DIPLOMARBEIT

Development of an Interoperable Exchange, Aggregation and Analysis Platform for Health and Environmental Data

ausgeführt zum Zwecke der Erlangung des akademischen Grades einer
Diplom-Ingenieurs in Biomedical Engineering
eingereicht an der Technischen Universität Wien, Fakultät für Elektrotechnik und Informationstechnik

von

Mhd Adnan Jouned
Matr.Nr. 01529935

unter der Anleitung von

Projektass. Dipl.-Ing. **Florian Thürk**
Ao.Univ.Prof. Dipl.-Ing. Dr.techn. **Eugenijus Kaniusas**

Institut für EMCE
Gußhausstraße 25/354
1040 Wien
Austria

Kurzfassung

Telemedizin wird aufgrund der kontinuierlich steigenden Krankenhauskosten immer beliebter. Kosten können eingespart werden während die Wahrscheinlichkeit auf erneute Einweisung drastisch sinkt. Es wurden bis dato schone einige verschiedene Telemedizinsysteme entwickelt; das große Problem besteht in der fehlenden Kommunikation. Die Systeme sind separat gehalten und können deshalb nicht untereinander Daten austauschen oder anderweitig miteinander arbeiten. Dies könnte jedoch Kosten weiter senken sowie die Fehlerquote, die bei manueller Übertragung unabdinglich ist, reduzieren. Die Interoperabilität von Gesundheitsdiensten würde eine gute Grundlage für den Austausch und das richtige Verständnis von Informationen von verschiedenen Systemen, einschließlich der Telemedizin, bieten.

Es wurden mehrere Studien zu Gesundheitsinformationssystemen auf der Grundlage verschiedener Gesundheitsinteroperabilitätsstandards durchgeführt. Leider ziehen nur wenigen von ihnen den neusten Standard in Betracht: Dabei handelt es sich um „Health Level Seven“ auch HL7, der im Bereich "Fast Healthcare Interoperability Resources" oder kurz FHIR, entwickelt wurde. Der Fokus liegt zumeist entweder auf der Anwendung des Standards oder auf die Entwicklung und Implementierung des Programms. In diesem Artikel werden wir uns umfassend mit dem HL7-FHIR-basierten Telemedizinsystem befassen, welches kurz zusammengefasst, Daten von Gesundheitsüberwachungsgeräten per Smartphone an den zentralen Aggregationsserver übermittelt.

In diesem Exzerpt werden wir auf die theoretischen Aspekte eingehen, die beim Design von Gesundheitsinformationssystemen auf struktureller, semantischer und syntaktischer Ebene berücksichtigt werden müssen um Interoperabilität zu gewährleisten. Diese Zusammenfassung soll einen detaillierten Überblick über die Erfassung von Gesundheitsdaten vom Ursprungsgerät, sowie deren Übertragung durch Bluetooth Low Energy (BLE) an ein Smartphone, verschaffen. Ferner werden wir uns mit der Umwandlung der erfassten Daten in das HL7-FHIR-Protokoll beschäftigen sowie mit der daraus resultierenden Möglichkeit der Integration des semantischen Standards in FHIR. Auch der Datenaustausch mit dem Server und der Aufbau der Programmieranwendungsschnittstelle zum Empfangen und Weiterleiten von Informationen an Datenbankverwaltungssysteme wird analysiert. Darüber hinaus wird die Beziehung zwischen den Programmierumgebungen und den in der Implementierung verwendeten Protokollen wie FHIR, Bluetooth GATT-Profile und SSL erläutert sodass Sie am Ende eine gute Übersicht über den Datenfluss im Gesundheitswesen, inklusive aller Systemteile haben werden.

In der Praxis ist es gelungen, Smartphone-Anwendungen und die notwendige Server-Software bereitzustellen, die es ermöglicht sich Blutdruckmesswerte und die Herzfrequenz auf dem Smartphone anzeigen zu lassen. Diese Daten wurden über Bluetooth Low Energy an das mobile Gerät und dann gemäß den Interoperabilitätsstandards, an den zentralen Server gesendet. Die Daten auf dem Server werden Teil eines Gesundheitsinformationsmanagementsystems und sind für andere Systeme die das HL7 FHIR Interoperabilitätsprotokoll verwenden, zugänglich und übertragbar.

Diese These ist Teil der "Interoperablen Austausch-, Aggregations- und Analyseplattform für Gesundheits- und Umweltdaten", die eine Plattform für die Integration von Gesundheitsdaten mit Big-Data bieten soll, um analytische Verarbeitung durchzuführen. Das hat das Potenzial, intelligente und effiziente Gesundheitsversorgung zu liefern und versteckte Korrelationsmuster zu entdecken, die zur früheren und genaueren Diagnose von Krankheiten beitragen können und damit sogar menschlichen Spezialisten voraus sein können.

Abstract

The continuous growth in hospitalization-related healthcare costs has been a strong incentive for the spread of telemedicine systems, which contributes to cost savings and reduces the risk of patient re-hospitalization. Although there are many systems currently in place in the field of telemedicine, most of them lack the ability to operate and connect with other systems to exchange information, which results in turn in a cost burden and an increase in the rate of medical errors. Health interoperability provides a solid ground for proper exchange and understanding of information between different systems including telemedicine.

Several studies have been conducted on healthcare information systems based on different Health interoperability standards, but few of them are looking for the latest standard "Fast Healthcare Interoperability Resources" FHIR which has been developed by Health Level seven HL7. On the other hand, current studies on telemedicine systems focus either on the application of the standard itself or on the design and implementation of telemedicine without paying attention to health interoperability. In this work, we provide a wide overview of a HL7 FHIR based telemedicine system, which transmits data from health monitoring devices via smartphone to the central aggregation server.

This work covers theoretical aspects on how to design the healthcare information system components that support interoperability with its structural, semantic and syntactic levels. To reflect the theoretical study into practical telemedicine system, this work provides a detailed view of healthcare data acquisition and transmission from health monitoring device via Bluetooth Low Energy (BLE) to a smartphone, highlighting the role of BLE healthcare profiles. Further, the conversion of these acquired data into HL7 FHIR protocol, and the possible integration of semantic standard into FHIR to make data ready to be transmitted to the server are covered. To exchange data from the server point of view, the work also explains the process of building a programming application interface to receive information and pass it to database management systems. In addition to describe the inter-relationship between the programming environments and the protocols used in the implementation like FHIR, Bluetooth GATT profiles, and SSL, and provide a view of healthcare data flow in the parts of the system.

The practical part has succeeded in providing smartphone applications and server software that enables developed telemedicine system to acquire blood pressure signs and heart rate from health monitoring devices. These can be send it via BLE to a smartphone and then to the central server according to health interoperability standards. The data on the server will become part of a healthcare information management system and will be accessible and transferable by other systems using the HL7 FHIR Interoperability standard.

This thesis is part of the "Interoperable Exchange, Aggregation and Analysis Platform for Health and Environmental Data" project which aims to provide a platform for the integration of healthcare data with Big-data to perform analytical processing, that has the potential to deliver smart and efficient health care and reveal hidden correlation patterns which can contribute to earlier and more accurate diseases diagnosis, which in some cases could perform better than human specialists.

Acknowledgements

This work would not have been possible without the support of many persons.

All thanks to Mr. Florian Thürk, the supervisor who did not spare the assistance and support, I am especially indebted to Prof. Kaniusas Eugenijus, Chairman of Study Commission Biomedical Engineering at TU Wien, who have been very supportive and worked to provide us biomedical engineering students with the academic knowledge to pursue our goals.

I have to thank Mr. Philipp Urbauer, for his great help and motivation along the project, and Prof. Stefan Sauermann Program Director of Medical Engineering & eHealth at Fachhochschule Technikum Wien, who have been very encouraging and supportive.

Nobody has been more important to me in the pursuit of this project than my loving wife and study friend Nada, whose love and guidance are with me in whatever I pursue, who provide unending inspiration. I would especially like to thank my amazing friend and work colleague, Mahmoud, hoping for him the best future carrier.

Finally, I would like to acknowledge the people who mean the world to me, my parents and family.

List of Abbreviations

AES	Advanced Encryption Standard
API	Application program interface
App	Application
ART	Android runtime
ASTM	American Society for Testing and Materials
ATT	Attribute Protocol
BAN	Body Area Network
BLE	Bluetooth low energy
BLP	Blood pressure profile
BPM	Beats Per Minute
BSN	body sensor network
CCM	Communications Control Mode
CCOW	Clinical Context Object Workgroup
CDA	Clinical Document Architecture
CDA	Clinical Document Architecture
CGMP	Continuous Glucose Monitor Profile
CSRK	Connection Signature Resolving Key
DBP	Diastolic Blood Pressure
DC	Direct Current
DICOM	Digital Imaging and Communications in Medicine
ECDH	Elliptic curve Diffie–Hellman
ECG	Electrocardiogram
ERD	Entity Relationship Diagram
FCC	Federal Communications Commission
FHIR	Fast Healthcare Interoperability Resources
GAP	Generic Access Profile
GATT	Generic Attribute Profile
GLP	Glucose Profile
HAL	Hardware abstruction layer
HCI	Host Controller Interface
HIMSS	Healthcare Information and Management Systems Society
HL7	Health Level-7
hPa	Hectopascal
HTP	Health Thermometer Profile
HTTPS	Hypertext Transfer Protocol Secure
IC	Integrated circuit
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IOS	iPhone Operating System
IP	Internet Protocol
IPC	inter process communication
ISPs	International Ship and Port Security

ITK	The Interoperability Toolkit
JSON	JavaScript Object Notation
L2CAP	Logical Link Control and Adaptation Protocol
LCD	Liquid Crystal Display
LL	Link Layer
LOINC	Logical Observation Identifiers Names and Codes
MAP	Mean arterial pressure
MeSH	Medical Subject Headings
MITM	Man in the middle
mmHg	Millimeters of Mercury
MRN	Medical Record Number
MVC	Model View Controller
MySQL	My Structured Query Language
NHS	National Health Service
open MAX AL	Open media acceleration
openGL ES	Open graphic library for embedded system
PHP	Personal home page
PHY	Physical Layer
REST	Representational State Transfer
RESTful	Representational State Transfer
RIM	Reference Information Model
SBP	Systolic Blood Pressure
SDK	Software Development Kit
SIG	Bluetooth Special Interest Group
SM	Security Manager
SNOMED CT	SNOMED Clinical Terms
SOAP	Simple Object Access Protocol
SQL	Structured query language
SSL	Secure Sockets Layer
SS-MIX	Standard Structured Medical Information exchange
UI	User Interface
UML	Unified Modeling Language
UMLS	Unified Medical Language System
URL	Uniform Resource Locator
UUID	Universal unique identifier
UV	Ultraviolet
VO2	Oxygen Consumption
WBAN	Wireless Body Area Network
WHO	World Health Organization
WSDL	Web Services Description Language
XML	Extensible Markup Language
BLE	Bluetooth Low Energy
PHD	Personal Healthcare Device

Contents

1. Introduction 10
1.1 Problems and challenges 11
1.2 General Project Overview 12
1.3 Goals 13
2. Health Interoperability 14
2.1 Introduction 14
2.2 Bio-medical data problem 14
2.3 Health Interoperability aspects 14
2.3.1 Foundational Interoperability 14
2.3.2 Structural & Syntactic Interoperability 15
2.3.3 Semantic interoperability 15
2.4 Implementation approach 17
2.4.1 Interoperability interface layers design 18
3. Health monitor device – Mobile device data transfer 20
3.1 Introduction 20
3.2 Choose wireless protocols for health/medical data transmission 20
3.2.1 Hub concept / Wireless body area network (WBAN) 20
3.2.2 Power efficiency 21
3.2.3 Compatibility and interoperability 21
3.2.4 Data transmission speed and latency 22
3.2.5 Other aspects 22
3.2.6 Conclusion 22
3.3 Bluetooth low energy for health data 23
3.3.1 Bluetooth Low energy Architecture 23
3.3.2 Generic Access Profile (GAP) 24
3.3.3 Generic Attribute Profile (GATT) 24
3.4 Implementation approach 26
3.4.1 Health Monitoring Device 26
3.4.2 GAP layer & GATT Layer 26
3.4.3 Application layer 28
3.5 Other concerns 31
3.5.1 Security measures in BLE for healthcare data 31
3.5.2 User privacy 31

3.5.3 Integration of non-medical data with medical data 32
3.5.4 User data storage in smart devices 32
4. Mobile device – Aggregation server data transfer 33
4.1 Introduction 33
4.2 Choose standard for health care data transmission 33
4.2.1 HL7 versions 33
4.2.2 CDA 34
4.2.3 Other standards 35
4.2.4 Conclusion 36
4.3 HL7 FHIR 36
4.4 Implementation approach 40
4.4.1 Smartphone part 40
4.4.2 Server API side 45
4.5 Other concerns 57
4.5.1 User privacy and security issues 57
4.5.2 Non-expert user problem 57
5. Testing and evaluation 58
5.1 System testing and Evaluation 58
5.1.1 Method 58
5.1.2 Results 58
5.1.3 Discussion 58
5.2 Physiological Measurements and Evaluation 59
5.2.1 Introduction 59
5.2.2 Method & Measurements 59
5.2.3 Results 60
5.2.4 Discussion 61
6. Conclusion 62
7. Appendices 63
7.1 Health care BLE profiles 63
7.2 GATT health related services and characteristics UUID 64
7.3 Health monitoring device technical specification 66
7.4 Blood pressure device parsed output 67
7.5 HL7 FHIR patient resource XML template 68
7.6 HL7 FHIR Observation resource XML template 69
7.7 HL7 FHIR DiagnosticReport resource structure 70
7.8 HL7 FHIR Patient, Observation resources UMLs 71

7.9 HL7 FHIR Practitioner, Organization and DiagnosticReport resources UMLs 72
7.10 User interface for observation update and history 73
8. Bibliography 74
List of Figures 78
List of Abbreviations 5

1. Introduction

The significant scientific advancement which has taken place in the last decades has been clearly reflected in improving living conditions, which led in turn to noticeable increase in the expectation of life worldwide. Consequently, the global population aged over 60 years has been doubled in the last three decades to reach almost one billion today [1]. This population usually need more health care, posing new challenges to health care services. In addition, modern lifestyle is accompanied with the spread of various disease, especially chronic ones, such as diabetes and blood pressure disorders [2]. Telemedicine which allows distant patients monitoring and links health care service provider and recipient can provide innovative solutions to face these challenges.

