Software Requirements Specifications

HealthNet

Group 3

Andrew Hill
Catilina Self
Amy Stewart
Lance Fisher
Patrick Taylor

Software Requirements Specifications

Revision	Date	Author(s)	Remarks
1.0	27 March 2016	Group 3	Initial Writing
2.0	26 April 2016	Group 3	Refined Bugbar & security and design requirements
3.0	28 April 2016	Catilina, Amy, Andrew	Reviewed/Edited use cases and abuse cases

Software Requirements Specifications

TABLE OF CONTENTS

Software Requirements Specifications

1 INTRODUCTION

1.1 Product Overview

The product to be delivered entails a secure means of creating, retrieving, and storing the medical records of patients for the client hospital. In addition to covering the listed client specified requirements, we will also be addressing a number of security concerns that could arise based on the features desired by the client. This program will assist in the storage of files and information associated with patients, nurses, and doctors. It will allow for tracking of all relevant medical data as well as maintain Health Insurance Portability and Accountability Act (HIPAA) standards on personal information.

The following use and abuse cases will detail specifications given by the prospective client based on the supplied HealthIT.gov website. This project will cover the Stage 1 Core Objectives and the Menu Objective requirements.

2 SPECIFIC REQUIREMENTS

2.1 External Interface Requirement

2.1.1 User Interfaces

The user will be able to input information in a text base command line interface.

2.1.2 Hardware Interfaces

The program will take input from a keyboard and output text to a screen.

2.1.3 Software Interfaces

No other software will be interfacing with this program.

2.1.4 Communications Protocols

Does not apply

2.2 Software Product Features

Core Objective - Computerized Provider Order Entry (CPOE) for Medication Orders

Name:	UC-1: Creating User Profiles
Summary	For the program to properly generate reports the program must verify the user is a licensed healthcare professional who can enter orders into the medical per state, local and professional guidelines. Therefore the first step is to have the user create a profile that verifies these credentials.
Preconditions	The application has been launched.
Basic Course of Events	1. The user will select to create a profile.

	2. The user will fill out information about themselves. 3. The user will verify they are a licensed health-care professional who can enter orders into the medical per state, local and professional guidelines. 4. The user will create a login ID. 5. The user will create a login password. 6. The user will verify the login password. 7. The user will select to save the profile.
Postconditions	The profile has successfully been created and it’s information is saved. The user can now login with the specified credentials. The client verifies the specified credentials.

Name:	UC-2: Authenticating User Requirements
Summary	Compare login credentials to the stored list of active user in a specified role.
Preconditions	The application has been launched. The client provides a list of all needed users meeting the requirements to create a CPOE. The client assumes full responsibility for verifying all supporting documents for said users.
Basic Course of Events	1. The user inputs a valid username and password combination. 2. Program verifies the user requirements are met. The program identifies the correct permissions associated with the user.
Postconditions	The user gains access with a valid username and password combination. The user is denied access with an invalid username and password combination. The user is only given access to one role; Patient, Nurse, Doctor or Staff Admin.

Name:	UC-3: Generating/adding to a Parameterized Report
Summary	Create a blank report the program can complete and save in various states. Report is attached to the patient's profile or identify the report in the patient's profile.
Preconditions	The application has been launched.
Basic Course of Events	The user selects the option to create a report or edit a report.
Postconditions	The report has been added or updated successfully to the applications database and linked to the patient’s profile.

Core Objective - Medication Allergy List

Name:	UC-4: Active Medication Allergy List
Summary	Obtain an up-to-date allergy list for a specified patient.
Preconditions	The application has been launched. The user is logged in. An up-to-date list of all patients allergy medication is available or the user can enter the required information.
Basic Course of Events	1. The user searches or selects the patient’s name. 2. The user reviews or updates the patient’s allergy list. 3. The user saves any changes made.
Postconditions	A list of the patient’s allergic medications is available for display. The user can add or edit the Allergy medication list.

