

# Solution Guide: CIA Triad and Security Scenarios

---

1. A hospital only allows authorized healthcare personnel within one department to access patient Personal Identifiable Information (PII). When employees move to another department, they lose access.
  - **Solution:** Confidentiality
2. A technology firm maintains an alternate site that is running at all times. Operations can be moved to this location in the event of a major disaster.
  - **Solution:** Availability
3. Employees need key cards in order to enter their company offices.
  - **Solution:** Confidentiality
4. A company hashes their data files to monitor whether information has been tampered with.
  - **Solution:** Integrity
5. Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.
  - **Solution:** Integrity
6. A company employs redundant servers, which means that systems are duplicated. In the event of a malfunction, one server will step in for the other.
  - **Solution:** Availability
7. A company's network infrastructure uses load balancers, which distribute the "load" of tasks, such as file requests and data routing, to a variety of servers. This ensures that no single device is overburdened.
  - **Solution:** Availability
8. A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

- **Solution:** Confidentiality

9. A hacker cracks a hashed message and changes its contents.

- **Solution:** Integrity

10. A hacker launches a DoS attack that floods a website with unwanted traffic from multiple computers and takes the site offline.

## **- Solution: Availability**

---

Trilogy Education Services © 2020. All Rights Reserved.