In 2014 around 21% of Austrians have chronic high blood pressure diseases, 46% of people were more than 60 years old [3], for those telemedicine can offer better health care, deliver more comfortable treatment experience and reduce expenses, even from national health care planning perspective, this could lower the pressure on health care service demand, provide solutions in emergency cases like disasters and more, it provides huge amount of vital data to use for research purposes.

On other hand, telemedicine systems are in need for common ground to exchange information between systems, protect user privacy, reduce medical errors and provide stable service. This is achieved by health interoperability [4], which uses standards and techniques to provide seamless information flow and confirms mutual understanding between systems.

This thesis is a part of “Interoperable Exchange, Aggregation and Analysis Platform for Health and Environmental Data” which is part of the research project INNOVATE (funded by the City of Vienna Municipal department 23 Economic Affairs, Labour and Statistics), which aims the establishment of development-kits regarding interoperability, open data, security, usability and accessibility for eHealth solutions. The project goal is to deliver tele-monitoring system which is able to transfer data from health monitoring devices to aggregation server over smartphones, then analyze this data and Big-data from other resources, to find any hidden correlations pattern. At the same time, system design and implementation have to follow health interoperability standards. This thesis covers the acquisition of vital data from patient using health monitoring devices, transmission this data to mobile device, as well as transmission to aggregation server, and focuses on delivering this system according to health interoperability standards.

1.1 Problems and challenges

Information and communication technologies that have utterly changed our lifestyle, have great potentials to contribute to contemporary health problems solutions [5], one of these problems is the growing costs of observation hospitalizations [6]. In Austria the costs per bed in hospitals have increased 5% in ten years [7], many patients have to stay in hospitals after recovery just for monitoring, which makes them less comfortable and leads to additional cost. Telemedicine systems can be used to monitor patient remotely after discharge from hospital, of course discharge decision is made by the specialist when patient medical condition allows.

Telemedicine systems contains health monitoring devices or personal health devices which are connected to Health care system, in which specialists can have continuous monitoring of patients, which is resulted in improving in their health conditions, reduction of re-hospitalization chances and reduction of related expenses [5].

Electronic information sharing is essential for Telemedicine, where exchanging data correctly between different systems is the point, and since systems are usually different in terms of structure and communications, there is always a chance to meet problems with data exchange, this problem could be larger between health care systems in different countries, since even the medical terminologies could differ, in that sense information technologies systems should be built to cross this gap and provide unified model to represent and exchange information, this is achieved by health interoperability.

Today there are many standards competing to offer wide framework of health interoperability, some of them are introduced based on domestic needs such as SS-MIX in Japan and xDT-family in Germany, while others introduced and succeeded on larger scale such HL7 version 2.x [8]. In addition to other standards that have emerged recently such as HL7 FHIR, which looks promising to solve many problem that were pending in other standards. Aside from health interoperability issues, increasing usage of information and communication technologies nowadays, poses new challenges to telemedicine in respect of information security and user privacy.

According to IBM “Cyber Security Intelligence Index" of 2016, health care industry was the most vulnerable field of cyber attacks, with more than 100 million healthcare records were breached only in year 2015 [9], and since the storage of patients’ information is not a decision, the privacy and security of this data are fundamental to avoid such breaches, in that sense protection of health care information is part of the health care service systems.

In contrast, ubiquitous ICTs usage resulted in enormous complex amount of data which is known as Big-data. This data is so valuable, since it covers almost every field in our lives, and if we consider that health care data collected such as patients’ vital signs, radiology data and specialists’ diagnostic information is rising around 50% every year and will reach 2,314 exabytes by 2020 [10], then the combination of these data: healthcare collected information and other Big-data resources can provide precious input for artificial intelligence and analysis algorithms, which in turn has the potential to deliver smart and efficient health care and reveal hidden correlation patterns which can contribute to earlier and more accurate diseases diagnosis [11], which in some cases could perform better than human specialists, as is the case with heart attacks [12]

1.2 General Project Overview

This thesis is part of "Development of an Interoperable Exchange, Aggregation and Analysis Platform for Health and Environmental Data" project, which has been started in 2016 and implemented at University of Applied Sciences, Technikum Wien. Figure 1 shows the main components of the project, starting from collecting data from participants and ends with analytical platform.

The first step starts when health motoring devices are used to collect vital data from participants, then data is transmitted using Bluetooth low energy to smartphone, so all devices which could be used in this step must have Bluetooth Low Energy in order to be integrated in this system, to get benefits of BLE features to achieve standard connections. Blood pressure monitoring device which uses BLE and blood pressure profile BLP is used in the initial phase to provide practical use-case, participants in this project must measure their blood pressure and use developed smartphone application to transfer monitoring device values. When participant smartphone device receives vital data, it displays the values on screen and then converts this data into proper FHIR resources to send it to the server.

From server point of view, Application Programming Interface is essential to provide the capacity to connect to other systems, so we will design and build programming interface which can receive data from smartphone device and make it suitable for storage. API is used as well to send measurements that have been made by the participants to their smartphone, so each participants can see his. Also in this phase we concern about authentication and authorization, to allow users to register and login using their smartphones. All connections between mobile device and server should be secure and protected. This implementation focuses on health interoperability between server and other parts including mobile device based on FHIR resources and Web programming framework Yii2.

In order to store healthcare data in the server we worked to choose and provide a secure, extensible, and interoperable storage reservoir, to fulfill these requirements, comparison between current technologies is made, then "HAPI FHIR" databases systems and "FHIRBASE PostgreSQL" are chosen. The resulted storage developed system permits a wide range of basic and advanced management actions such as creation, editing, removing of FHIR resources and viewing a browsing history, also the ability to switch between different database systems is included.

Additionally to collect and integrate environmental data which is consider as a sample of Big-data with health care data, an application programming interface (API) from the Medical University of Vienna is used, which contains the exposure concentration values of pollen of different fine particles in Vienna's ambient air [13]. This API provided concentration for ten pollen types in semi-real time. Which provides the large variety of datasets as input.

Finally, customized analysis platform have designed and built to offers the ability to analyze all data (medical and big-data) which has been stored in the aggregation server. To achieve this, special interfaces for statistical analysis are developed to carry out analytical mathematical processes to show correlation patterns between datasets.

So the workflow of the project can be summarized in the following tasks:

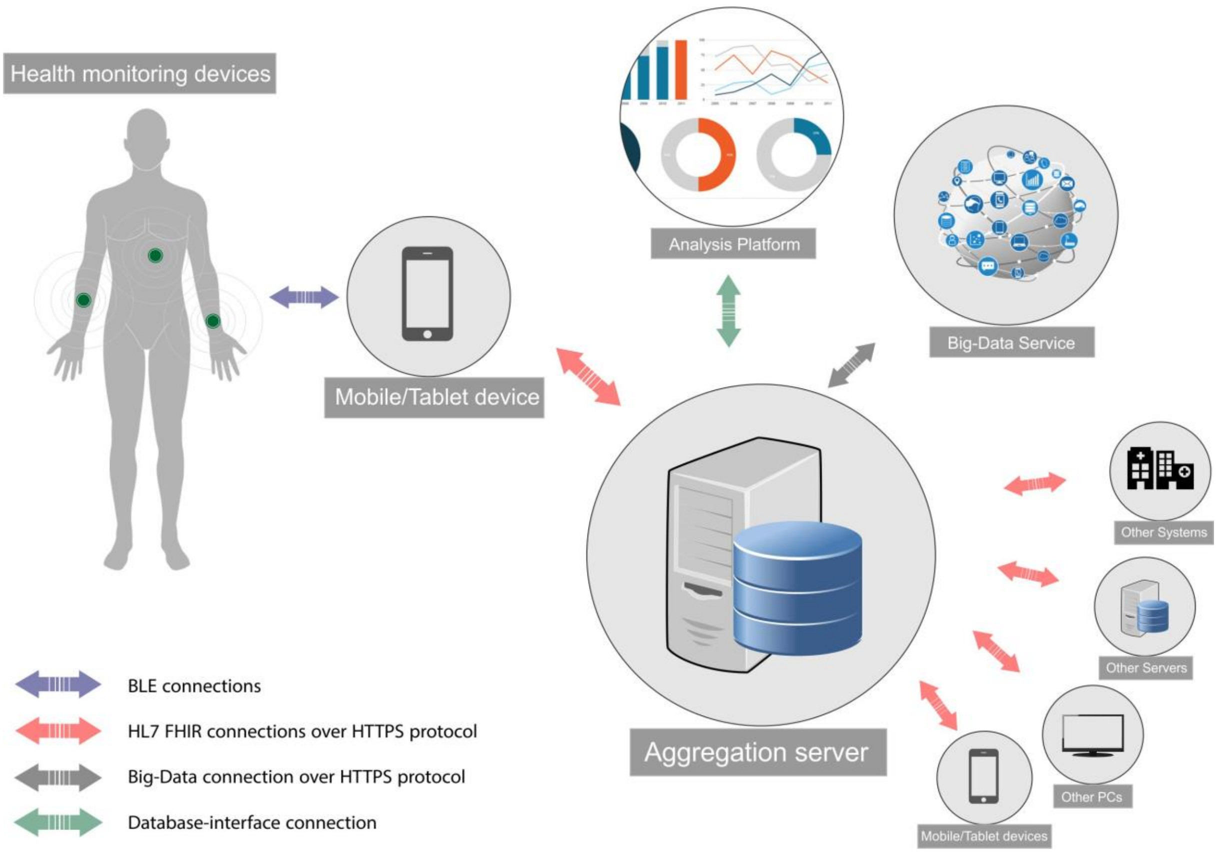


Figure 1 Structure of the project shows vital data acquisition and the transmission to smartphone and the server, also shows big data resource collection and analysis platform [reformed from original project picture]

A. Vital data collecting from Health monitoring device
B. Send data from smartphone device to aggregation server
C. Build server interface to request and respond to smartphone to achieve interoperability
D. Choose and build aggregation storage reservoir for healthcare data.
E. Retrieve data from big data resources
F. Make analysis between vital collected data and big-data

Tasks D, E and F were done by my colleague during the course of his master thesis [14], so this thesis provides study and implementation of the points A, B and C.

1.3 Goals

The thesis aims to offer theoretical study of the structural, syntactic and semantic level of interoperability between project parts, choosing the optimum solutions and tools to provide information security and patient privacy protection alongside with health interoperability for the communications between smartphone and server.

The work also tries to focuses on vital data transmission from health monitoring device to smartphone then to aggregation server according to health interoperability standards. After that, the project will be used in one use-case to measure patients' blood pressure value, and apply statistical tests.

2. Health Interoperability

2.1 Introduction

Interoperability usually refers to an umbrella of concepts and standards in which different technologies are used to achieve the ability of the systems to work together and share information without boundaries or restrictions. Firstly this concept were developed for information technology disciplines to allow higher extent of free information exchange and usage between two or more different components and systems [15], and whereas "compatibility" were focusing more on small pairs of entities, interoperability addressing providing solutions for larger groups.

In healthcare it could denote to "the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged" as it defined by HIMSS [16], since it focuses on both data transmission and interpretations to have the same meaning by different systems.

Health interoperability plays key role in improving health service including reduce costs and provide better care for patients [4].

