OLIVER LONG – Secure Development and Deployment (COM6003)

Lab 0: Business Requirements Document

1. Introduction

The Hospital Management Application (HMA) is a secure, mobile-based system designed to optimise the daily operations of hospitals. Its primary objective is to improve efficiency, usability, and patient care for both healthcare professionals and patients, while maintaining full compliance with data protection regulations such as the General Data Protection Regulation (GDPR) and the NHS Data Security and Protection Toolkit (DSPT).

The HMA will combine multiple hospital functions into one single platform, providing secure features for patient registration, appointment scheduling, clinical records management, and role-based access control (RBAC). The system's development will prioritise operational efficiency, data security, patient experience, and scalability to ensure adaptability across different healthcare departments.

2. Key Features

- Patient Registration: Simplifies patient onboarding and digital record creation.
- Appointment Scheduling: Enables efficient booking, modification, and tracking of patient appointments.
- Clinical Records Management: Provides secure storage, retrieval, and maintenance of medical histories and treatment data.
- Role-Based Access Control: Restricts access to authorised data only, ensuring confidentiality and integrity.

3. Stakeholders

- Patients: Primary users who register, manage appointments, and view their medical records. They require a secure, user-friendly interface to access personal data.
- Doctors and Healthcare Professionals: Manage appointments and update patient records. Require quick, reliable access to accurate clinical data.
- Hospital Administrators: Oversee system usage, manage user roles, and ensure compliance with internal and external security policies.
- IT and Security Staff: Maintain infrastructure, ensure uptime, enforce encryption, and manage authentication mechanisms.
- Hospital Management and Policymakers: Focus on improving efficiency, reducing costs, and maintaining compliance through system analytics and reporting tools.

4. Business Goals

1. Operational Efficiency: Automate manual hospital processes to reduce administrative workload.
2. Data Security and Compliance: Ensure full adherence to GDPR and DSPT standards.
3. Improved Patient Experience: Provide intuitive tools for registration, booking, and accessing medical records.
4. Enhanced Clinical Support: Offer real-time access to accurate patient data for healthcare professionals.
5. Scalability and Integration: Enable seamless integration with external systems such as billing, laboratory management, and electronic health records (EHR).

---

5. Epics

Epic 1: Patient Registration and Management
Focuses on secure patient onboarding and data management. Patients can register, update information, and manage profiles, while administrators oversee verification and compliance. Encryption and access controls ensure data integrity and confidentiality.

Epic 2: Appointment Scheduling
Allows patients to book, reschedule, and track appointments. Doctors can view and manage their schedules, while administrators generate performance reports. The feature reduces waiting times and scheduling conflicts.

Epic 3: Clinical Records Management
Provides secure access to patient medical histories, prescriptions, and notes. Doctors can edit and update data; patients have read-only access. Encryption, RBAC, and audit logs protect sensitive information.

Epic 4: Security and Access Control
Implements security mechanisms such as multi-factor authentication (MFA), password encryption, and RBAC. The system monitors and logs user activity to maintain compliance and prevent breaches.

---

6. User Stories and Acceptance Criteria

Epic 1 – Patient Registration

User Story 1:
As a patient, I want to register securely so that I can access hospital services and manage my medical information safely.
Acceptance Criteria:

- Registration requires personal details and a secure password.
- Passwords must meet complexity standards.
- Email verification is mandatory before account activation.
- All transmitted and stored data is encrypted.

User Story 2:
As an administrator, I want to view and manage patient records so that system data remains accurate and compliant.
Acceptance Criteria:

- Administrators can view, edit, or deactivate patient accounts.
- Only authorised staff can modify records, with all changes logged.

Epic 2 – Appointment Scheduling

User Story 1 – Patient Appointment Booking:
As a patient, I want to book an appointment with a doctor so that I can receive medical care at a convenient time.
Acceptance Criteria:

1. Patients can view available time slots by doctor, department, and date.
2. When a slot is selected and available, the booking is confirmed and a notification sent.
3. The system prevents double-booking.
4. Booked appointments appear in the patient's dashboard.

User Story 2 – Doctor Schedule Management:
As a doctor, I want to view and manage my upcoming appointments so that I can plan my schedule efficiently.
Acceptance Criteria:

1. Doctors can view upcoming appointments by date and time.
2. Modifications update patient records in real-time.
3. Unauthorised access attempts are denied and logged.

User Story 3 – Administrative Appointment Reporting:
As an administrator, I want to generate appointment reports so that I can monitor hospital performance.
Acceptance Criteria:

1. Reports can be filtered by department, doctor, or date range.
2. Exported reports anonymise patient data.
3. Non-administrative users cannot access reporting tools.

