Portable Electronic Health Records (PHR)

April 14, 2012

Version 8

Author

[redacted]

Project Advisor

[redacted]

WORCESTER POLYTECHNIC INSTITUTE

SYS 585 – Systems Engineering Capstone

Table of Contents

Table of Contents 2

Abstract 6

1.0 Introduction 7

1.1 Problem Statement 8

1.2 Problem Summary 9

2.0 Needs Analysis 10

2.1 Needs Overview 10

2.2 Referenced Systems 11

2.3 Needs Elicitation 12

2.4 Needs Description 12

2.4.1 Information Security (ND-01) 13

2.4.2 Regulations Compliance (ND-02) 13

2.4.3 Automation (ND-03) 14

2.4.4 Communication (ND-04) 14

2.4.5 Reliability (ND-05) 14

2.4.6 Portability (ND-06) 15

3.0 Concept of Operations 16

3.1 System overview 16

3.2 Operational Needs 16

3.3 Operational environment 17

3.3.1 Electronic Systems 17

3.3.2 Physical environment 17

3.3.3 User Environment 17

3.4 Operational Scenarios 18

3.4.1 Use Case 1 (UC-01) 19

3.4.2 Use Case 2 (UC-02) 19

3.4.3 Use Case 3 (UC-03) 20

3.4.4 Use Case 4 (UC-04) 21

3.4.5 Use Case 5 (UC-05) 21

3.4.6 Use Case 6 (UC-06) 22

3.4.7 Use Case 7 (UC-07) 22

3.5 Concept of Operations Summary 23

4.0 Systems Engineering Management Plan 24
4.1 Project Organization Structure and Staffing 24
4.1.1 NPI: Executive Management 27
4.1.2 NPI: Core Development Team 27
4.1.3 NPI: Core Program Management Team 27
4.1.4 NPI: Core Integration and Test Plan 28
4.1.5 NPI: Sales and Marketing 28
4.1.6 NPI: Global Services 28
4.1.7 PGA: Business Management Team 28
4.1.8 PGA: Program Management Team 28
4.1.9 PGA: Sustaining Engineering 28
4.1.10 PGA: Production Engineering 29
4.2 Work Breakdown Structure 29
4.3 Communication Plan 30
4.4 Change Management method 30
5.0 System Requirements 32
5.1 Functional Requirements 32
5.2 Performance Requirements 33
5.3 Non Functional Requirements 33
5.4 System Constraints 33
6.0 Trade Study 34
6.1 Background 34
6.2 Purpose and Scope 34
6.3 Methodology 34
6.4 Evaluation Factors 36
6.5 Trade Space 38
6.5.1 Biometric Authentication 38
6.5.2 Two Factor Authentication 44
6.5.3 Radio Frequency Identification (RFID) 46
6.5.4 Traditional Computer authentication (Password) 48
6.6 Decision Matrix 49
6.7 Results and Summary 51
7.0 System Reference Architecture 53

7.1 Applicable References 53
7.2 PHR System Architecture All View (AV-1) 53
7.2.1 Architecture Overview 53
7.2.2 Architecture Models 54
7.2.3 Purpose 54
7.2.4 Context 54
7.2.5 Components 55
7.2.6 Summary 55
7.3 System Context 55
7.4 Architecture Operational View 57
7.5 Cloud Infrastructure 58
7.6 Storage and Backup subsystem 61
7.7 Security 63
7.8 System Fault Management 63
7.9 PHR System Reference Architecture Summary 65
8.0 Risk Management Plan 66
8.1 Organizational Structure and Responsibilities 66
8.2 Definitions 67
8.3 Risk Management Process 68
8.4 System Risk identification and documentation 71
8.4.1 System Risk 1 Statement 72
8.4.2 System Risk 2 Statement 72
8.4.3 System Risk 3 Statement 72
8.4.4 System Risk 4 Statement 72
8.4.5 System Risk 5 Statement 72
8.4.6 System Risk 6 Statement 73
8.4.7 System Risk 7 Statement 73
8.5 System Risk Analysis and Prioritization 73
8.6 System Mitigation Plans 74
8.7 Risk Management Communications Plan 75
8.8 Summary 75
9.0 Test and Evaluation Master Plan (TEMP) 76
9.1 System Description and background 76