2.2 Bio-medical data problem

Most of the patients' information are recorded and placed at different locations using different configurations and representations. This could start from health insurance agencies and extend to cover doctors and specialists clinics, health care centers, laboratories, radiology centers, hospitals and others facilities. Furthermore different countries and states usually have different health infrastructures, different medical vocabularies and abbreviations, pharmaceutical drugs names, data representations and health care regulations which results in loosing of large part of health care service efficiency and build barriers for easy data exchanges.

If patients' information were delivered in a way that all health service parts are able to access and provided in uniformed usable format, this would help to provide higher quality, cost-effective and most importantly patient centered services. Today there is more ability to implement such as concepts depending on new technologies and information management systems.

2.3 Health Interoperability aspects

Interoperability between health care systems usually goes through three layers: foundational, structural, and semantic [17]. Usually structural layer covers syntactic interoperability also.

2.3.1 Foundational Interoperability

Foundational or basic technical layer concerns always about the common technical infrastructure which is required to allow information exchange between systems without need of additional interpretational data, so it makes sure that systems have the valid mutual technical ground and same connection methods. This layer usually are provided by hardware manufacturer and software providers.

Good example of lack of foundational interoperability is old radiology centers, where x-ray images printing is still analogue and using physical films. In case the center wanted to send patient's images

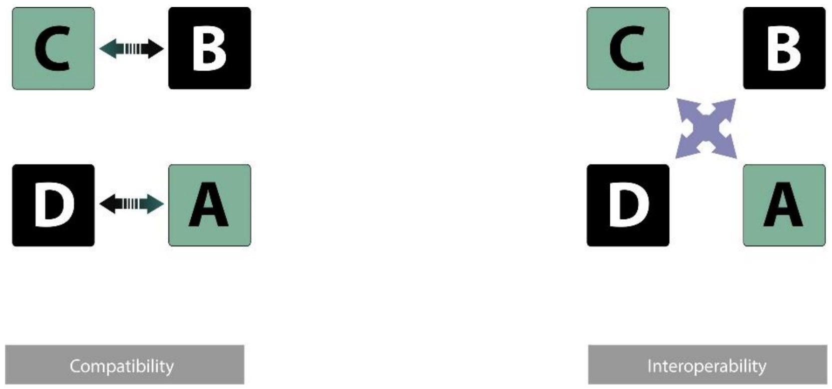


Figure 2 Compatibility focuses on small number of entities, in contrast inoperability provides communications between all entities. Health information systems nowadays are seeking the transition from compatibility to interoperability.

to specialist online, then there is a need to use computer scanner to scan the image manually, then send it via PACS systems or via Email, therefor the integration of digital printing system is the condition to fulfill foundational interoperability in this case.

2.3.2 Structural & Syntactic Interoperability

The middle layer in the pyramid, usually focuses on two main points: to provide a common data format for messages exchange and common syntax all parts of the structure, then systems can use same content structure for writing and reading, that's why this layer sometimes referred to structural interoperability while at other times refer to syntactic interoperability.

This layer permits uniform data-type formats for health information, organizing and arranging how the information's parts and properties will be represented and linked to each other in form of packets or files. Without this layer the information itself could be transferred between different systems but couldn't be parsed correctly, which could results in wrong or lack of interpretations.

Each type of clinical data is represented in this layer in specific way, so this first step usually in structural interoperability is to classify clinical data into groups, and then each group can has its own representation. For example various health care diagnostic systems such as CT, MRI and X-ray are using different "modalities" using DICOM, which corresponds to structural and syntactic layers in term of interoperability.

Many standards are introduced in this layer of interoperability like CDA, DICOM and HL7 version. Chapter 4.2 discuss more these standards.

2.3.3 Semantic interoperability

Semantic layer placed at the top to provide the transmission of the meaning alongside with data, and this is usually accomplished using metadata, which provides a predefined meaning for transmitted data, allowing all parts to have the same meaning, preventing ambiguity and misunderstanding.

In order to provide unified terminology sources for all clinical and health related vocabularies, many projects were introduced such as:

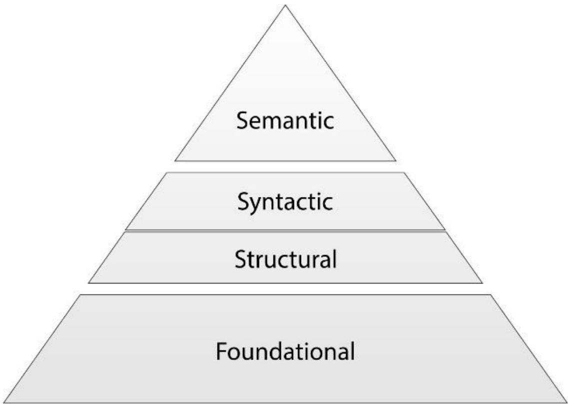


Figure 3 Interoperability pyramid layers: foundational layer at the base assure the basics for mutual technical ground, structural & syntactic layer at the middle provide the same content structure and syntax and semantic layer at the tope to assure correct understanding of the meanings

- **UMLS**: Unified Medical Language System, links vocabularies and terms to structure, allows effective and interoperable health information systems and health services, and facilitating health records systems [18].
- **MeSH**: The National Library of Medicine's controlled vocabulary, containing groups of descriptors integrated in hierarchical structure, allowing searching at different levels [19].
- **RxNorm**: Mainly used for clinical drugs, it also links names of many drug vocabularies commonly used, which is very beneficial in pharmacy and drug management software.
- **SNOMED CT**: A terminology resource, which can crosslink classifications and terms between different systems.
- **LOINC**: Logical Observation Identifiers Names and Codes, which is a resource to identify health measurements, observations, and documents.

Most of these projects offer direct access to terminology servers using web services, which considers a main feature for the integration with health information system and achieving interoperability on structural level and feeding the systems with continuous reliable updated data. Web services can also be a key factor to link various these projects to each other, to overcome obstacles of using multiple resources of semantic interoperability by mapping these resources together [20]. Figure 4 shows how terminologies and values of blood pressure monitoring device can be linked together to provide semantic interoperability.

Lack of semantic interoperability cloud result in many obstacles such as [21]:

Ambiguity: occurs when term representation could have many different interpretations. For example ‘country of origin,’ code is could have different meanings, so it could refers to the country where patient has raised, or the country where the patient currently residence.

Lack of expressivity: some parts of medical assessment and discretional narrative, could be so complicated or redundant to be included in code for universal scale, good example of this obstacle is the medical answer in medical report of falls assessments in USA, in case the is no injury detected, the assessment code will be *‘no evidence of any injury is noted on physical assessment by the nurse or primary care clinician; no complaints of pain or injury by the resident; no change in the resident’s behavior is noted after the fall.'* [22]

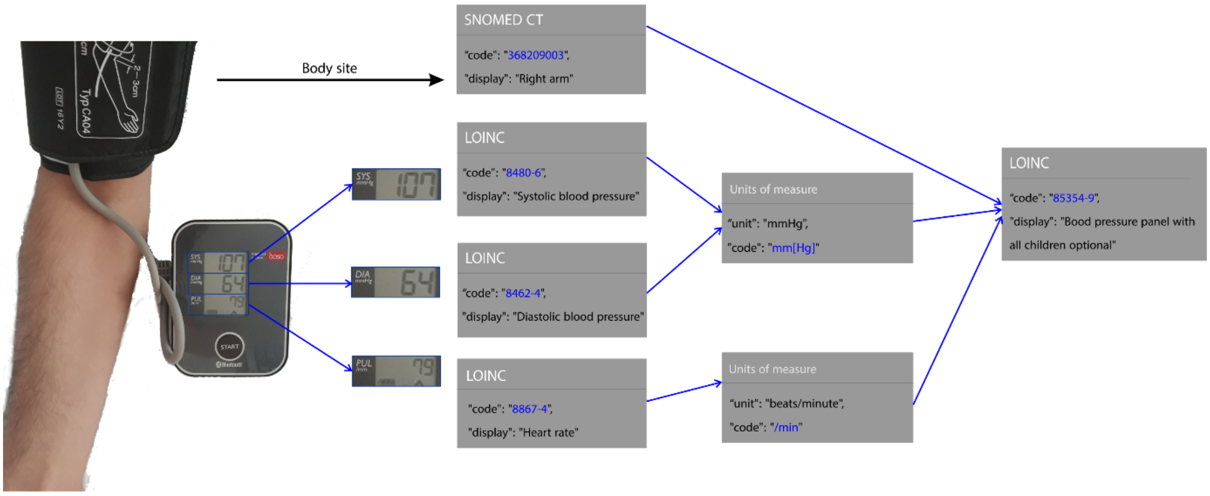


Figure 4 Semantic interoperability of blood pressure and heart rate measurements, using SNOMED CT and LOINC. Site of acquisition is determined according to SNOMED CT at the right arm, while vital value and category of the measurements provided according to LONIC, these values can be integrated later with structural level of health interoperability to offer full interoperability implementation.

Multiple representations: when certain value stored twice or more in the system without any additional meaning. This usually occurs because of data duplication or overlapping in the information hieratical structure.

Implicit semantics: some expressions and statements could be clear if the reader has suitable background, but for others or for computers it needs to be clarified and this solved usually by building relations between information each other's, since each info individually may has different interpretations.

Incomplete context: when the information like: clinical observation missed a part, this could lead to wrong interpretation. For example the observation of patient could contain "high blood pressure, his father has no clear symptoms", in this sense the blood pressure could interpreted as patient father blood pressure not the patient himself.

2.4 Implementation approach

In order to address interoperability different layers in the implementation, a programming "interface" was designed. The design was based on data model which deals with medical/health data as layers starting from the core information and then add additional layers as shown in Figure 5.

The layers of the design are:

1. **Basic information**: which is the main part of the design is located firstly in the core, this information could be any kind of medical information such as patient info, clinical observations, radiology images or even continuous signal information such as ECG.
2. **Narrative**: this could be any kind of comments for narrative proposes, such as patient medical related story or even redundant description.
3. **Meta-data**: this is the data which provide additional information without being part of the information it self, such as date-time, location or any other related data which is important but can't be classified as a part of the medical/health information. In this layer semantic interoperability resources are linked.

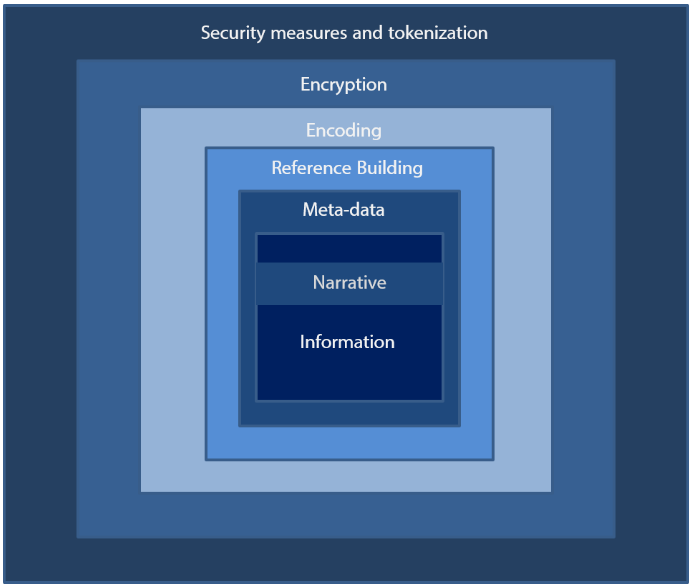


Figure 5 Proposed data representation and transmission model design. Basic information at the core followed by other complementary layers, some layer designed for security and privacy protection.

4. **References building**: at this layer any other entities, which has participated in the forming of the core information or have relationship with it are linked here. For example: patient medical observation is stored as the core part while the doctor who made this observation is another entity who is linked at this layer.
5. **Encoding**: after the whole mandatory and optional information is accumulated, the whole set of information is encoded in specific way to provide structural interoperability.
6. **Encryption**: this layer provide the protection against eavesdropping and tampering, to provide both security and privacy.
7. **Other measures**: other measures such as tokenization is placed here to provide further functions and integration in the system.

The information will be exchanged via interfaces, which are extensions that convert not interoperable information to interoperable information, in this way we have the ability to achieve interoperability for the whole system.

2.4.1 Interoperability interface layers design

Each interface consists of layers for implementation, each layer is responsible for some processes. Layers are show in Figure 6.

Object generator: is the layer which pulls and pushes information in the form of certain objects which are in understandable form for the system below, such a systems could be databases management systems or health information systems or others, thus this layer is customized according to the system which will connect to.