4. Automated reports are sent securely to authorised recipients.

Epic 3 – Clinical Records Management

User Story 1 – Clinical Record Updates:
As a doctor, I want to update patient records so that treatment information remains accurate.
Acceptance Criteria:

1. Doctors can view and edit patient clinical data.
2. All updates are timestamped and attributed to the doctor.
3. Data is securely stored and updated in real-time.
4. All changes are logged for compliance.

User Story 2 – Patient Access to Medical History:
As a patient, I want to view my medical history so that I can stay informed about my treatments.
Acceptance Criteria:

1. Access requires MFA authentication.
2. Only authorised fields are viewable.
3. Data is encrypted end-to-end (TLS).
4. All access events are logged.

User Story 3 – Data Backup and Recovery:
As an administrator, I want regular data backups so that patient data is not lost in case of system failure.
Acceptance Criteria:

1. Backups run automatically at scheduled intervals.
2. Successful backups are verified and logged.
3. Recovery restores data accurately.
4. Backup files are encrypted and access-controlled.

Epic 4 – Security and Access Control

User Story 1 – Secure User Authentication:
As a user, I want to log in securely so that my data remains protected.
Acceptance Criteria:

1. Valid credentials grant access; failed attempts are logged.
2. After five failed logins, accounts are temporarily locked.
3. MFA is required for all users.

4. Passwords are hashed using strong algorithms (e.g., bcrypt).

User Story 2 – Role-Based Access Management:
As an administrator, I want to manage user roles so that data access aligns with responsibilities.
Acceptance Criteria:

1. Permissions are role-based and enforced immediately.
2. Unauthorised access attempts are denied and logged.
3. Security alerts are triggered for violations.

User Story 3 – System Monitoring and Threat Detection:
As a security officer, I want to monitor system activity so that I can detect and prevent threats.
Acceptance Criteria:

1. All user actions are logged in real time.
2. Repeated failed logins trigger alerts.
3. Logs are immutable and retained for compliance.
4. Detected anomalies initiate incident response procedures.

---

7. Evil User Stories and Mitigations

Epic 1 – Patient Registration
Evil Story: As an attacker, I want to create multiple fake accounts to overload the system.
Mitigation: CAPTCHA verification, email confirmation, IP rate-limiting, and activity monitoring.

Epic 2 – Appointment Scheduling
Evil Story: As an attacker, I want to cancel or modify appointments to disrupt hospital operations.
Mitigation: Authentication with valid tokens, RBAC enforcement, and logging of all appointment actions.

Epic 3 – Clinical Records Management
Evil Story: As an attacker, I want to access patient records without authorisation.
Mitigation: Encryption in transit and at rest, MFA, RBAC, and detailed access logging.

Epic 4 – Security and Access Control
Evil Story 1: As an attacker, I want to intercept network traffic to capture credentials.
Mitigation: HTTPS with TLS, certificate pinning, disabled insecure protocols, and regular penetration testing.

Evil Story 2: As a malicious insider, I want to access data outside my role.
Mitigation: Least privilege enforcement, access logging, audit reviews, and staff security training.

---

8. Prioritised Release Plan

Release 1 – Foundation and Patient Registration
Focus: Secure architecture and patient registration.
Deliverables: Database schema, authentication, registration UI with encryption and CAPTCHA.
Security: Password hashing, RBAC, GDPR compliance.
Objective: Establish a secure and stable foundation.

Release 2 – Appointments and Core Security
Focus: Appointment management and enhanced authentication.
Deliverables: Scheduling module, notifications, and secure sessions.
Security: HTTPS, account lockout, audit logging.
Objective: Improve usability while embedding core security controls.

Release 3 – Clinical Records and Advanced Features
Focus: Clinical data management and integration readiness.
Deliverables: Encrypted record storage, EHR integration, backup and recovery.
Security: MFA, immutable audit trails, data integrity verification.
Objective: Ensure secure handling of clinical information.

Release 4 – Comprehensive Security Enhancement
Focus: Final system hardening and compliance.
Deliverables: Real-time monitoring, intrusion detection, and security analytics.
Security: Continuous vulnerability scanning, penetration testing, DSPT alignment.
Objective: Deliver a fully secure, compliant, and resilient hospital management system.

---

9. Conclusion

The Hospital Management Application (HMA) provides a secure, scalable, and efficient solution for managing hospital operations. By integrating essential functions within a single platform and following a security-first agile development approach, the HMA ensures enhanced patient experience, operational efficiency, and strict compliance with healthcare data protection standards.