9.2 Measures of Effectiveness 76
9.3 Process 77
9.3.1 Engineering Validation Testing (EVT) 78
9.3.2 Design Validation Testing (DVT) 79
9.3.3 Manufacturing Validation Testing (MVT) 80
9.3.4 Beta testing 81
9.4 TEMP Program and Schedule 81
9.4.1 Schedule 82
9.4.2 Materials 82
9.4.3 Test Facilities 83
9.5 TEMP risks 84
9.6 Additional Resources 84
10.0 Life Cycle Management Plan 85
10.1 Introduction 85
10.2 Mission 85
10.3 Program 85
10.3.1 General Availability Plan 85
10.4 Business Strategy 87
10.5 Risk Management 87
10.6 Cost and Performance Management 88
10.7 Product Support 88
10.7.1 Organization Structure 88
10.7.2 Total Customer Experience 89
10.8 End of Life Planning 90
10.9 Summary 91
11.0 Bibliography 92

Abstract

The objective of the project was to apply Systems Engineering principles to the design of a portable electronic health records system (PHR). A secondary objective was to leverage existing EMC products and technologies to develop a reference Architecture.

The PHR System was inspired by the author's experience with medical professionals and practices during an illness. The author discovered that most electronic health records (EHR) products were designed mostly for practice management and did not account for patient's needs. In this project, the patient is identified as a key stakeholder and the PHR System requirements are developed to satisfy his needs.

The project followed the Kossiakof System Life Cycle process which is divided into three major components: Concept, Development, and Post Development. Multiple Systems Engineering activities were carried under each phase; occasionally EMC best practices were employed to augment or in replacement of Systems Engineering processes. The lesson learned here is that the Systems Engineering discipline is flexible and adaptable to circumstances, tools and methods.

In summary, the Systems Engineer has a complex set of responsibilities that range from engaging stakeholders to writing detailed specifications. These responsibilities include program management, technical analysis and business analysis which are not traditional technical engineering activities and thus require a particular mindset capable of thinking in a holistic way. This makes Systems Engineering a difficult profession; however, it can be highly rewarding for the right individual.

1.0 Introduction

In the summer of 2010 the author went on vacation with his family to the Dominican Republic. While there, he became ill with an infection which on return to the U.S. resulted in him having to stay home in Franklin, MA for 6 weeks.

During this period, the author was subject to a wide variety of tests ranging from simple blood work analysis to more complicated procedures such as an endoscopy. Most of these tests were carried out in different facilities in the Boston Metro West area

In total, the author was under the care of 5 different medical specialists along with his primary care physician. Unfortunately, each of the specialists was affiliated to a different health network from the other. For example, the gastroenterologist was part of UMASS, while the endocrinologist was part of Boston Metro-West Hospitals.

Interestingly, all of the doctors used some kind of electronic health record. However, the records were not “shareable”, in other words only the doctor attending the author could see the records. Furthermore, these electronic records were not available to him; there was no provision in their system to grant the patient access to the electronic health records. Rather, the doctors had to print copies of their records and results for, which the author then had to carry in a folder for the other physicians to see. The manual effort of keeping each physician up to date with the material he had to carry with himself added stress to his health since he was essentially doing all the coordination between his doctors.