Interoperability layers: this layers are responsible for providing all necessary steps to convert the information from the bottom layer to be interoperable information, this includes all aspects of structural, syntactic and semantic required processes, furthermore in this step metadata integration occurs and references between information are created and linked, the output of this layer is an

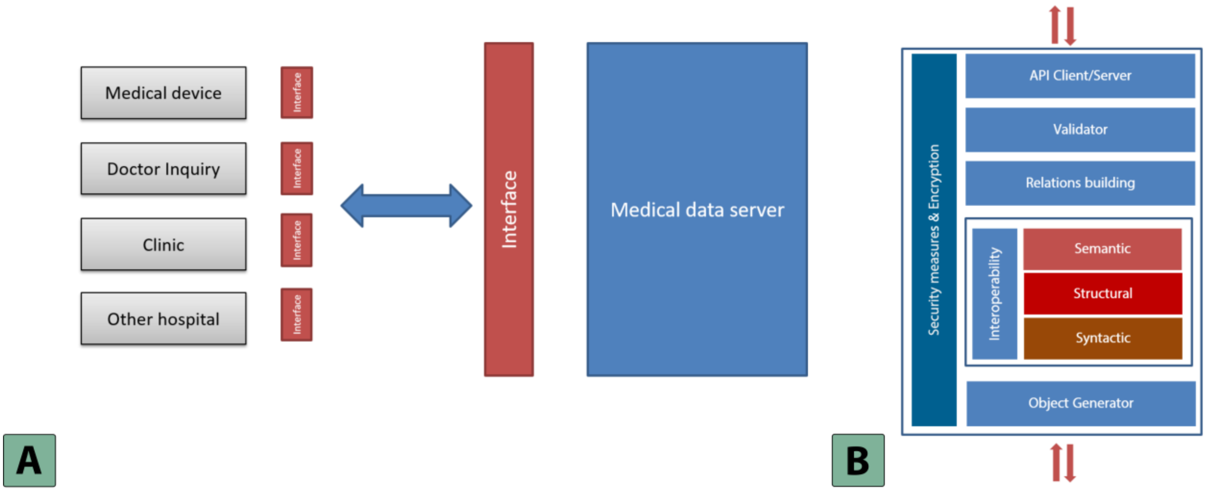


Figure 6 shows A) communication interfaces of different systems, provide the ability of interoperability, B) communication interface layers, where information are transferred from non-interoperable systems below to other inoperable systems on the top

interoperable converted data. This layer contains structural/syntactic interoperability programmed solutions such as HL7 and DICOM, and integrated semantic resources such SNOMED CT and LOINC.

Validation layer: which performs validation of the information in both directions, to prevent any not valid information to pass from/to outside the system, this not valid information will not be understood or will have wrong interpretation, so this layer acts as protection layer.

Application programming interface (API) layer: here where the pull and push processes are executed, so it provide a way to make connection to external parts in order to perform various tasks and queries.

3. Health monitor device – Mobile device data transfer

3.1 Introduction

The vital data which is acquired from health monitoring devices, is transferred to terminal devices such as mobile, tablet. This chapter is focusing on searching for best wireless communication technologies for health monitoring devices and provides programming solution to achieve health interoperability. Figure 7-A shows the first step in the project.

The practical implementation covers transmission of blood pressure information from blood pressure monitoring device to smartphone using Bluetooth Low Energy. The selected device uses BLE standards in connections, so our developed application will decode connections and parse standards to conclude patients' vital values to make it ready for later processes.

Other aspects also will be discussed to show features and limitations of wireless health data transmission using current available tools.

3.2 Choose wireless protocols for health/medical data transmission

The rapid growing nowadays of internet of things devices including personal health device, allows competing for new evolved protocols for wireless communication technologies, but although there are a large number of wireless protocols and standards competing for a position in the new expanding production market, showing different features in terms of bandwidth, power consumption, and working range, there are few wireless standards compete for a share in terms of healthcare applications.

In this study we provide comparison for health care usage aspects for Bluetooth low energy and Wi-Fi especially "IEEE 802.15.4" version which consider the main competitor to BLE [23].

3.2.1 Hub concept / Wireless body area network (WBAN)

Bluetooth Low energy and Wi-Fi "IEEE 802.15.4" are presented originally to boost the Internet of things, from this perspective the normal concept of Master/Slave is changed, and a new "Hub" concept is raised. Hub Concept permits using different connections together to send/receive data, this approach could be very supportive for medical applications and personal health monitoring where many sensors are used simultaneously to evaluate the user's physical health.

Bluetooth low energy also supports Medical Body Area network, referred to as a wireless body area network (WBAN) or body sensor network (BSN) [24].Wi-Fi "IEEE 802.15.4" also is able to perform the same concept [25].BSN may be embedded inside the body [26], as implants or could be as wearable sensors, this could prompt the minimizing of monitoring devices since the device could only contain radio frequency antenna, ICs, and bio-signal sensor. Figure 7-*B* displays schema of system built based on the hub concept where all devices can be the communication hub.

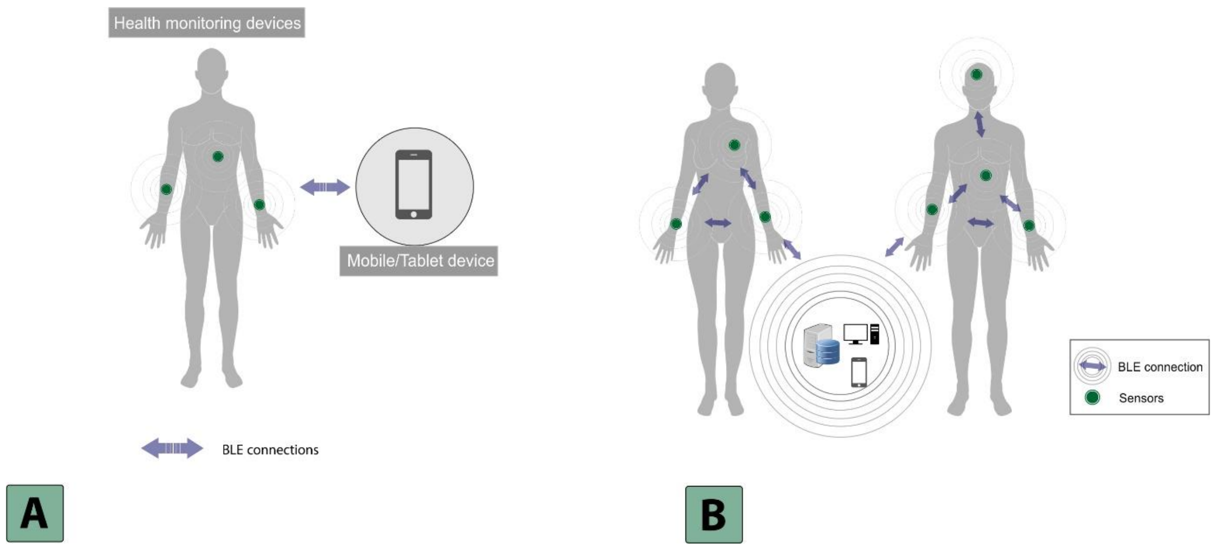


Figure 7 A) Transfer data from health monitor device to smartphone using Bluetooth Low Energy, b) BLE hub concept for medical purposes, where sensors wireless tranmissters form network of connections

3.2.2 Power efficiency

Reduction in the size of medical devices is a necessity in order to provide more comfortable monitoring/therapeutic processes for users/patients and to guarantee less pain of implantable devices. In contrast, minimal size in its turn resulted in small batteries, leading to power problems such as batteries failure or shortcoming [27].

Based on this situation, low power consumption for the whole system is highly critical, especially in case of implantable systems. BLE provides quite high power consumption efficiency in comparison to other well-known techniques [28].

BLE uses what is called “low peak" power consumption as it functions based on a shutdown technique, where the signaling system is always down and wakes up just when it sends/receives signal. It has a 3 milliseconds wake-up delay time. Peak power consumption reaches a maximum of 15 mA [29], preventing the power caused system failure and decreasing system power threshold. In principle, BLE could work for months or years on small coin-size battery [27].

Comparing to the IEEE 802.15.4 in terms energy consumption per data transmission, BLE shows almost 30% more energy efficiency to perform data transmission [30], and even at smartphones side, around 13% more consumption has shown in devices operated using IEEE 802.15.4 for data transmission rather than BLE [30].

3.2.3 Compatibility and interoperability

BLE is supported in all modern operating systems and usually provides backward compatibility for older versions [31], on the other hand although Wi-Fi has a/b/c/n/ac versions which are supported in most devices, but those are not the versions which used in low rate health monitoring devices [32], usually IEEE 802.4.15 version is the version which has designed for this purpose and it is not supported in major operating systems such as IOS [33].

Furthermore BLE manufactures designed profiles to support interoperability for health care purposes, which we will discuss more in chapter 3.3.3.1.

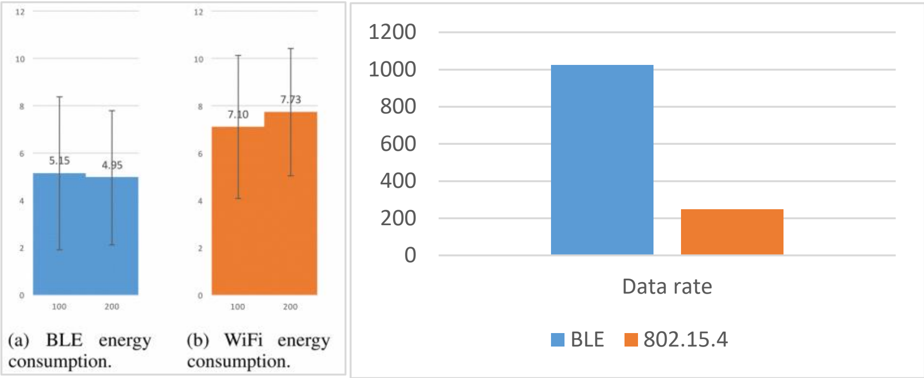


Figure 8 Left) Energy consumption measurement result with 100 and 200 of beacons data for both BLE (a) and Wi-Fi (b) [30], Right) BLE vs. IEEE 802.15.4 data rate Kbit/s [34], both charts shows the superiority of Bluetooth low energy.

3.2.4 Data transmission speed and latency

Data rate which is a count of bits transferred per second. For BLE the maximum is about 1 Mbit/s while it could reach 11 Mbits/s in Wi-Fi for lowest power 802.11b mode but about 250Kbit/s for 802.15.4 [34].

In terms of latency which is the time between a signal being transmitted and received and it is dependent on configuration and operating conditions. For Bluetooth low energy the maximum is about 2.5ms while it is 1.5ms for 802.11b and 20ms second for 802.15.4 [34].

3.2.5 Other aspects

Bluetooth Low Energy (BLE) provide lower manufacturing costs [35] while on the other hand, its ubiquity provides a feature for healthcare developers to achieve interoperability easily between the systems.

3.2.6 Conclusion

From this comparison it's clear that Wi-Fi 802.15.4 and BLE can both used to build Wireless body area network WBAN, but BLE can provide higher data rate and less latency, in addition to better power consumption and more ubiquity which allow better compatibility.

In regards to other Wi-Fi versions, they are not used in health monitoring devices, since typically large data rate is not required in personal health device, because data of sensors output in scale of bytes per second. Furthermore low latency is not important for health monitoring devices which sends and receive data perhaps twice per second.

So the most mature and ubiquitous standard that seems robust and highly reliable for wide medical/healthcare application is Bluetooth Low Energy.

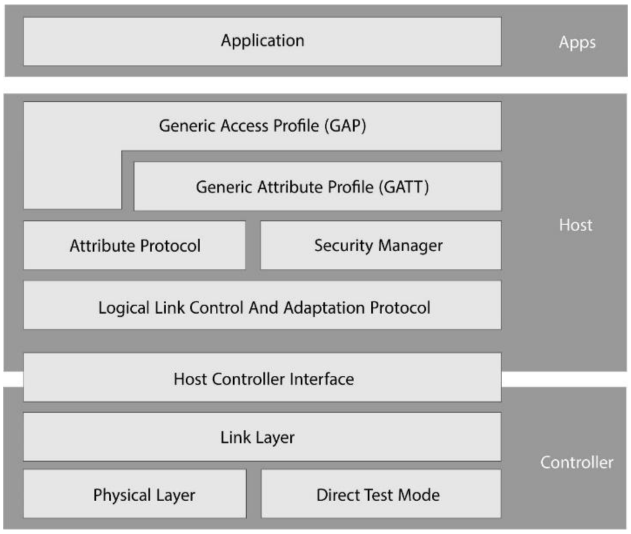


Figure 9 Bluetooth Low Energy architecture showing physical and virtual layers, image adapted from [35], smartphone application development deals usually with tope three layers: Apps, GAP and GATT.

3.3 Bluetooth low energy for health data

Bluetooth Low Energy is one of Bluetooth versions which had introduced to support novel application such as health care applications, fitness and security. It uses the same 2400 MHz [29] frequency of the previous Bluetooth version which allow devices to have single Bluetooth chip/Antenna to support both versions. It has structure of physical and virtual layers, certain layers are designed to certain services, and thus we can take the advantages of these services in health information transmission.

