishing, Unauthorized Access	Poor user training, reused passwords	High	Mitigate – Conduct security awareness training and enforce strong password policies (authentication, integrity).
	Data Leakage	USB ports enabled, no DLP software	Medium	Mitigate – Disable unused ports, deploy DLP software

				(confidentiality, non-repudiation).

D. Reflection

- How do your proposed treatments reinforce IA principles?

  The treatments suggested reinforce the principles of IA by directly addressing the threats each poses. For instance, if you were to implement controls to reduce malware attacks on the patient record server, that would help with the availability and integrity of information. Using encryption and access controls can increase confidentiality, especially on physical resources like backup drives.

- Why did you choose that risk treatment approach?

  Mitigation is selected over acceptance because a healthcare environment requires controls in place to protect the patient's information and to adhere to legal obligations (e.g., HIPAA). If a healthcare organization purposely accepts risks such as malware or insider threats, the impact could include loss of patient data or compromise in patient care. Every treatment follows the relevant IA principle to minimize potential impact, maintain trust, and sustain the functionality of the healthcare system.

References

Rouse, Margaret. “Confidentiality, Integrity and Availability (CIA).” TechTarget, TechTarget, https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. Accessed 28 July 2025.