Core Objective - Record Demographics

Name:	UC-5: Collection of Patient Demographics
Summary	A questionnaire given at the time of registration

	to collect specific information on each patient in order to view the practice's performance and assist with billing.
Preconditions	The application has been launched.
Basic Course of Events	1. The user selects a preferred language. 2. The user selects a gender. 3. The user selects a race. 4. The user selects an ethnicity. 5. The user selects a date of birth.
Postconditions	The user's data is stored into their profile and saved.

Core Objective - Active Medication List

Name:	UC-6: Active Medication List
Summary	Maintain active medication list.
Preconditions	The application is launched.
Basic Course of Events	1. A list of the Patient's current prescribed medications are listed. 2. The user is allowed to enter additional medication the patient is currently taking.
Postconditions	The information is saved to the patient's record.

Core Objective - Protect Electronic Health Information

Name:	UC-7: Protect Electronic Health Information
Summary	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
Preconditions	The application is not launched
Basic Course of Events	The application is launched and information is either entered or retrieved.

Postconditions	Information is entered or retrieved by an authorized user.

Menu Objective - Patient Electronic Access

Name:	UC-8: Creating Patient Accounts
Summary	For the program to provide patients with access to their health information the program must verify the user is a patient who can view personal records. Therefore the first step is to create patient accounts that allow patients to access to their information.
Preconditions	The application has been launched.
Basic Course of Events	1. A nurse creates an account for a patient. A default account is automatically created for the patient. 2. The nurse enters information about the patient. 3. The nurse is given a loginID and default password for the patient. The nurse provides the patient with this information. 4. At a later time the patient logs into their account with the specified loginID and default password. 5. The patient is prompted to change the passwords IAW password policy. 6. The patient will verify the login password. 7. The patient will select to save the profile.
Postconditions	The account has successfully been created and it's information is saved. The patient can login with the specified credentials. The account is allowed access to reports when published. Patients can view personal health records when logged in.

Menu Objective - Immunization Registries Data Submission

Name:	UC-9: Submission of Immunization Information
Summary	Submit immunization registries to public

	immunization database.
Preconditions	The application is launched. The patient has a current profile. All electronic transmission are via SFTP.
Basic Course of Events	1. The user enters immunization data into the patient's record. 2. The user saves the patient's profile.
Postconditions	The patient's immunization record is uploaded to the public records database.

Menu Objective - Clinical Lab Test Results

Name:	UC-10: Patient Release of Lab Test Results
Summary	Make lab tests available to patients via electronic profile.
Preconditions	The application is launched. The patient has a current profile.
Basic Course of Events	1. The user uploads test data into the patient's profile. 2. The user saves the patient's profile.
Postconditions	The patient's file is updated. The patient can view test documents.

2.3 Software System Attributes

2.3.1 Reliability

Program will function as expected with minimal breakdown. Leaks of file system will not occur.

2.3.2 Availability

The primary attributes of the application (logging information, creating new records, organization of records, etc.) will be available to the medical and administrative personnel. A limited list of functions (accessing records pertaining to themselves) is available to patients, so long as they have permission/authorization to access the specified account and record.

2.3.3 Security

All coding is IAW the CERT C Secure Coding Standard, version 1.0.

2.3.3.1 Security and Privacy Requirements

All user information is subject to and IAW U.S. Privacy Act of 1974.

2.3.3.2 Definition of Terms

Authenticated

Any attack which has to include authenticating by the network. This implies that logging of some type must be able to occur so that the attacker can be identified.

Anonymous

Any attack which does not need to authenticate to complete.

Client

Either software that runs locally on a single computer or software that accesses shared resources provided by a server over a network.

Default/common

Any features that are active out of the box or that reach more than 10 percent of users.

Scenario

Any features that require special customization or use cases to enable, reaching less than 10 percent of users.

Server

Computer that is configured to run software that awaits and fulfills requests from client processes that run on other computers.

WTF

A security vulnerability that would be rated as having the highest potential for damage. And loss of System Control.

Umm

A security vulnerability that would be rated as having significant potential for damage, but less than Critical.

Meh

A security vulnerability that would be rated as having low potential for damage.