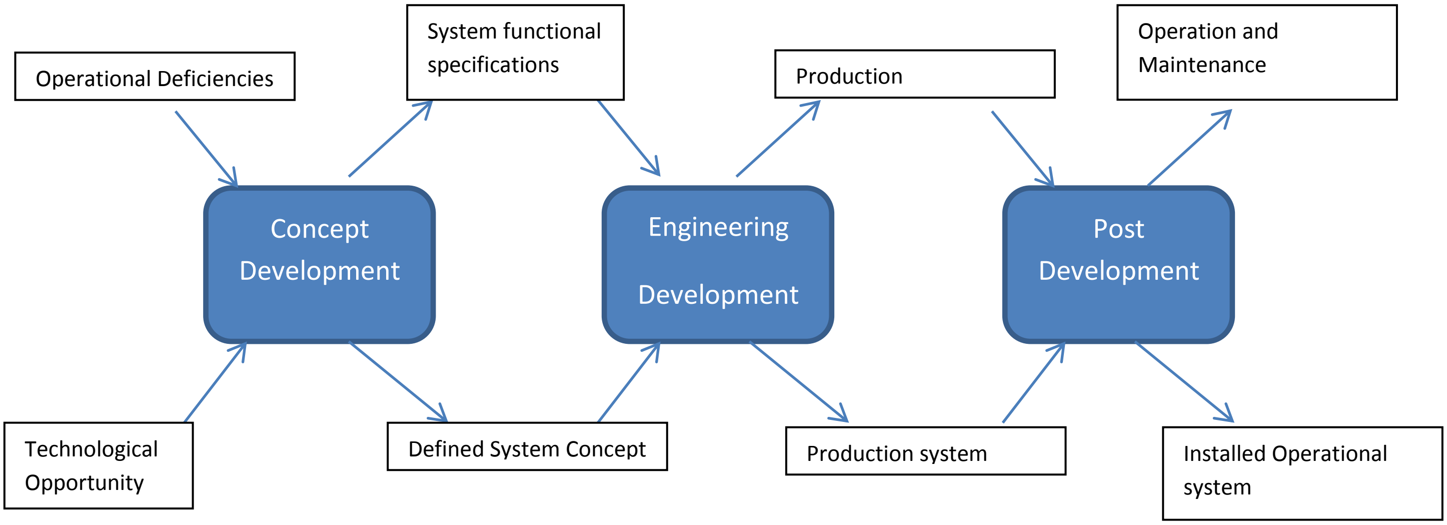
An additional problem the author noticed was that his doctors could not communicate with each other electronically. Although, they could pick up the phone and call, invariably their schedules almost never aligned. This resulted in him also having to carry notes from one doctor to another during his visits or calling their offices to make sure that they had talked before he went to his next appointment. The author believes that had his doctors been able to coordinate, communicate and have access to his complete health records that he would have recovered from the illness faster than he did and would have saved him the added stress of having to actively manage sharing his health records.

1.1 Problem Statement

The purpose of this project is to design a portable cloud based health records (PHR) system by leveraging EMC cloud storage technologies where possible. This project will not focus on the underlying technologies such as storage systems or analytics algorithms although each technology will be sufficiently explained as to make clear its role in the system and how it ties to the system requirements (traceability).

This project will utilize the Kossiakoff Systems life cycle process, shown in Figure 1 and will limit its scope to the Concept Development and Engineering Development phases.

Figure 1 - Kossiakoff. System Life Cycle



In this project, the Concept Development phase will cover the following aspects:

- Needs Analysis
- Concept of Operations
- System requirements
- Systems Engineering Management Plan

And in the Engineering Development phase will cover these aspects:

- Trade Studies
- System Architecture
- Risk management plan
- Test and Evaluation Master Plan

In the final phase, the project will cover these aspects:

- Life cycle management plan

1.2 Problem Summary

The typical health records systems employed by the medical community do not allow for easy patient access or easily shared records between different medical information systems. In addition, the apparent lack of medical electronic -information data sharing standards and the availability of U.S. Government funding have generated a large (750 companies in 2011)-ecosystem of differing solutions which are mostly not compatible with each other (Eisenberg, pars. 2 -3).   The technology to create a portable cloud based electronic health records system may be available already in commercial products. This project's objective is to demonstrate if such solution can be architected by integrating these products utilizing systems engineering principles (Kossiakoff).

2.0 Needs Analysis

The objective of this section is to describe what problem or needs this proposed system will address. It is based on stakeholder input and analysis.

2.1 Needs Overview

The proposed portable health records system is an application and infrastructure that would allow patients and doctors to create, maintain and share a patient's health records in a secure, simple to access and ubiquitous manner.

