Software Quality Assurance

SQA Group Project - Assignment #1

Gio Monci, Joseph L, David R, Derek M

Department of Engineering, Florida Gulf Coast University

CEN 4930 - Software Quality Assurance

Dr. Buckley

SQA Process & Checklist....3
1. Introduction....3
2. SQA Process Overview....3
3. Metrics for Evaluating Requirements....3
4. Standards and Frameworks....4
5. Identifying Missing Requirements....5
6. Compliance Verification with Industry Standards....5
7. Classification of Requirements....5
8. Comprehensive Checklist....6
1. Metrics (Requirements check....6
2. Standards and Frameworks (Document check)....6
3. Missing Requirements (Requirement & Document Check)....7
4. Industry Standards (Document Check)....7
5. Classification (Requirement Check)....7
9. Results....8
10. Main Issues Identified....8
11. Corrective Actions....8
Correction of Requirements....9
1. Functional:....9
FR1: User Profile Management....9
FR2: Patient Request Management....10
FR3: Doctor Request Handling....10
FR4: Request Status Management....11
2. Non-Functional....12
NFR1: Security & Compliance....12
NFR2: Performance & Availability....13
NFR3: Maintainability & Scalability....13
Appendix A....14
References....16

SQA Process & Checklist

1. Introduction

a. This section outlines the SQA process and checklist for the Health Connect Project. This section explains our evaluation methodology, quality metrics, standards & frameworks, and a checklist to ensure the requirements are satisfactory.

2. SQA Process Overview

a. As stated in the directions, our SQA process for Health Connect is preventative, which means we are focused on reducing and eliminating bad requirements. Using rules, standards, and good practices with measurable & realistic metrics, to ensure our requirements meet industry standards.

3. Metrics for Evaluating Requirements

a. Completeness: gauge if all necessary requirements are included, this will make sure that the system's functionality is fully conveyed. [1]

b. Clarity: check to see if all requirements are unambiguous, easy enough for a kid to understand, and does have any conflicting interpretations. [1]

c. Feasibility: determine whether or not the requirements can actually be realistically implemented given our constraints (ex: time, technology, budget) [1]

d. Testability: make sure that every requirement can be verified through some sort of testing or inspection. [1]

e. Consistency: Make sure that the requirements don't contradict each other or any part of the document. [1]

4. Standards and Frameworks

a. Requirements Assessment:

   i. ISO/IEC/IEEE 29148-2018 for systems and software engineering requirements.[5]

   ii. CUPRIMDSO Framework (Correctness, Unambiguousness, Prioritization, Realism, Importance, Modifiability, Dependency, Safety, Operationality) [1]

   iii. SMART Criteria (Specific, Measurable, Achievable, Relevant, Time-bound). [1]

   iv. GQM Analysis (Goal/Question/Metric).

b. **Software Quality Assessment:**

   i. ISO/IEC 25010 for evaluating software quality characteristics. [2]

c. **Domain-Specific Standards:**

   i. HIPAA, HL7, FDA SaMD for healthcare compliance. [6][7]

   ii. ISO 13485 for medical device software quality. [9]

   iii. ISO/IEC 27001 for security standards in handling patient data.[8]

5. Identifying Missing Requirements

a. Use Case testing: create real world scenarios and go through each and figure out if we missed any functionality.

b. Stakeholder Interview: get feedback from our client, users, etc. See if they think we are missing some functionality or if it's over the scope.

c. Gap Analysis: Compare our requirements with industry standards and or from SRS / any documentation we can find of similar medical software.

d. Risk Based Analysis: Research and brainstorm with the team about potential risks associated with the software. Do our requirements cover these risks? If not, then implement.

6. Compliance Verification with Industry Standards

a. Requirements Audit**:** Map each requirement to relevant standards.

b. NASA ARM Tool**:** analyzes requirements for various text-based properties such as depth, imperatives and directives. [3]

c. NASA FRET Tool**:** Elicit and formalize requirements into structured formats. [4]

d. Domain Expert Review**:** Obtain feedback from experts to identify gaps and areas for improvement.

7. Classification of Requirements

a. Functional Requirements: Specify what the system should do

b. Nonfunctional: Define the systems quality attributes

8. Comprehensive Checklist

- Simple checklist in Appendix A
- Requirement Check: analyzing the requirement against our SQA process
- Document Check: Analyzing the document against our SQA process
- Key: 1 – Poor, 3 – Adequate, 5 - Satisfactory

1. Metrics (Requirements check

Completeness	1☒ 2☐3☐4☐5☐
Clarity	1☒ 2☐3☐4☐5☐
Feasibility	1☒ 2☐3☐4☐5☐
Testability	1☐ 2☒3☐4☐5☐
Consistency	1☐ 2☒3☐4☐5☐