Targeted information disclosure

Ability to intentionally select (target) desired information.

Temporary DoS

A temporary DoS is a situation where the following criteria are met:

- The target cannot perform normal operations due to an attack.
- The response to an attack is roughly the same magnitude as the size of the attack.
- The target returns to the normal level of functionality shortly after the attack is finished. The exact definition of "shortly" should be evaluated for each product.

For example, a server is unresponsive while an attacker is constantly sending a stream of packets across a network, and the server returns to normal a few seconds after the packet stream stops.

Temporary DoS with amplification

A temporary DoS with amplification is a situation where the following criteria are met:

- The target cannot perform normal operations due to an attack.
- The response to an attack is magnitudes beyond the size of the attack.
- The target returns to the normal level of functionality after the attack is finished, but it takes some time (perhaps a few minutes).

For example, if you can send a malicious 10-byte packet and cause a 2048k response on the network, you are DoSing the bandwidth by amplifying our attack effort.

Permanent DoS

A permanent DoS is one that requires an administrator to start, restart, or reinstall all or parts of the system. Any vulnerability that automatically restarts the system is also a permanent DoS.

2.3.3.3 Assets and Security Goals

Assets and associated goals.

1. Hash Keys - The Hash Key security goal is to prevent access to the key from all users and utilize the key as a secure method of data retrieval, user verification and authorization for application permissions.
2. Patient Information - The Patient Information security goal is to ensure the limitation of all patient data to authorized users.
3. Healthcare Professional Accounts - The Healthcare Professional Account security goal is to verify and ensure only authorized users have access to specified Health Care Professional accounts.
4. Patient Accounts - The Patient Account security goal is to verify and ensure only authorized users have access to the patient account.
5. System Admin Account - The System Admin Account security goal is to verify and ensure only authorized user have access to the System Admin Account.
6. Log Files - The Log Files security goal is to verify and ensure only the authorized services and users have access to the Log Files.
7. File I/O Availability - The File I/O security goal is to ensure data integrity is maintained and always available to the specified authorized users.

2.3.3.4 Quality Gates/Bug Bars

*These definitions are adapted from Windows Appendix N: Security Bug Bar Sample
Link: https://msdn.microsoft.com/en-us/library/windows/desktop/cc307404.aspx#EAAA

Client

"User interaction" can only happen in client-driven scenario. Normal user interaction - simple user actions, like logging in, viewing medical records, or updating account information. Extensive user interaction - includes users clicking through a series of yes/no application driven decisions and uploading documents.	
WTF	Loss of System Control Elevation of privilege - The ability to either execute arbitrary code or to obtain more privilege than intended. Examples: Running as a System Administrator. Unauthorized file system access: writing to the file system. Execution of arbitrary code without extensive user action. Low privileged user (patients) can elevate themselves to a higher user access (Healthcare professional users). Information disclosure (General) - Cases where the attacker can locate and read information on the system, including system information that was not intended or designed to be exposed. Example: Unauthorized file system access: reading from the file system. Unauthorized file system access: writing to the file system. Disclosure of patient and user personal information such as email, phone numbers, social security numbers and other identifying personal information.
Umm	Information disclosure (Limited) - Cases where the attacker can locate and read information on the system about a targeted user, including system information that was not intended or designed to be exposed.

	Example: Unauthorized file system access: reading from the file system. Unauthorized file system access: writing to the file system. Disclosure of patient and user personal information such as email, phone numbers, social security numbers and other identifying personal information. Spoofing - Ability for attacker to present a UI that is different from but visually identical to the UI that users must rely on to make valid trust decisions in a default/common scenario. A trust decision is defined as any time the user takes an action believing some information is being presented by a particular entity—either the system or some specific local or remote source. Examples: Displaying a different file name in a “Do you want to look up this record?” dialog box than that of the file that will actually be loaded in a default/common scenario. Display a “fake” login prompt to gather user or account credentials Tampering - Permanent modification of any user data or data used to make trust decisions in a common or default scenario that persists after restarting the OS/application. Examples: Modification of significant OS/application settings without user consent; Modification of user data/records. Security features - Breaking or bypassing any security feature provided. Examples: Encryption keys, user authentication, and input validation features.
Meh	Denial of service - Temporary DoS requires restart of application. Example: Opening a file that causes the application to crash.

