Technical Report: Deliverable #2 - User Stories and Use Cases

Project: Health History System

Course: C-SW312: Introduction to Software Engineering

1- Daniel Tarek: 23-101059

2-Karim Ehab: 23-101025

3-Ali Amin: 23-101159

1. Explicit Assumptions

The following assumptions were made during the creation of the User Stories and Use Cases for Deliverable #2:

1. **Stakeholder Identification:** It is assumed that the four stakeholder categories (Internal Operational, Internal Executive, External Operational, External Executive) and the specific examples provided in the Deliverable #1 report (Report.pdf) are correct and complete for the scope of the "Health History" system.
2. **System Scope:** It is assumed that the core functional requirements and system capabilities outlined in the System Vision Document from Deliverable #1 remain the definitive scope for this deliverable. Specifically, that imaging and hospital system integration are out of scope for v1.
3. **National ID:** It is assumed that a secure, unique, and verifiable National ID system is in place and can be used as the primary identifier for both patient record retrieval and user authentication.
4. **Perfect Technology Assumption:** It is assumed that the system will handle all necessary controls (e.g., login, logout, change password, backup/restore) as part of the underlying technology stack, and therefore, these were correctly excluded from the Event Decomposition Technique as per the guidelines.

2. User Stories

Based on the four stakeholder categories identified in Deliverable #1 (Internal Operational, Internal Executive, External Operational, External Executive), we have constructed eight user stories, two for each category.

- **Internal Operational (Developers, UI/UX Designers, Database Administrators)**

ID	User Story	Acceptance Criteria (Given-When-Then)	Verification (Good/Effective)
1	As a Database Administrator, I want to view a real-time log of all record access attempts, so that I can monitor for unauthorized activity and ensure compliance with audit requirements.	Given I am logged in as a Database Administrator, When a user attempts to access a patient record, Then a new entry is immediately added to the audit log with the user ID, timestamp, and access result (success/failure).	Good: It is independent (focused on a single task), valuable (ensures security), estimable, small, and testable.
2	As a UI/UX Designer, I want to ensure the patient record display loads in under 2 seconds, so that doctors can access critical information quickly during emergencies.	Given a doctor is logged in and searches for a patient by National ID, When the search is executed, Then the full patient record is displayed on the screen within 2 seconds.	Good: It is a performance requirement framed as a user story, making it valuable and testable against the system's performance goal.

- **Internal Executive (CEO, CTO, Head of Product Management)**

ID	User Story	Acceptance Criteria (Given-When-Then)	Verification (Good/Effective)
1	As the Head of Product Management, I want to track the number of successful patient record retrievals per day, so that I can measure system adoption and overall usage.	Given I am logged in as a Head of Product Management, When I access the system dashboard, Then I can view a graph showing the daily count of successful patient record retrievals over the last 30 days.	Good: It is valuable for the business, testable (dashboard feature), and independent of other operational tasks.
2	As the Chief Technology Officer (CTO), I want to receive an alert if system availability drops below 99% over a 24-hour period, so that I can immediately address critical infrastructure issues.	Given the system is monitored for availability, When the uptime metric falls below 99% over a 24-hour period, Then an automated email alert is sent to the CTO's registered email address.	Good: It is a critical, high-value story for system reliability and is clearly testable by simulating a system failure.

- **External Operational (Doctors & Nurses, Patients, Hospital Staff)**

ID	User Story	Acceptance Criteria (Given-When-Then)	Verification (Good/Effective)
1	As a Doctor, I want to add a new diagnosis to a patient's record, so that the patient's medical history is kept current and accurate.	Given I have an active session and the patient's record is open, When I enter a new diagnosis and click "Save", Then the diagnosis is added to the record with my user ID and a timestamp, and a success message is displayed.	Good: It is a core, valuable function for the primary user (Doctor) and is clearly testable.
2	As a Patient, I want to revoke a specific doctor's access to my record, so that I can maintain control over my health data privacy.	Given I am logged in to my patient portal, When I select a doctor from my access list and click "Revoke Access", Then that doctor is immediately unable to view my record, and I receive a confirmation email.	Good: It addresses the critical privacy and consent requirement, is valuable to the patient, and is testable.