There are 5 stakeholders or customers identified for this system:

1. The *owner*: of the health records, namely the patient
2. The Health plan *administrator*: health insurance company
3. The *content creator*: Those who generate the content of the health records (physicians, nurses, hospitals, test and laboratory establishments).
4. The *regulators*: essentially the Federal and State government who set regulations and laws regarding health records, privacy and security laws.
5. The *developers*: those who will be developing, engineering and supporting the system

The patient is the primary user for this system. The system will allow the user to access his or her health records anywhere in the world via available electronic platforms such as a web browser or a smart phone application; the patient will also want to share the health records with authorized individuals such as family or medical professionals.

The health insurance company will be a secondary user for the system. This user would generate certain content for the health records, but it should be expected to be focused mostly on health plan administrative tasks, not necessarily visible to everyone.

Content generators such as physicians, medical staff, hospitals, laboratories, etc. would use the system to enter data such as diagnostics, prescriptions, test results, etc.

The government, whether Federal or State, will play a significant role in what functionality the system has due to regulations and laws. In order for the system to be successful it will have to comply with these regulations.

The system as a whole would be a self-contained unit that can be universally accessed with the owner's permission, can be updated with medical information with the owner's permission, and that provides a platform for accessing information and communication between users but again, only with the owner's permission.

2.2 Referenced Systems

While the described PHR System does not exist as envisioned here in the market place, research shows a number of available products that have some of the functionality of our portable and personal health records system.

The products and documents described below are referenced in Section 4.0 of the document.

Allscripts EHR[1]

Physician/practice focused provides records management (patient history), clinical charting, prescribing electronically, lab orders, and patient follow up.

It does not allow for patients to access own records like our proposed system and it is mostly limited to a physician's practice or a network of physicians rather than a universal tool that can interface with any practice in the country.

There is an optional Patient Portal, but it is intended for patient to practices communication such as scheduling appointments, resolving billing questions, etc.

WebMD – PHR[2]

Patient focused provides health records management. It allows for secure, internet based access management and sharing of health records.

It does not automatically interface with physician/practice EHR systems. It requires manual content entering. It also does not allow for communication between patient and medical professionals.

CareCloud EHR[3]

Physician or Practice centered. Provides a complete "practice management system" that features scheduling, billing, Patient Management, analytics.

However, it does not provide patients with access to their own health records

MedeFile[4]

Collects, organizes and gives users access to their medical records. Users must first provide medical history, doctors contact information, insurance data, etc. MedeFile then will gather user's health records from all sources.

[1] http://www.allscripts.com/en/solutions/ambulatory-solutions/ehr.html

[2] http://www.webmd.com/phr

[3] http://www.carecloud.com/

[4] http://www.medefile.com/

Information is entered in the system manually by MedeFile personnel. They have complete access to user records. System provides multiple ways to access information via internet, smart phone applications and thumb drive.

This system is the closest product to the one envisioned in this project. With one large exception – the proposed system does not require a third person to access, view and enter the user's health records; it is done automatically. This is because the proposed system is a combination of "practice focused" system and Patient focused system.

2.3 Needs Elicitation

The elicitation process for the portable electronic health records system was simple. The needs come from personal experience and research of available systems in the market place (refer to section 3.0 for referenced documents and systems).

2.4 Needs Description

Information Security must be an integral part of the system. The contents of the electronic health records need to be protected against unauthorized access. The *owner* of the health records can grant or deny access to the health records and the system must have the appropriate security features to authenticate access privileges.

The HIPPA Security Rule applies specifically to electronic health records. The system must comply with this standard.

The contents of electronic health record must be portable. The owner must be capable of carry with his/her person the records in an electronic device. This allows the owner to view, analyze, communicate and share his/her medical records as needed anywhere in the world.

System must automatically update the electronic health records system with new information from the *content generators* without the need for intervention of third parties.

The system must enable communication between the *owner* of the electronic health records, the *content generator* and the *health plan administrator*. In this manner, all communication is efficient, traceable, searchable and part of the records.

