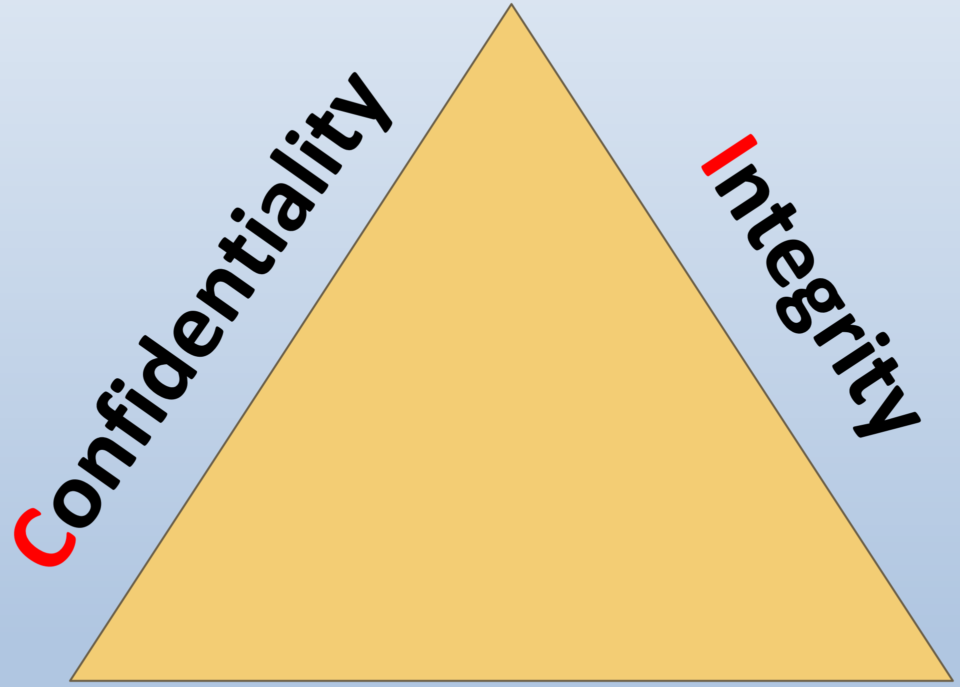
CIA Triad

Restricted Access
to authorised persons



Confidentiality

Integrity

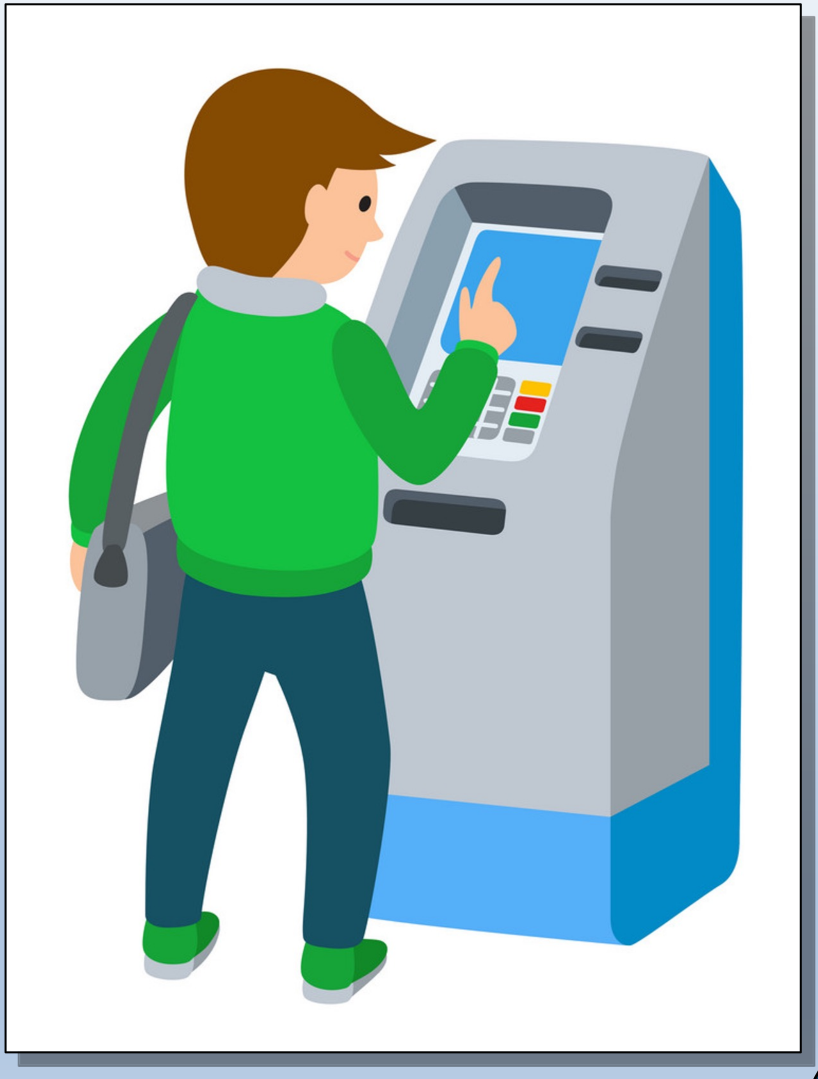
Restricted Changes
to authorised persons

