Sergio Hunter

Professor Kirkpatrick

CYSE200T_14936

6 September 2026

Write-Up: The CIA Triad

The CIA Triad is a model created to provide guidance for information security within an organization. The letters in CIA stand for three separate concepts that make up the model: confidentiality, integrity, and availability. Confidentiality involves making sure that digital information in an organization is protected from unauthorized access. This includes passwords, financial records, trade secrets, and more. Integrity involves keeping digital information accurate and trustworthy over its lifecycle by making sure no improper modifications are made. This doesn't just include the time where data is active. It also includes the time where data is no longer needed and decommissioned. Availability involves making sure that any digital information is readily accessible to authorized users. This requires both hardware and software to be maintained properly and consistently.

Alongside the CIA Triad are authentication and authorization. These concepts fall under all three concepts when it comes to protecting digital information. Authentication involves using the correct credentials to gain access to digital information you have authorization to view or alter. Authentication usually requires a user ID, a passcode, and a second way to authenticate a user, usually in the form of a two-factor authenticator, biometric verification like a fingerprint scanner, or physical security keys. Authorization refers to the level of privilege a user has within the organization's systems. An example of this would be a sales manager compared to a CEO. The CEO has authorization to view and change all the emails and phone numbers of the

organization's business partners while the sales manager is not authorized to access business partner information in any form.

Each component of the CIA Triad is crucial for maintaining proper security of organizational information. Confidentiality is important because it makes sure that both internal and external users are properly keeping sensitive information secure from any unauthorized attempts to steal data. Some examples of good confidentiality practices are using two-factor authentication for login attempts, continuous training on potential risk factors, and keeping access privileges up to date. Integrity is important because it makes sure that any data within an organization is only modified or changed by authorized users. It also ensures that data sent over a network is secure from modification as well. Some examples of good integrity practices are implementing access control lists for the organization, providing compliance training for employees about proper security procedures, and monitoring data logs for any integrity issues. Availability is important because it makes sure that any hardware or software responsible for making information available is running properly. This ensures that users always have access to authorized information. Some examples of good availability practices are implementing proper disaster-recovery procedures, regularly updating hardware and software, and implementing security measures to mitigate any malicious attacks.

While the CIA Triad provides quality guidance for protecting digital information, organizations are still vulnerable to attacks. A recent attack involving McKesson detailed that sensitive patient data was extracted by a group known as ShinyHunters. It was reported that "284 million patient data records were exfiltrated. The claim of 284M patient records relates to rows of raw data, not unique patients. Even so, this is clearly a significant data breach (Alder, 2026)." Currently, McKesson's cybersecurity team and third-party experts are investigating the incident

and working to minimize the impacts. As of now, McKesson is informing customers that they don't need to take any actions.

This is a clear violation of confidentiality due to the exposure of the raw data of confidential patient records. While McKesson stated that currently customers don't need to take any action to protect their information, this incident could negatively impact the trust of the organization with handling patient's sensitive data. It could also be the catalyst to other department breaches if ShinyHunters were able to expose an organizational vulnerability. This could lead to significant financial loss from legal action, loss of customers, and loss of business partners due to issues of trust. Unfortunately, data breaches like this are bound to happen, but there are things that can be done to prevent this in the future. McKesson will first have to finish their investigation of the data breach. After that, McKesson will have to figure out where the vulnerability came from and how to patch it. Moving forward, new policies and training will have to be created to educate both customers and staff on the breach and how individuals can remain compliant to prevent any future breaches of the same caliber. Most importantly, McKesson will have to reevaluate their current confidentiality practices and make sure they are up to date.

References

S. Alder (2026, August 31). *ShinyHunters Claims Theft of 284M Records from Healthcare Giant McKesson.* The HIPAA Journal. https://www.hipaajournal.com/mckesson-data-breach/

W. Chai (2023, December 21). *What is the CIA Triad? Definition, Explanation, Examples.* Tech Target. Retrieved on September 6, 2026. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on