3.3.1 Bluetooth Low energy Architecture

The architecture of BLE consist of Apps, host and controller layers. The Host layers are:

- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Attribute Protocol (ATT)
- Security Manager (SM)
- Logical Link Control and Adaptation Protocol (L2CAP)
- Host Controller Interface (HCI)

The Controller layers are:

- Host Controller Interface (HCI), Controller
- Link Layer (LL)
- Physical Layer (PHY)

BLE architecture is show in Figure 9.

In this thesis, Generic Attribute Profile (GATT), Generic Access Profile (GAP) and application layers are discussed since they are the layers which have relation to medical data transmission and structure, other layers are concerned with other issue outside our interest.

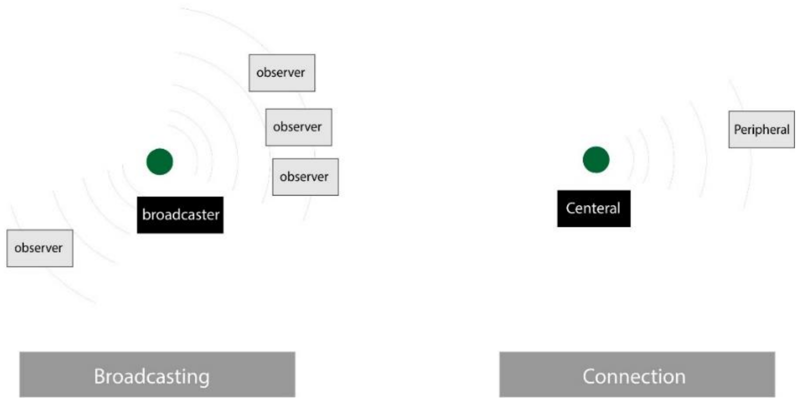


Figure 10 Connection types based on GAP configuration. Left) Broadcasting: where there is or broadcaster and one or more observer. Right) Connection: one central and one peripheral [36]. The case on right is usually used in health care where device has Peripheral role to send data to the device has Central role which could be Computer, Smartphone or other.

3.3.2 Generic Access Profile (GAP)

Defines the general topology of the BLE, displays information about device and manufacturing. General access profiles determine the availability of BLE device and more determine how two devices will communicate between each other.

GAP determine one of two connection modes, which are seen in Figure 10:

- **Broadcasting**: in this case there are two parts, the broadcaster device who send data and observers which are the device that can listen to the data an collect them, in this case there is no need for direction connection between observer and the broadcaster.

- **Connection**: where two parts are directly connecting to each other, in this case there are peripheral and central devices, once the connection established peripheral device listens to the central and responds, while the central sends the data and other configurations.

In terms of health monitoring devices communication, the common scenario which occurs, that the device plays the role of Peripheral device who sends data to the Central smartphone or PC, and the peripheral responds with certain respond which could contain important configuration messages such as confirmation that the messages has been delivered or the log has been updated.

3.3.3 Generic Attribute Profile (GATT)

Generic attribute profiles determine the final shape and values of BLE message, so at least one GATT is mandatory for any BLE application, in contrast to GAP there is just one connection mode contains client and server only. Clients can read and write or make requests, while server assigns values to profile attributes and then sends information to the client. Structure of GATT is depicted in Figure 11.

GATT layer usually contains one or more services, which are arranged in the following hierarchy:

Figure 11 BLE GATT structure. Each profile contains characteristics which is used to store information, different profiles could have links to each other, this is can be used to transmit healthcare data as predefined segments called "BLE healthcare and fitness profiles"

- **Profile**: define group of information sets for certain purpose.
- **Service**: set of information has set of values and predefined identifier to describe certain event. Services could be primary or secondary depends in their function whether it's fundamental or not.
- **Characteristic**: in which the values are stored. Each characteristic has single value and optional description about the value. Additionally it has a property which describes which operations are allowed to apply for this value, this property will be READ when the counter part is allowed to read this value, WRITE when it is allowed to modify this value and INDICATE to indicate that the value has changed.

UUID or Universally Unique Identifier is the way to define a common names for services and characteristics, to prevent overlapping and conflict between Identifiers, it's usually 16 bit long for standard and 128 bit for UUID which is defined by manufactured or system designers. For example to send the age of the patient, UUID value is '0x2A80', the whole list of predefined UUIDs for health care purposes are mentioned in (Appendix 7.2 GATT health related services and characteristics UUID)

This hierarchy provides very good ground to encode health data, since it corresponds to the concept of interoperability in terms of focusing on the clustering of the medical information in specific clusters, where each cluster represents specific event, accordingly we can consider GATT profiles as proper representation of data model which has described in previous chapter. GATT represents health data of the patient in form of services, and get befit from characteristics to store values and linking which occurs between profiles, while other processes such as encoding and encryption occurs in consequent layers of BLE architecture.

For example: ECG data could be transmitted where ECG device could play 'Central' role and PC or smart phone play 'Peripheral' role. Data are encoded as a matrix of peaks and valleys which is stored in one service and has the proper UUID, and we can use additional characteristics using WRITE property from the peripheral to the central to tell if the ECG data is transmitted correctly to remove old data from ECG device.

3.3.3.1 Bluetooth low energy healthcare and fitness profiles

Bluetooth Low Energy provide different profiles for healthcare applications such as

- BLP (Blood Pressure Profile) — for blood pressure measurement.
- HTP (Health Thermometer Profile) — for medical temperature measurement devices.
- GLP (Glucose Profile) — for blood glucose monitors.
- CGMP (Continuous Glucose Monitor Profile)

A full list of BLE Health care profiles and related services profiles are show in (Appendix 7.1 Health care BLE profiles).

3.4 Implementation approach

This part of the project works on receiving health monitoring device output, decode it to find GAP and GAT profiles including health care profiles. If we successes to design and implement such a component in the project, then we can proof that this connection between health monitoring device and smartphone is following interoperable standards.

To do this we built Android App, which can receive BLE connection, decode it and parse it to conclude desired data, after that this data will be ready for next step in the project.

3.4.1 Health Monitoring Device

In order to implement this part of the project, health monitoring device has chosen, which is "**BosoMedicus System** Wireless upper arm blood pressure monitor", this device is designed to provide standard blood pressure profile along with other profiles through wireless connection of Bluetooth Low Energy. Technical specifications of selected device are show in (Appendix 7.3 Health monitoring device technical specification).

3.4.2 GAP layer & GATT Layer

To detect GAP layer values, UUIDs should be known first in order to parse the profile and conclude the values, Figure 12 shows founded output of GATT and GAP profile services.

Using our application to decode BLE message, we were able to receive and parse all profiles/services values and UUIDs, property of services also has been parsed (R: READ, W: WRITE, I: INDICATE), the full list of Services are shown in (Appendix 7.4 Blood pressure device parsed output)

From this output, we can notice that Blood Pressure Profile BLP is a part of the message and vital values are included here, also the mandatory GAP profile are shown containing many values like "Device name" which is defined by the manufactured, and "Reconnection Address" which contain the address of the next communication to protect connection privacy. Other profiles are shown such as "Battery Service" which display battery level and "Generic Attribute" which contain basic information about hardware and software and firmware versions.

Undefined service also detected, these kind of services usually is predefined privately by the manufactures for customized usage to provide some complementary functions.

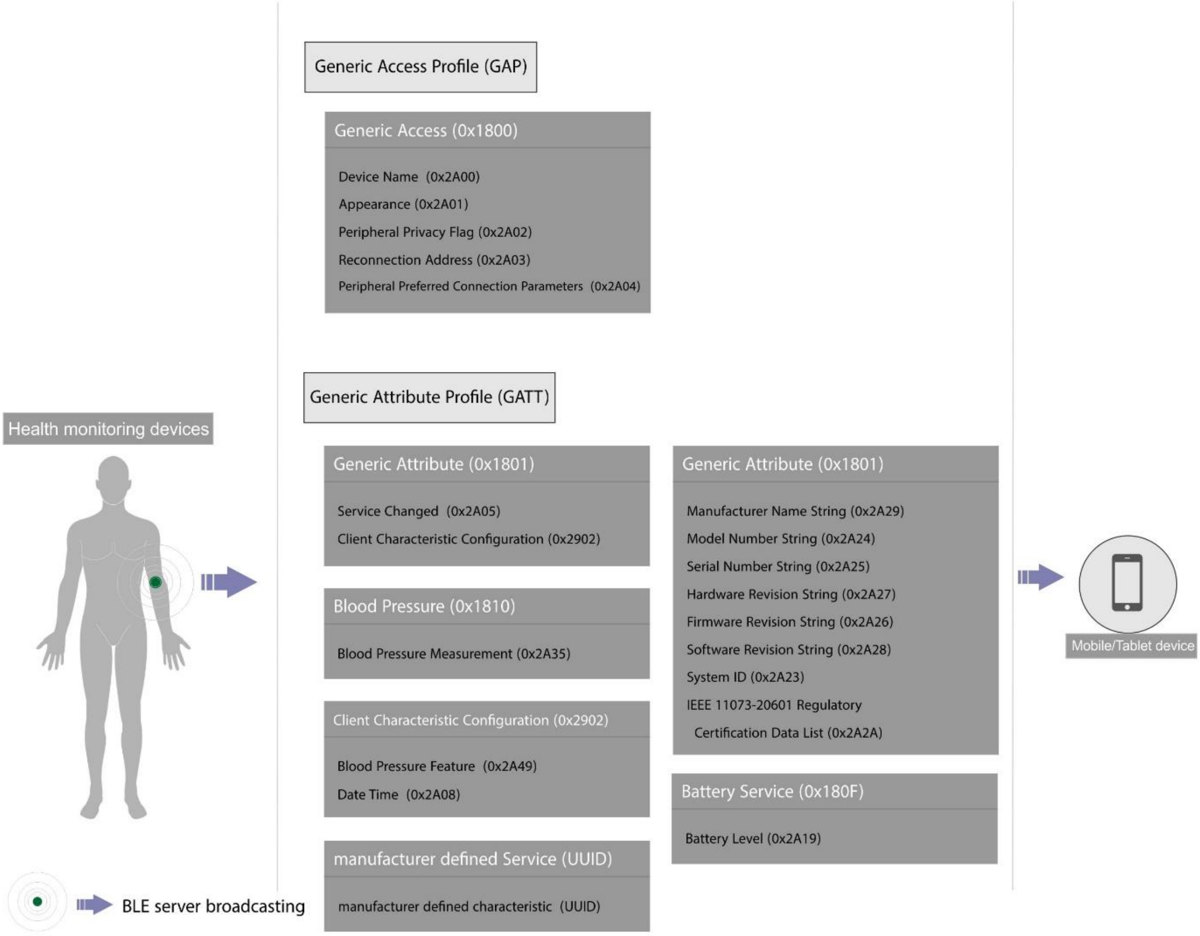


Figure 12 GAP and GATT BLE profiles and services in "Boso Medicus" blood pressure device output to the smartphone. Blood pressure measurements are shown in Blood pressure profile (0x1810), while other profiles transfer other kinds of data such as battery level, times of measurements and device manufacturing information

To extract Systolic pressure, Diastolic pressure and Pulse rate from Blood Pressure Profile BLP, further analysis is applied to parse this value. Figure 13 shows how BLP is parsed and converted to absolute values.

The value of BLP is a string of HEX characters, which consists of many segments, each segment corresponds to certain value and meaning [37].

I. The first octet defines which data fields are present in the Characteristic values.
II. The next three octets define systolic, diastolic and mean pressure.
III. Next 7 octets for timestamp, which contains data and time.
IV. Pulse rate is encoded in the next two octets
V. Last octet is booked for user id, but this value could be empty, which is founded in our case.

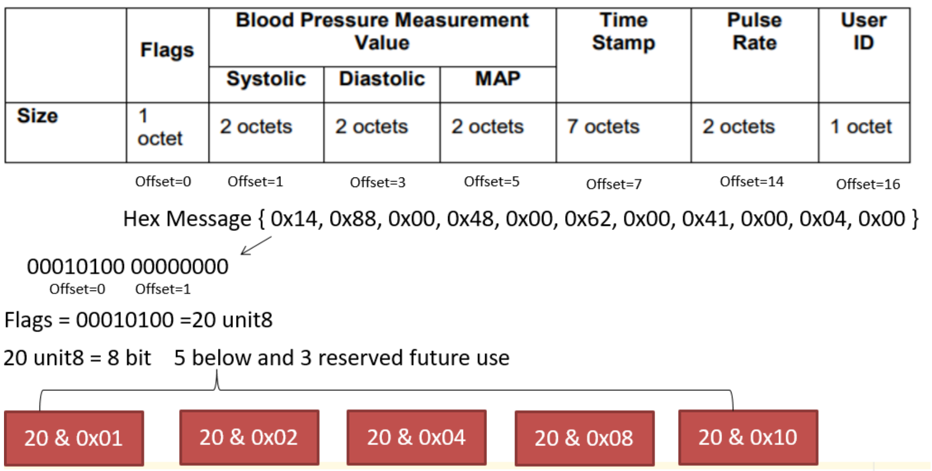


Figure 13 Blood pressure profile (BLP) consists of segments, each segment has its own interpretation. From left: Flags used to determine the unit of the measurements (Kpa or mmHG) and to determine which of next segments has values or empty, Blood Pressure Measurement Value is used to pass the value of Systolic, Diastolic and mean arterial pressure, Time Stamp used to pass time of the measurements, Pulse Rate used to pass heart rate and User ID can be used to assign ID for specific user or can be empty. This segments has redundant sequences can be used for future updates, this helps to provide backward compatibility of BLP.