	Tampering - Temporary modification of any data that does not persist after restarting the OS/application. Information disclosure (untargeted). Example: Leak of random heap memory that may or may not include partial, encrypted patient data.

2.3.3.5 Security and Privacy Risk Assessment

Abuse Case - Unauthorized Access Through Valid Account

Name:	AC-1: Unauthorized Access of Authorized Account
Summary	When an unauthorized user gains access to an authorized user's profile. #WTF
Preconditions	The application has been launched. A user's profile is created with access to account information and records.
Basic Course of Events	1. An unauthorized user enters an authorized user's login information. 2. The unauthorized user is given access to the files available to the authorized user. 3. The user accesses files with unauthorized or malicious intent.
Postconditions	The unauthorized user gains access to privileged information and possibly patient records. The unauthorized user can prescribe and alter medications in patient records if compromising a Nurse or Doctor account.

Abuse Case - Fuzzing

Name:	AC-2: Fuzzing
Summary	User performs actions in contrast to the principle of usability in attempts to find a unexpected or unaccounted for program responses/errors. (Such as crashing,

	providing memory output, etc..) #UMM
Preconditions	Application is launched.
Basic Course of Events	1. User has textfield to input data. 2. User can use keyboard or mouse commands to communicate with the program. 3. User finds crashes or produces an unaccounted for result and proceeds to exploit the program flaw.
Postconditions	Program can crash, data can become corrupted or user can gain access to files.

Abuse Case - Brute Force Login

Name:	AC-3: Brute Force Login
Summary	Attacker uses an application to produce password credentials to login to software. #WTF
Preconditions	Attacker has access to hardware containing HealthNet software
Basic Course of Events	1.User inputs password 2.The unauthorized user is given access to the files available to the authorized user. 3.The user accesses files with unauthorized or malicious intent.
Postconditions	The unauthorized user gains access to privileged information and possibly patient records.

Abuse Case - Malicious Code Input

Name:	AC-4: Malicious Code Input
Summary	A user may be able to utilize the program's text fields to input malicious code. #UMM
Preconditions	Application is launched User has access to text fields presented by the program.
Basic Course of Events	1. User gains access to any text field presented by program

	2. User inputs code into text field to induce malicious software behavior (eg; Exploit stored data, release private information, privilege escalation, etc...) 3. Input is not validated and is allowed to be processed 4. malicious code is allowed to execute
Postconditions	Abusive User defined code is allowed to run.

Abuse Case - Unauthorized Information Retrieval or Manipulation

Name:	AC-5: Unauthorized Information Retrieval or Manipulation
Summary	If the electronic health information is not properly encrypted and programed to only open with the application, then it could be accessible by unauthorized users. #WTF
Preconditions	The application is not launched
Basic Course of Events	An unauthorized user accesses the plain text contents of patient health information. Or an unauthorized user access the encrypted text file and decrypts the information.
Postconditions	Patient information is compromised.

2.3.4 Maintainability

The two Health Net components needing maintenance are the log files and accounts that need disabling/archiving. Maintenance requires a full reinstall due to isolation on client machine.

2.3.5 Portability

The Health Net is specifically built for client Desktops using the Rose Checkers Linux Operating System. This application is not guaranteed to be compatible with other operating systems.

2.3.6 Performance

The performance of Health Net should have the following response time.

The login information is verified within 5 seconds.
The load time for user interface screens should take no longer than 2 seconds.
Queries shall return results within 5 seconds.

2.4 Database Requirements

The Health Net application utilizes a File Input/Output data storage system. All file input/output information is retrieved using a specific identification number verified against the user's permissions.

3 ADDITIONAL MATERIAL

No additional material at this time. Additional topics are covered in the Software Design and Software Testing documents.