Availability

Available when needed

Example of CIA

- You are the only one who can access your bank account : **Confidentiality**
- No alteration to your account without valid transactions : **Integrity**
- You can access your account anytime : **Availability**



CIA for HealthBridge

- **Confidentiality:**
  - **Authorized access to patient data**
  - **Measures to prevent access to wrong people**
- **Integrity:**

  Accurate and trustworthy patient data

  Access control to prevent unauthorized alteration
- **Availability:**
  - **Accessible patient data for authorized personnel**
  - **Redundant systems and backups**

Basic Definitions

- **Information Security Event** : a change that may violate a security policy or a security control has failed.

- **Information Security Incident** : a security event that have a significant probability compromising information security

Example

- **Information Security event :** Spam email because it may contain a malware

- **Information Security incident** : an employee clicking on a link in spam email that made it through spam filters.

Security Incident for HealthBridge

Data breach: unauthorized access to patient data

Phishing attack: staff disclosed login credentials

Malware attack: loss of important patient data

Proper security controls are crucial for healthcare providers

ISMS framework like ISO 27001 can mitigate potential risks.

Risk

Risk : Effect of uncertainty on objectives

Example : Adam has an exam at 8 AM.

- **Objective** : Arrive on time
- **Uncertainty** : Not waking up
- **Effect of uncertainty** : Missing the exam

Threat, Vulnerability and Risk

- **Threat** : Potential cause which may harm a system or an organisation
- **Vulnerability** : weakness of an asset or a resource that can be exploited by one or more threats
- **Risk** : The potential of a loss or damage when a threat exploit a vulnerability

Threat

Risk of taking control

Vulnerability

HealthBridge Example

Vulnerability: outdated software on employee's computer.

Threat: a hacker exploiting the vulnerability to access patient data.

Risk: compromise of sensitive patient data.

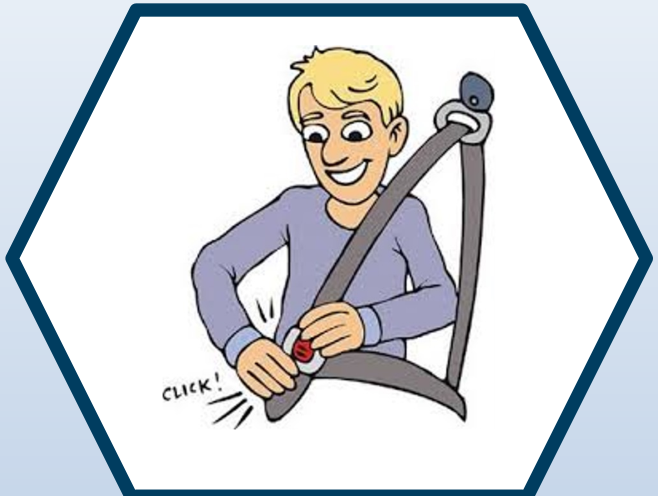
Risk

Risk Owner : Accountable and has authority to manage the risk

Residual Risk

The remaining risk after treatment

- Example : Risk of car accident with the use of seat belt



Risk Acceptance

Informed decision to take a given risk

- Example : Accept the risk of not having a full car insurance

Example of HealthBridge

- CISO is risk owner
- Residual risk may remain

  Example: patch management system

- Risk acceptance when not feasible

  Example: physical security measures