3.4.3 Application layer

Application layer contains smartphone application which receives data from health monitoring device, parse it and display it via proper user interface. In this study we will not go into user interface design details and techniques, since it out of study interests. The next chapter discuss sending this data after processing to the main aggregation server.

The application designed for Android 4.3 (API level 18) operating system and higher to assure BLE support, and developed using native Java language and Google Android Java SDK. Usually applications are passing across different layers to use smartphone physical and virtual resources in order to complete certain task such as using camera to capture a photo, Figure 14 shows Android Apps architecture. In our case the aim was to use BLE adapter to establish connection to health monitoring device and then exchange data, thus the application was using Linux kernel layer to communicate with Bluetooth service, display, shared memory and other resources which used normally during operation, then using Hardware Abstraction Layer (HAL) which acts as an interface allows software codes to call hardware components such as Bluetooth and other related hardware components without a detailed understanding of how the hardware works. After that the application uses native libraries and runtime which form the basic layer from which known Android API Java classes begin to work.

The sequence of the data flow in the application is as the following:

- The whole process starts when health monitor device starts to send its signal after the pressure measurement is finished.
- Smartphone starts to scan for nearby devices showing all available devices, usually this happens using native Android “BluetoothLeScanner” Classes that provides the capacity to operate Bluetooth adapter and perform scan for BLE devices.
- User chooses health monitoring device to connect.

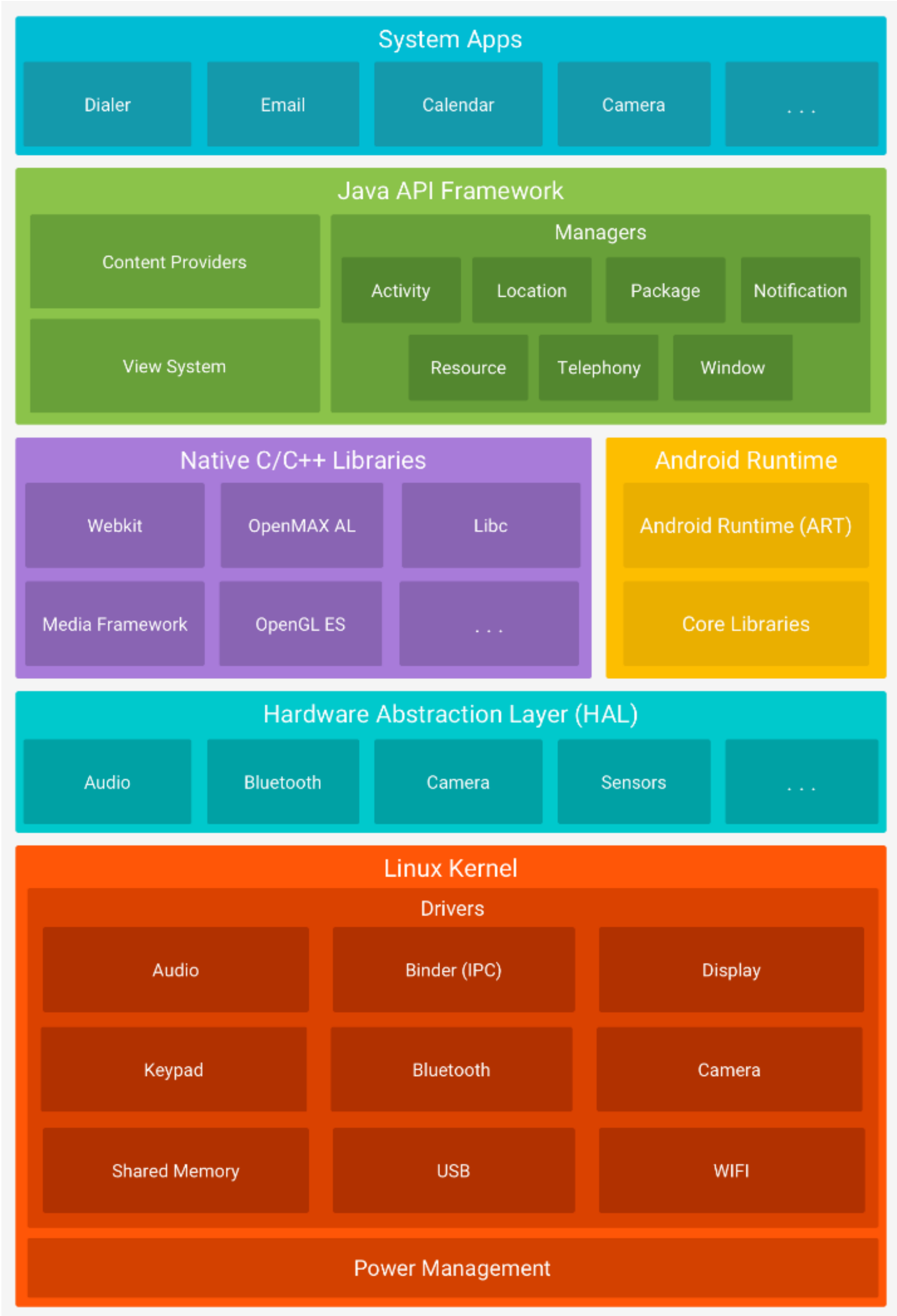
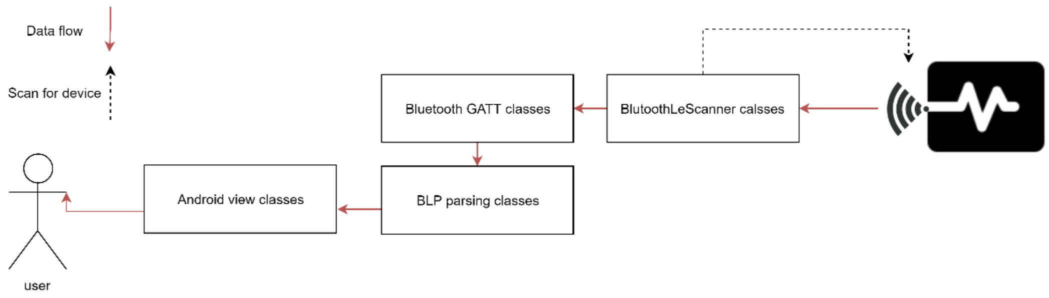


Figure 14 The Android software stack[1], shows basic OS layers, API layers and software development layer. Any application should cross different layers in order use smartphone hardware resources.

- When device is chosen by “BluetoothLeScanner” Classes in smartphone, other classes are operated to exchange data. In this step we developed new classes called GAP and GATT classes, which use predefined UUIDs lists to detect all GAP and GATT profiles and services and then extract their content. Each profile has its own structure, so we had to search for proper parsing method to provide understandable values to be assigned and grouped in data models.

[1] https://developer.android.com/guide/platform/index.html




```java
public class BPMManager extends BleManager<BPMManagerCallbacks> {
    String TAG = "Ss";
    /**
     * Blood Pressure service UUID
     */
    public final static UUID BP_SERVICE_UUID = UUID.fromString("00001810-0000-1000-8000-00805f9b34fb");
    /**
     * Blood Pressure Measurement characteristic UUID
     */
    private static final UUID BPM_CHARACTERISTIC_UUID = UUID.fromString("00002A35-0000-1000-8000-00805f9b34fb");
    /**
     * Intermediate Cuff Pressure characteristic UUID
     */
    private static final UUID ICP_CHARACTERISTIC_UUID = UUID.fromString("00002A36-0000-1000-8000-00805f9b34fb");

    private BluetoothGattCharacteristic mBPMCharacteristic, mICPCharacteristic;
    private Handler mHandler;
    private BluetoothLeClass mBLE;
```

Figure 15 Top) Information flow from health monitoring device to user interface throw smartphone application, shows GATT and BLP programming classes which have been developed to extract values from GATT and BLP profiles, Bottom) Systolic, Diastolic and mean blood pressure parsing using Java during Android App development, code shows how UUIDs are used to determine BLP profile and other service

- Blood pressure profile BLP is the main profile which is one GATT profiles, since Android native libraries don't provide specific way to extract content and parse it so we had to develop our own classes which we called "BPManager" classes. Parsing process firstly starts to convert binary data into hex data, after that splits hex string into segments, then analyze the segments: **Flags** segment contains 1 octet or 8 bits, five of those are used to determine the unit of the measurements (Kpa or mmHG) and to determine if next segments doesn't have values. **Blood Pressure Measurement Value** is used to pass the value of Systolic, Diastolic and mean arterial pressure, it has 6 octets: three of them provide pressure measurements in mmHG and others in Kpa. Flags determine which ones are activated. **Time Stamp** used to pass the time when measurements have taken place, Flags determine if this field activated. **Pulse Rate** used to pass heart rate and **User ID** can be used to assign ID for specific user or can be empty, both them are activated also using Flags. Furthermore The Blood Pressure Feature characteristic which is seen in Figure 12 is used to provide further information about movement artefacts of device cuff or to notify about irregular pulse. Figure 13 Bottom shows part of parsing processes using Android Java code.
- User interface is initiated using Android view classes and XML files.
- Data acquired from health monitoring device is now available to be displayed for user.

Figure 15 Top depicts this sequence, while Figure 28, Figure 27 and Figure 26 show UI design of the application.

3.5 Other concerns

3.5.1 Security measures in BLE for healthcare data

Ensuring the security, protection, and stability of healthcare data transmission is one of the most critical issues as regards to health/medical system design and implementation. Bluetooth core specification provides various features covering data encryption, data integrity and the privacy of users' data.

3.5.1.1 Pairing

It's a mechanism where different parts which are interconnected, exchange identification information including encryption keys for further secure data exchange. Different types of key pairing could be used, based on the aim of connection [38].This could be used in health devices to offer "plug and play" feature after first pairing.

3.5.1.2 Encryption

Using AES (Advanced Encryption Standard [39]) with CCM [29] to provide "authenticate-then-encrypt" technique allows high encryption connections. This encryption method is integrated into many microcontroller systems, enabling a high level of security for portable healthcare devices [40].

3.5.1.3 Signed Data

BLE supports sensing data without encryption after the authentication process with other "trusted devices". This means that there is a possibility to protect unencrypted data by accompanying it with Connection Signature Resolving Key (CSRK), which needs to be verified each time to check if the signed data is received with the correct key. This approach could be a valid way to transfer certain kinds of medical data such as fitness health data where there is no high importance for encryption.

3.5.2 User privacy

3.5.2.1 MITM

Man in the middle, a widespread way to intercept communication between two sides and inject or modify transferred data. This is shown in Figure 16-A. Many protection methods have been proposed by Bluetooth SIG Company [39] to eliminate this problem in BLE. In addition to this, there are different ways which provide further protection in telemedicine applications [41].

3.5.2.2 Passive sniffing

Passive sniffing could be executed via sniffing device, which is a technique for listening to private communication without approval secretly.

To avoid this problem, Elliptic curve Diffie–Hellman (ECDH) public key cryptography which is an anonymous agreement protocol allows two devices, each one has public–private key pair to create directly or in directly key to establish secure connection [42]. This approach provides a very strong way [38] for unencrypted connection, which could be the case in many healthcare devices such as wireless BLE blood pressure devices.