2. Standards and Frameworks (Document check)

ISO/IEC/IEEE 29148-2018	1☒ 2☐3☐4☐5☐
CUPRIMDSO Framework	1☒ 2☐3☐4☐5☐
SMART Criteria	1☒ 2☐3☐4☐5☐
GQM Analysis	1☒ 2☐3☐4☐5☐
ISO/IEC 25010	1☒ 2☐3☐4☐5☐
HIPAA	1☒ 2☐3☐4☐5☐
HL7	1☒ 2☐3☐4☐5☐

FDA	1☒ 2☐3☐4☐5☐
SaMD	1☒ 2☐3☐4☐5☐
ISO 13485	1☒ 2☐3☐4☐5☐
ISO/IEC 27001	1☒ 2☐3☐4☐5☐

3. Missing Requirements (Requirement & Document Check)

Use Case testing	1☐ 2☒3☐4☐5☐
Gap Analysis	1☒ 2☐3☐4☐5☐
Risk Based Analysis	1☐ 2☒3☐4☐5☐

4. Industry Standards (Document Check)

Requirements Audit	1☒ 2☐3☐4☐5☐
NASA ARM Tool	1☒ 2☐3☐4☐5☐
NASA FRET Tool	1☒ 2☐3☐4☐5☐
Domain Expert Review	1☒ 2☐3☐4☐5☐

5. Classification (Requirement Check)

Functional	1☒ 2☐3☐4☐5☐
Nonfunctional	1☒ 2☐3☐4☐5☐

9. Results

a. Health Connect Document and its Requirements only passed 29/125 of our tests in our SQA process / Checklist. This is a very bad score of 23.2%, meaning that a great amount of work and resources will be needed to fix the document and requirements.

10. Main Issues Identified

a. Upon inspection of the requirements, they were all found to be very poorly written, and they did not adhere to any industry standards [2][5][7][8]. They lack clarity, completeness, atomicity, feasibility, and testability. Upon Inspection of the document, they were missing all the industry standards and frameworks we look for. On top of that, they did not use tools to check their requirements.

11. Corrective Actions

a. We took drastic corrective actions, and we decided to completely rewrite the requirements while trying to retain their original intent. The revised requirements are below and align with industry practices and standards.

Correction of Requirements

1. Functional:

FR1: User Profile Management

1.1: The User Profile Management system shall allow users to create a profile with authentication credentials.

1.2: The User Profile Management system shall store user profile data securely in a database with encryption.

1.3: The User Profile Management system shall differentiate user roles between doctors and patients and enforce role-based access control (RBAC).

1.4: The User Profile Management system shall prevent the creation of duplicate profiles using the same email or government-issued ID.

1.5: The User Profile Management system shall allow users to update their profile information, except for unique identifiers (e.g., username, national ID).

1.6: The User Profile Management system shall provide a secure authentication mechanism, including password hashing and multi-factor authentication (MFA).

FR2: Patient Request Management

2.1: Only registered patients shall be able to submit a medical request.

2.2: Each request shall be assigned a unique Request ID (RID) and a timestamp at submission.

2.3: Patients shall not view or modify requests assigned to other patients.

2.4: The Patient Request Management system shall enforce input validation and sanitization to prevent SQL injection attacks.

2.5: Requests shall be categorized into three states:

- **Open** – Awaiting a doctor's response.
- **In Progress** – A doctor is reviewing the request.
- **Closed** – The request has been resolved.

2.6: The Patient Request Management system shall automatically notify the assigned doctor when a new request is submitted.

FR3: Doctor Request Handling

3.1: Doctors shall only see unassigned patient requests.

3.2: When a doctor opens a request, it shall be automatically assigned to them.

3.3: Once assigned, a request shall not be available for other doctors to claim.

3.4: The Doctor Request Handling system shall allow doctors to communicate with patients via a secure messaging system.

3.5: The Doctor Request Handling system shall allow doctors to change the status of a request to "In Progress" or "Closed".

3.6: The Doctor Request Handling system shall maintain a complete log of all interactions related to a request.

FR4: Request Status Management

4.1: The Request Status Management system shall track the status of all requests and log every status change.

4.2: The Request Status Management system shall enforce status updates in the following sequence:

- **Open → In Progress → Closed** *(Requests cannot skip states)*

4.3: The Request Status Management system shall automatically escalate requests that remain in the "Open" state for more than 24 hours.

4.4: The Request Status Management system shall provide a dashboard for doctors to filter and view their assigned requests by status.

4.5: The Request Status Management system shall prevent requests marked as "Closed" from being reopened.

2. Non-Functional

NFR1: Security & Compliance

1.1: The Security & Compliance system shall encrypt all patient and doctor data both at rest and in transit using AES-256 and TLS 1.3 encryption.

1.2: The Security & Compliance system shall comply with HIPAA and ISO/IEC 27001 security standards.