- **External Executive (Ministry of Health/Regulators, Hospital Administrators, Legal & Compliance Officers)**

ID	User Story	Acceptance Criteria (Given-When-Then)	Verification (Good/Effective)
1	As a Legal & Compliance Officer, I want to generate a report of all emergency override accesses, so that I can audit system compliance with the emergency access protocol.	Given I am logged in as a Legal & Compliance Officer, When I specify a date range and click "Generate Audit Report", Then a PDF report listing all emergency override accesses within that range, including justification and user ID, is downloaded.	Good: It is valuable for compliance, independent, and testable against the system's audit log.
2	As a Ministry of Health Regulator, I want to verify that all patient data is encrypted at rest, so that I can ensure the system meets national data security standards.	Given I am reviewing the system's security documentation, When I check the data storage architecture, Then the documentation confirms that all patient-identifiable data is encrypted using AES-256 encryption.	Good: This is a high-level security requirement framed as a user story, which is valuable for the regulator and testable via documentation/audit.

3. Use Cases: Event Decomposition Technique

The Event Decomposition Technique was applied to the "Health History" system to define requirements by identifying external, temporal, and state events that require a system response.

1. Step-by-step Application of Event Decomposition

A. External Events

External events are initiated by an actor outside the system.

Checklist Item	Event Identification	Use Case Name
External Agent wants information	Doctor requests a patient's record.	Retrieve Patient Record
External Agent wants to update data	Doctor adds a new clinical note.	Update Patient Clinical Note
External Agent wants to change system state	Patient revokes consent for a doctor.	Manage Patient Consent
External Agent wants to log in/out	(Excluded by Perfect Technology Assumption)	-
External Agent wants to perform maintenance	Database Admin generates an audit report.	Generate Audit Report

B. Temporal Events

Temporal events are triggered by a point in time.

Checklist Item	Event Identification	Use Case Name	Trigger Point
System needs to generate a report	Monthly system usage report is due.	Generate Monthly Usage Report	End of each calendar month.
System needs to update data	Patient consent for a temporary access expires.	Revoke Temporary Access	48 hours after temporary access was granted.
System needs to send a reminder	User's password is due to expire.	Send Password Expiration Reminder	7 days before password expiration date.

C. State Events

State events are triggered by a change in the system's internal state.

Checklist Item	Event Identification	Use Case Name	State Change
System detects a critical threshold	System availability drops below 99%.	Alert System Administrator	System_Availability changes from >99% to <99%.
System detects a data integrity issue	A record access attempt fails due to data corruption.	Log Data Integrity Error	Record_Status changes from Valid to Corrupt.

2. Table of Identified Events and Use Cases

The following table summarizes the identified events, categorized by type, the associated stakeholder, and the resulting use case.

Event Type	Stakeholder/User	Event Description	Use Case Name
External	Doctor	Doctor requests a patient's record by National ID.	Retrieve Patient Record
External	Doctor	Doctor adds a new prescription to the patient's file.	Update Patient Clinical Note
External	Patient	Patient changes their consent settings for a specific doctor.	Manage Patient Consent
External	Admin	Admin requests a report of all user activity.	Generate Audit Report
Temporal	Internal Executive	End of the month for business analysis.	Generate Monthly Usage Report
Temporal	System	48 hours have passed since a doctor was granted temporary emergency access.	Revoke Temporary Access
State	System	The system's measured uptime falls below the 99% threshold.	Alert System Administrator

3. Brief Use Case Descriptions

The following table provides a brief description for the core use cases identified.

Use Case Name	Actor	Description
Retrieve Patient Record	Doctor, Nurse	Allows an authorized healthcare professional to search for a patient using their National ID and view their complete medical history (diagnoses, medications, allergies, lab results, notes).
Update Patient Clinical Note	Doctor	Allows a Doctor to add new clinical notes, prescriptions, or test results to an existing patient record. All changes are automatically version-tracked and attributed to the doctor.
Manage Patient Consent	Patient	Allows the Patient to view a list of doctors who have access to their record and to grant or revoke access for specific individuals.
Generate Audit Report	Admin, Legal & Compliance Officer	Allows an authorized user to generate a time-bound report detailing all system accesses, modifications, and emergency override events for compliance review.
Generate Monthly Usage Report	System (Internal Executive)	Automatically compiles and delivers a report to the Internal Executive team detailing key metrics such as daily record retrievals and system availability for the past month.
Revoke Temporary Access	System	Automatically removes the temporary access privileges granted to a doctor after a defined time period (e.g., 48 hours) has elapsed since the emergency override was initiated.
Alert System Administrator	System (Admin)	Automatically sends a high-priority alert to the System Administrator when a critical performance metric, such as system availability, drops below the required threshold (99%).