3.5.2.3 Identity tracking

A third-party device could track communicated device addresses since most BLE devices declare address. This can be protected if the privacy measures are activated to frequently change the addresses and allow just the trusted devices to be updated with new addresses. Even though a mitigation and countermeasures have been provided by the US National Institute of Standard and

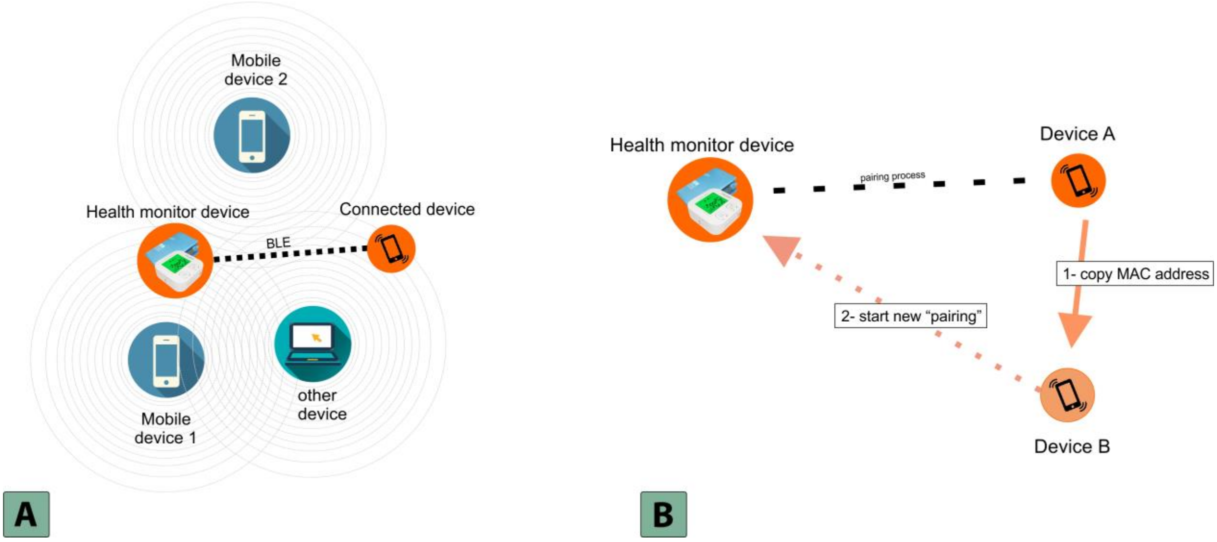


Figure 16 A) Health monitoring device location estimation using 2 smartphones and one PC located differently in the space which violate users' privacy, B) Establish new "pairing" process is the first step to intercept communication between already connected devices, this is used in Man in the middle attack.

technology at 8th May 2017 under the title of "Guide to Bluetooth Security" to enhance connection security and override Bluetooth concerns [43].

3.5.2.4 Proximity detection

Bluetooth low energy provides the ability to estimate devices even if not connected, since this could be feature in some application to improve user experience, but it considers as privacy violation because it allows to estimate the proximity or location even for devices which are not connected. Figure 16-B shows an example where rough location can be estimated using three devices located differently in the space.

3.5.3 Integration of non-medical data with medical data

This problem occurs when manufactures include undefined services in the BLE message, this results in ambiguity of the information and reduce interoperability chances. Although sometimes this could be used to pass non-medical data but it is recommended to use standard BLE UUIDs to avoid any possible data duplication or conflict, since even non-medical data has predefined UUIDs cover almost every aspect of data.

3.5.4 User data storage in smart devices

It is recommended to send any sensitive data including medical and health data directly to the server where security measures are better. Smartphone usually an open environment for applications, it is basically a personal device not health care device, so it could contain all kinds of applications which may have permission to access to data and modify it.

4. Mobile device – Aggregation server data transfer

4.1 Introduction

Health interoperability refers to the ability to exchange information and have the correct understanding without restrictions, in that sense it is the basic step to develop health information systems. Many concepts have introduced in this field to provide complete model which is able to deal with all aspects and issues, and many companies and organization trying to provide stable and efficient standards and protocols such as Health Level Seven International orginzation which created HL7 standards and National Electrical Manufacturers Association which producded DICOM standard.

Usually these standards play the basic role in structral and syntactic layers in introperability pyramid - please see Figure 3 , while semantic layers is integrated (for more description about sematic layer standards please see 2.3.3) to this layers.

This chapter tries to find the best current health care data standard and best technologies and structures to implment that.

4.2 Choose standard for health care data transmission

To find the appropriate standards to be used in this project, we browse the available standards and solutions in and then provide the result of the research.

4.2.1 HL7 versions

Hl7 standards are developed by Health Level Seven International organization, and they have been used dramatically in health information systems, they are group of standards which describe how transfer clinical and administrational data between different parts. Some HL7 versions are adopted by ISO and American National Standards Institute [44]. Hl7 provided HL7 v1, HL7 v2, HL7 v3 and HL7 FHIR which is the version that is now in development. Figure 17 shows HL7 versions [14].

HL7 standard packages information in form of entities and defines general messages structure and data types for sub units of the message, also it integrates with other standards such as semantic standards to provide full solutions. In general it provides complete framework of tools and concepts supporting software development in health care.

HL7 version 2.x is the most implemented standard in health care information system industry worldwide and 95% of healthcare organizations in US [8].

The structure of this version consists of segments combined together with delimiters, these segments have their own defined data type and the identification is possible using the sequence of the segments. Each segment have sub units which splitted by composite-delimiter, these structures are shown in Figure 19 A.

HL7 version 3.x provides new concept as it is bulit based on object based model rather that structre based model, it also uses refrence infromation model (RIM) which defines the define the life cycle of the infromation, define data types and has the ability to integrate other standards.

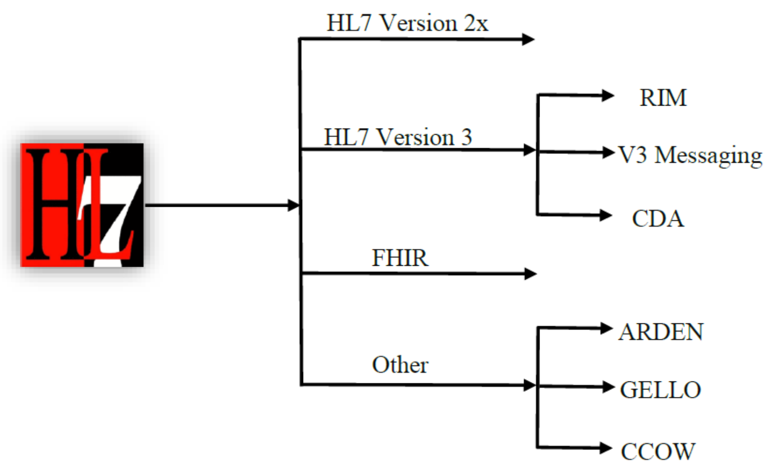


Figure 17 Overview of the various standards developed by HL7 [14], among them version 2x is the most ubiquitous one [8]. FHIR the most recent and still in development stages.

The HL7 version 3 RIM consists of four base classes and other sub classes:

- Entity: persons, organization, Hospitals etc.
- Role: patients, health professionals, doctors
- Participation: detailed description of the participation in certain event.
- Activity: Actions in the context of medical treatment, examinations, procedures etc.

HL7 version 3 has used XML format to represent information.

HL7 FHIR is the last version of HL7 standards, it is an acronym for Fast Healthcare Interoperability Resources, built based on modular design, in which each module called "resource", these resources define actual real information entity, this resource usually contains the properties of the entity, for example: patient could be a resource and the age of the patient is one of the properties which is included in FHIR resource representation. Also FHIR provides data type definition and furthermore it provides links between resources. It includes also the concept of RIM components as version 3.xx.
HL7 FHIR information message are usually represented in XML, JSON data format for output and input.

4.2.2 CDA

Clinical Document Architecture is a document markup standard which offer the structural and sematic capacity to exchange "clinical document" [45]. It represent data in XML format, with ability to include text, images and other multimedia content, also it could be integrated in HL7 FHIR resources. CDA is designed to transfer only clinical data, so it lacks of administrational and logistic data representation. Figure 19 B) shows an example of CDA document.

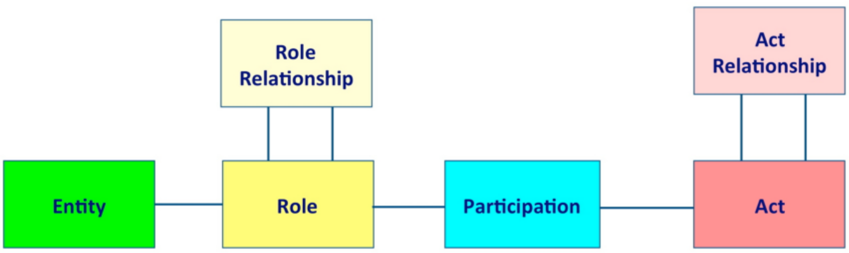


*Figure 18 HL7 v3 HL7 Reference Information Model (RIM) [46], shows the interaction between parts of the concept where **Entity** can represent organization or person such as doctor or hospital, **participation** describes the involvement of an entity in an act such as diagnostic exam performer , **Role** and **Role Relationship** define who can play certain roles to apply actions in the system, **Act and Act Relationship** determine the type of the action that entities can play such as diagnostic report.*

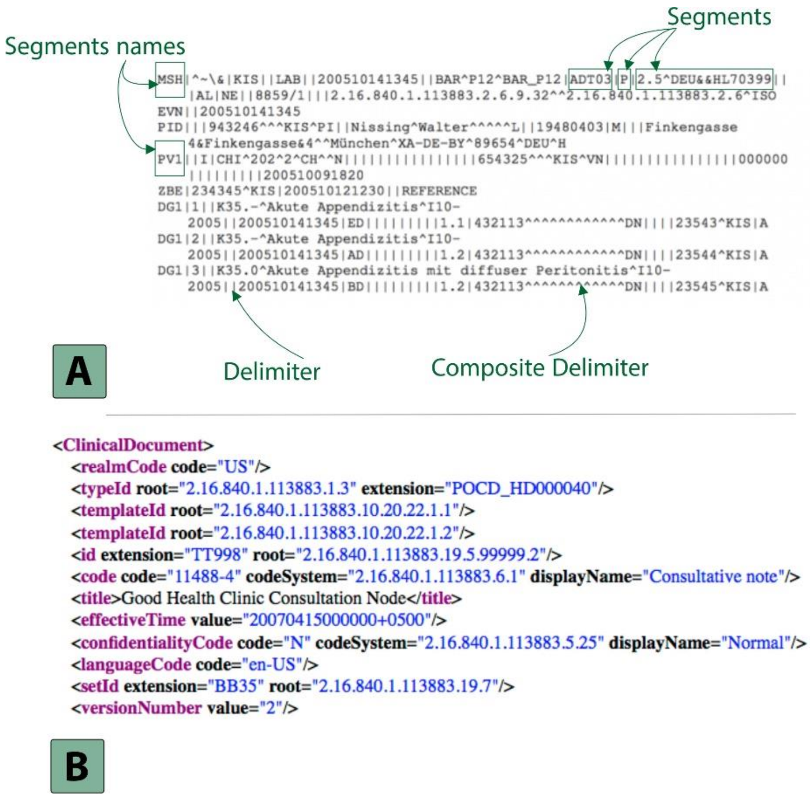


Figure 19 A) Description of HL7 version 2.xx structure. Segments are separated by delimiter and composite delimiter used to form sub segments which contains the values, B) Standard schema for Clinical Document Architecture template contains all mandatory header attributes [2]

4.2.3 Other standards

4.2.3.1 DICOM

Digital Imaging and Communications in Medicine which is a standard to store and transfer medical images, it is widely used to allow access to medical imaging information in radiology centers and hospitals. Although DICOM is very strong to transfer imaging data, but it couldn’t be consider as full framework to transfer all types of health care data.

4.2.3.2 Other national standards

USA: ASTM (American Society for Testing and Materials) has developed standards to exchange of information between clinical instruments and computer systems.

Germany: xDT is a group of formats developed by National Association of Statutory Health Insurance Physicians in Germany to be used in health care administration [47].

United Kingdom: The Interoperability Toolkit (ITK), a group of implementation guidelines developed by United Kingdom’s National Health Service (NHS) to support local interoperability between health care providers, it could be integrated with HL7 and 'Integrating the Healthcare Enterprise' (IHE) [48].

Japan: Japanese Ministry of Health has introduced SS-MIX (Standard Structured Medical Information exchange) for health care data exchange, it could also export HL7 and DICOM formats [49].

[2] http://help.interfaceware.com/v6/generate-a-cda-document

4.2.4 Conclusion

- HL7 version 2.x is very widely used but still uses very primitive methods to represent data comparing to other solutions and there is no clear structure to simulate health care scenarios.
- Hl7 version 3.x is better in comparison to version 2.x in terms of data type and modeling but it lacks of ability to link different data entities together in efficient way, so it could be weak to classify health care data into groups.
- CDA, although it provide similar XML structure of HL7 FHIR but it is limited to clinical data, it can't be considered a comprehensive standard which can simulate full health care scenarios and can't be used to extend health data with other kinds of data, which is necessary in our project to link our data to other big data resources. For further comparison between CDA and HL7 FHIR, you can read my colleague work [14].
- DICOM is a standard to transfer medical imaging data rather than being a comprehensive framework.
- All other national implementation are designed for local issues, they couldn't introduce solutions for interoperability on global scale, additionally many of them using Hl7 version as interoperability standard.
- HL7 FHIR can provide clear data type definition and has the capacity to make links between resources. It has distinct definition to health care scenarios.

Based on comparison, it has been clear that HL7 FHIR fulfills our project requirements and provide better features for healthcare interoperability.

4.3 HL7 FHIR

HL7 FHIR is built based on modular concept, each module called "Resource", these resources represent real clinical or administrative cases. This resources can linked together on different levels to simulate real world scenarios in health care systems.

All resources should have the common characteristics, they are defined and represented based on individual from data types and contain metadata and human readable part. Figure 20 Top depicts shows main common part in FHIR resources.