1.3: The Security & Compliance system shall log all user actions, including request views and updates, with audit trails.

1.4: The Security & Compliance system shall automatically log out users after 15 minutes of inactivity.

1.5: The Security & Compliance system shall require a password complexity policy enforcing:

- A minimum of 12 characters.
- At least one uppercase letter, one lowercase letter, one number, and one special character.

1.6: The Security & Compliance system shall implement account lockout policies after five failed login attempts.

NFR2: Performance & Availability

2.1: The Performance & Availability system shall handle at least 100 concurrent users without performance degradation.

2.2: Database queries shall be executed within two seconds under normal load conditions.

2.3: The Performance & Availability system shall maintain 99.5% uptime, excluding scheduled maintenance.

2.4: The Performance & Availability system shall support automatic database backups every six hours.

NFR3: Maintainability & Scalability

3.1: The Maintainability & Scalability system shall be built using modular architecture to support future feature additions.

3.2: All database transactions shall follow the ACID (Atomicity, Consistency, Isolation, Durability) principles.

3.3: The Maintainability & Scalability system shall support automatic software updates without requiring downtime.

3.4: The Maintainability & Scalability system shall provide a logging mechanism for debugging errors.

Appendix A

Simplified Checklist

Key: 1 – Poor, 3 – Adequate, 5 - Satisfactory

Completeness	1☐ 2☐3☐4☐5☐
Clarity	1☐ 2☐3☐4☐5☐
Feasibility	1☐ 2☐3☐4☐5☐
Testability	1☐ 2☐3☐4☐5☐
Consistency	1☐ 2☐3☐4☐5☐
ISO/IEC/IEEE 29148-2018	1☐ 2☐3☐4☐5☐
CUPRIMDSO Framework	1☐ 2☐3☐4☐5☐
SMART Criteria	1☐ 2☐3☐4☐5☐
GQM Analysis	1☐ 2☐3☐4☐5☐
ISO/IEC 25010	1☐ 2☐3☐4☐5☐
HIPAA	1☐ 2☐3☐4☐5☐
HL7	1☐ 2☐3☐4☐5☐
FDA	1☐ 2☐3☐4☐5☐
SaMD	1☐ 2☐3☐4☐5☐
ISO 13485	1☐ 2☐3☐4☐5☐

ISO/IEC 27001	1☐ 2☐3☐4☐5☐
Use Case testing	1☐ 2☐3☐4☐5☐
Gap Analysis	1☐ 2☐3☐4☐5☐
Risk Based Analysis	1☐ 2☐3☐4☐5☐
Requirements Audit	1☐ 2☐3☐4☐5☐
NASA ARM Tool	1☐ 2☐3☐4☐5☐
NASA FRET Tool	1☐ 2☐3☐4☐5☐
Domain Expert Review	1☐ 2☐3☐4☐5☐
Functional	1☐ 2☐3☐4☐5☐
Nonfunctional	1☐ 2☐3☐4☐5☐
Total Score	___/125

References

[1] R. Halligan and F. Cpeng, “Requirements Quality Metrics: The Basis of Informed Requirements Engineering Management *,” 2014. Accessed: Feb. 06, 2025. [Online]. Available: https://www.ppi-int.com/wp-content/uploads/2019/05/Requirements-Quality-Metrics-Paper-with-Addendum-PPA-005330-9-140710.pdf

[2]“ISO/IEC 25010,” *iso25000.com*, 2022. https://iso25000.com/index.php/en/iso-25000-standards/iso-25010

[3]“ARM Tool,” *Laplante.io*, 2025. https://arm.laplante.io/ (accessed Feb. 06, 2025).

[4]“FRET : Formal Requirements Elicitation Tool(ARC-18066-1) | NASA Software Catalog,” *Nasa.gov*, 2025. https://software.nasa.gov/software/ARC-18066-1 (accessed Feb. 06, 2025).

[5]"ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Requirements engineering," in *ISO/IEC/IEEE 29148:2018(E)* , vol., no., pp.1-104, 30 Nov. 2018, doi: 10.1109/IEEESTD.2018.8559686.

[6]CDC, “Health Insurance Portability and Accountability Act of 1996 (HIPAA),” *Public Health Law*, May 13, 2024. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html?CDC_AAref_Val=https://www.cdc.gov/phlp/publications/topic/hipaa.html

[7]U.S. Department of Health and Human Services, “Summary of the HIPAA privacy rule,” *HHS.gov*, Oct. 19, 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[8]*ISO/IEC 27001:2022* (2022) *ISO*. Available at: https://www.iso.org/standard/27001 (Accessed: 06 February 2025).

[9]Abuhav, I. (2018) *ISO 13485:2016: A Complete Guide to Quality Management in the medical device industry, Second edition*. CRC Press.