# COM6003 – Epics and User Stories

## User Authentication – Secure login for users –

* User story - As a hospital staff member, I want to be able to securely log into my account to access patient records.
  + Must provide valid username and password.
  + Multi-factor authentication to gain access to accounts with sensitive patient data.
  + Password requirements to maintain security integrity (eg, minimum password length, uppercase and lowercase characters, numbers and symbols).
* Evil User Story – As an unauthorised person I want to gain access to the application by bypassing security measures, allowing me to exploit the systems and gain access to sensitive information.
  + System must have account lockout implemented. Multiple failed login attempts will lock a user’s system for a set period of time before another login attempt can be made.
  + Logging of all login attempts, successful and unsuccessful
  + Denying access to users with inactive accounts

## Patient Management – Adding patient records –

* User Story – As a hospital staff member, I want to be able to update patient information, so that we and maintain patients records and provide care that is up to date.
  + User must have the appropriate permissions to update patient information.
  + Changes to patient information must be tracked, using the ID of the user who made the change and timestamps to create a log of who did what.
* Evil User Story – As an unauthorised person I want to update patient information with incorrect information to compromise data integrity.
  + System must enforce role-based access control for all data modification actions.
  + All updates and actions must be logged and accessible for audit purposes.
  + Any unauthorised actions must trigger alerts

## Surgery Management – Recording Surgery Information –

* User Story – As a hospital staff member, I want to record patient information relevant to the surgery the patient needs, this is so that the surgery details are accurately documented.
  + - * Only users with specific role-based access and add or modify surgery information.
      * Surgery information must be linked to the patient record.
      * All sensitive information must be encrypted and stored securely.
* Evil User Story – As an unauthorised person, I want to modify surgery details without permissions, so that I can alter medical outcomes and disrupt hospital operations.
  + - * Role-Based access control must be regulated and enforced.
      * Audit logging must track all changed made to surgery information, with User ID and timestamps.
      * Any suspicious activity must trigger an alert to system security teams

## Appointment Management – Schedule and cancel patient appointments –

* User Story - As a hospital receptionist, I want to schedule patient appointments so that patients receive the care and services they need in a timely manner.
  + Appointment scheduling must include verification of an available time slot.
  + User must have the appropriate role to create or modify patient appointments.
  + Appointments must be linked to the correct patients record
* User Story - As a hospital receptionist, I also want to ability to cancel appointments, so that resources can be reallocated and maintain the hospitals operations.
  + Only authorised user can cancel appointments.
  + Cancelation of appointments must trigger an email and/or SMS notification to the patient
  + Cancelation of appointments and the reasons of cancellation must be documented
* Evil User Story – As an unauthorised person, I want to cancel patient appointments without authorization so that I can disrupt patient care
  + Role-Based access control must be utilized for appointment cancellation.
  + All cancelations must be logged with user details and timestamps
  + Unauthorized cancellation attempts must trigger alerts.