Because health records are critical to ensuring proper care during an emergency, the system must be highly reliable. The PHR must be available 24hrs a day, every day of the year, with disaster recovery and backup solutions in place to ensure data recoverability and backup.

The following table categorizes the needs and references them for traceability.

Table 1 - Needs Reference

Need Ref. Num.	Name	Stakeholder
ND-01	Information Security	All
ND-02	Regulations Compliance	Regulator, developer
ND-03	Automation	Owner, Content creator, Administrator
ND-04	Communication	All
ND-05	Reliability	All
ND-06	Portability	Owner, developer, content creator

2.4.1 Information Security (ND-01)

The information stored in the PHR System is sensitive in nature. It contains the medical history of a person in excruciating detail and there are many reasons why this information should not be available to third parties without authorization. Among these reasons is identity theft that can lead to medical insurance fraud, un-fairly targeting individuals with a complex medical history by unscrupulous companies, etc.

The *owner* of the PHR must be able to have full control of who, when, for how long and to what extend the information in the PHR can be accessed by others.

The system must allow the *owner* to grant access in a simple way to whomever he or she determines. There must be 4 types of access to the PHR:

1. Read only: does not allow to copy, print, download, upload or edit the contents
2. Read/Write access: allows full access, read current content, upload new content, edit content, download content - with backup and verification in a portable data sharing format??
3. Upload: allows uploading content. Does not allow to copy, print, read, write, download or edit content
4. Time limited: content is accessible for an specific amount of time or period. Subject to the above 3 types.

In addition, the information stored in the PHR must be protected against unauthorized access. The system must use data encryption and protection mechanisms.

2.4.2 Regulations Compliance (ND-02)

In 1996 U.S. Congress enacted the Health Insurance Portability and Accountability (HIPPA) Act (Congress). This act is divided in two section or titles; where the first title is focused on health care access and the second title is focused on privacy and security.

Title II of the HIPPA Act has a section dedicated to protecting electronic health information; this section is called *The Security Rule*. The Security Rule provides standards and specifications on three areas: Administrative, Physical and Technical.

The system must comply with Title II of the HIPPA Act and all other U.S. and State laws and regulations.

2.4.3 Automation (ND-03)

Maintaining health records manually is an extremely time consuming effort. There are diagnostics documents, prescription documents, historical information, charts, laboratory results, procedure results, communication between patient and medical staff, etc. The number of variety of information can be overwhelming.

In addition, it can be a matter of life or death that the information in the health records is accurate. The wrong chart, typo in medication dosage, wrong laboratory results, etc. could result in serious medical consequences for the patient and legal liability for the medical staff.

The system must allow for automatic updates of the health records. When a *content creator* generates a new document, the new content must be able to be uploaded to the PHR without the need of a third party.

2.4.4 Communication (ND-04)

It is essential that patients and physicians communicated in order to ensure accurate and comprehensive care of a condition or to prevent a potential problem. Also, if a patient is being treated for a condition by multiple physicians, communication between them, the patient and the insurance provider can greatly accelerate recovery or prevent a more serious situation (DeBronkart).

The *owner* of the PHR must be able to communicate with his or her medical care provider and health insurance. The communication can be an email, voicemail or exchange of documents.

The system must provide a means for communication between the *owner* of the PHR, the *content creators* and the *administrator*. All communication must be private and secure per regulations and recorded in the system permanently.

2.4.5 Reliability (ND-05)

Because the contents of the PHR contain the *owner's* entire medical history, it is essential that they are always available.

In an emergency, medical professionals must be able to access the patients' health records immediately and as needed.

The system must be available 24hrs a day, 7 days a week, every week of the year to provide full access to the PHR to the *owner*; those that PHR *owner* has granted access, the *content creators* and the health plan *administrator*.

The system must also provide means for data integrity and recovery in the case of a system failure or natural disaster.

2.4.6 Portability (ND-06)

The *owner* of the health records or physicians may require access to the contents in a location where there isn’t access to the internet or remote connectivity to the system.

The health records must be able to be transported electronically anywhere in the world for easy access to the contents on a standard computer or electronic device.