Resource structure

Each resource has its own structure, this structure is defined by FHIR development committee, and since FHIR is an open source standard, everyone can contribute to define resources and structure of resources, but the approval occurs in many levels by FHIR specialized committees. Figure 20 Bottom depicts an example of DiagnosticReport structure, while Appendix 7.7 shows how the resource has its own characteristics and each characteristic has its own data type, role and constraints.

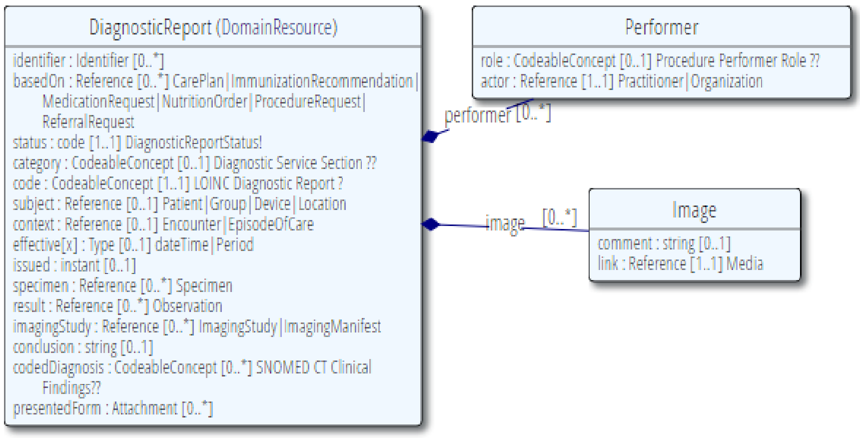


Figure 20 Top) FHIR standard resource parts. Each resource has its own data (Standard Data), identity and metadata. Also it could have human readable part and reference to other resources [3] , Bottom) FHIR Resource DiagnosticReport UML diagram[4]. DiagnosticReport resource contains set of information that is provided by a diagnostic service when medical investigations are finished. It has the ability to integrate SNOMED CT and LONIC to offer the semantic interoperability of the clinical finding. Also it has relation with Performer and Image Resources.

[3] https://www.hl7.org/fhir/summary.html

[4] https://www.hl7.org/fhir/diagnosticreport.html

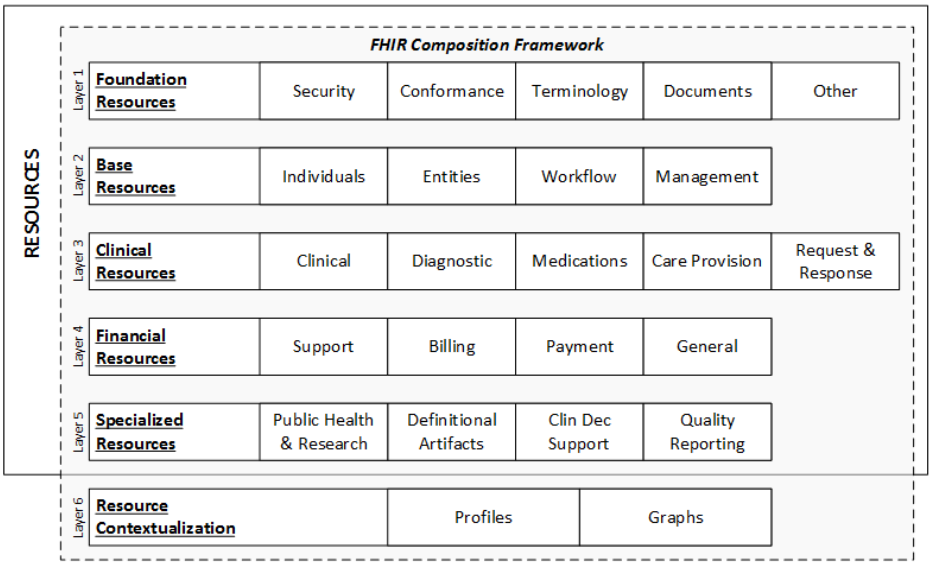


Figure 21 FHIR resources layers and sub groups, this method of grouping has adapted by FHIR committee based on common sense groupings or patterns describing expected structures and/or behaviors amongst resources in the same category [5]

FHIR resources types

FHIR resources are divided into groups according to the aim of the usage, each group has sub groups of resources which has similar meaning. Figure 21 shows how FHIR groups are sorted into: foundation resources, base resources, clinical resources, financial resources and specialized resources.

Relation between resources

Resources also can be linked to each other based on one characteristic or more. For example in DiagnosticReport resource (Figure 20 Bottom) we notice that the field identifier is the characteristic which links this resource to other resources (*CarePlan | ImmunizationRecommendation | MedicationRequest | NutritionOrder | ProcedureRequest | ReferralRequest)* which represents real world scenarios, also the field performer is the characteristic which links performer resource to our current resource. Using these links when needed, development processes can focus on resource-based implementation rather than building customized solutions to build links between resources.

Output/input format

Resources can be used in format of JSON or XML, FHIR adapt this as a part of the standard, but it doesn't suggest any tool to implement there hierarchies. Thus the next part of this project will focus on solution to implement them, below and example of DiagnosticReport using XML format. Figure 22 shows XML FHIR resource output.

FHIR REST API and transactions

FHIR is designed to support RESTful APIs, using resources to exchange information. This approach considers also part of the interoperability, that's because RESTful API is stateless, has uniformed architecture and can be easily extended in contrast to other approach like SOAP or WSDL.

[5] https://www.hl7.org/fhir/overview-arch.html#framework

```xml
<DiagnosticReport xmlns="http://hl7.org/fhir">
  <id value="ultrasound"/>
  <text> <status value="generated"/> <div xmlns="http://www.w3.org/1999/xhtml"><p> <b> Generated Narrative with Details</b>
  </p> <p> <b> id</b> : ultrasound</p> <p> <b> status</b> : final</p> <p> <b> category</b> : Radiology <span>
  (Details : {SNOMED CT code '394914008' = 'Radiology - speciality', given as 'Radiology'};
           {http://hl7.org/fhir/v2/0074 code 'RAD' = 'Radiology)</span> </p> <p> <b> code</b> :
           Abdominal Ultrasound <span> (Details : {SNOMED CT code '45036003' = 'Ultrasonography of abdomen', given as 'Ultrasonography
           of abdomen'})</span> </p> <p> <b> subject</b> : <a> Patient/example</a> </p> <p> <b> effective</b> : 01/12/2012 12:00:00 PM</p>
           <p> <b> issued</b> : 01/12/2012 12:00:00 PM</p> <h3> Performers</h3> <table> <tr> <td> -</td> <td> <b> Actor</b> </td> </tr>
           <tr> <td> *</td> <td> <a> Practitioner/example</a> </td> </tr> </table> <h3> Images</h3> <table> <tr> <td> -</td> <td> <b>
           Comment</b> </td> <td> <b> Link</b> </td> </tr> <tr> <td> *</td> <td> A comment about the image</td> <td> <a> WADO example image</a>
           </td> </tr> </table> <p> <b> conclusion</b> : Unremarkable study</p> </div> </text> <status value="final"/>
  <!--    No identifier or request details were available    -->
  <category>
    <!--    The request was honored by the Department of Radiology    -->
    <coding>
      <system value="http://snomed.info/sct"/>
      <code value="394914008"/>
      <display value="Radiology"/>
    </coding>
    <coding>
      <system value="http://hl7.org/fhir/v2/0074"/>
      <code value="RAD"/>
    </coding>
  </category>
  <code>
    <coding>
      <system value="http://snomed.info/sct"/>
      <code value="45036003"/>
      <display value="Ultrasonography of abdomen"/>
    </coding>
    <text value="Abdominal Ultrasound"/>
  </code>
  <subject>
    <reference value="Patient/example"/>
  </subject>
  <effectiveDateTime value="2012-12-01T12:00:00+01:00"/>
  <issued value="2012-12-01T12:00:00+01:00"/>
  <performer>
    <actor>
      <reference value="Practitioner/example"/>
    </actor>
  </performer>
  <image>
    <comment value="A comment about the image"/>
    <link>
      <reference value="Media/1.2.840.11361907579238403408700.3.0.14.19970327150033"/>
      <display value="WADO example image"/>
    </link>
  </image>
  <conclusion value="Unremarkable study"/>
</DiagnosticReport>
```


Figure 22 Example of DiagnosticReport FHIR resource in XML format for abdominal ultrasound report, contains human readable part at the top as HTML form, Patient resource reference and other metadata. Ultrasound image is linked through reference to Image resource.

4.4 Implementation approach

We have determine previously the suitable standard to use for structural and syntactical interoperability which was HL7 FHIR *(DSTU 2)*, then semantic interoperability can be achieved by integrating semantic code systems[6] such as SNOMED CT, LOINC and RxNorm, we chose to integrate SNOMED CT and LOINC codes to implement our use-case. There is no problem in the use of other standards, as the integration process is the same in FHIR. In this chapter we focus on technical tools and architecture to implement these standards according to system design which we proposed in chapter 2.4 – *Please take a look on Figure 5 -,* user interface design details and techniques ignored, since it out of study interests.

4.4.1 Smartphone part

In this task we aim to convert data acquired from health monitoring device to FHIR standard, and then send it to the server, in addition to display all results on smartphone application to allows users to register, login, send their new measurements and browse previous ones. Therefore we made integrate Hapi FHIR "ca.uhn.hapi.fhir" packages win Android Java Libraries. Hapi FHIR consists of programming libraries of HL7 FHIR for Java, it is an open source project[7] in which each resource is defined by model classes and data type according FHIR specifications, in addition to the parser which can also be used to encode a resource, JSON and XML data format are supported also.

Validation is an important step to ensure that no data is being missing during parsing or generating which ensure in its turn the validity of sending and receiving pressures. If anything wrong happened then, the applications will display error messages. HAPI FHIR provides two sorts of validation, Parser Validation and Resource Validation. Parser Validation used during the parsing of a resource, and it is used in our application basically in two cases: to check observations resources lists when users request for to see previous blood pressure records, and to check patient resource when application retrieve users data to perform certain tasks such as login and updating. Resource Validation is the validation of the raw or parsed resource against FHIR rules, it used in our application to check created resources before sending in case of creating new user profile and new blood pressure measurement.

After the integration of Hapi FHIR, Android native classes are able to use data model in sending and retrieving processes. API Restful client in smartphone are responsible only for executing certain tasks based on predefined conditions, these conditions are provided by the server and contains URL structure, HTTP actions, request parameters in addition to request token. Chapter 0 discuss this issue.

To ensure the protection against data sniffing or modification across of the data transmitted between smartphone and the server, all connections are forced to go through secure socket layer which encrypt all information using encryption key, and allows just the parts that have the key to decrypt the information, more description about this layer is mentioned in Chapter 4.4.2.3.

To display results for users Android XML and view classes are used, this way allows the ability to use data models and to organize the whole code structure in a way that allows extensibility and modification easily.

---

[6] https://www.hl7.org/fhir/terminologies-systems.html
[7] http://hapifhir.io/download.html

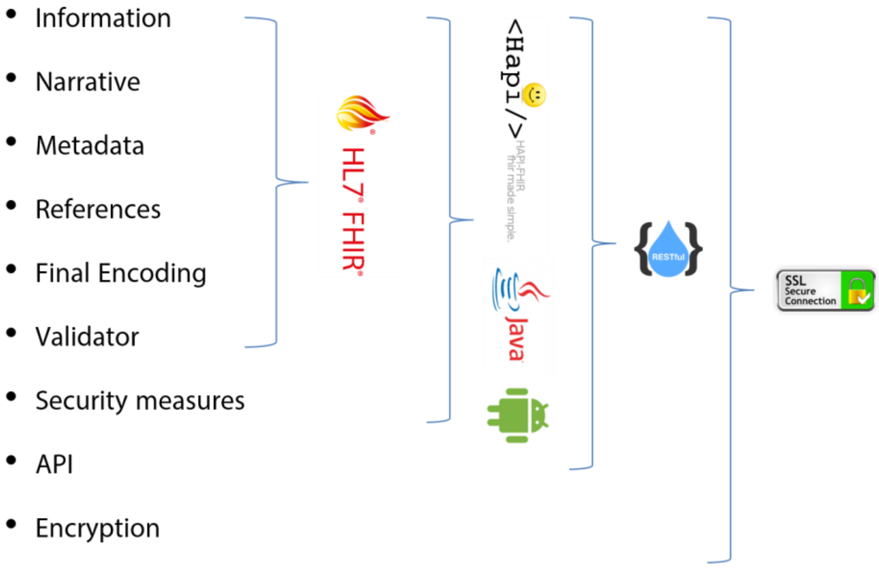


Figure 23 Tools which are proposed to build Application based on health interoperability FHIR standard in Android smartphones. Hapi FHIR libraries[8] are integrated in Android Java libraries to implement HL7 FHIR, then all used to provide secure API using RESTful architecture and secure socket layer encryption

Acquired information needs the following resources to be represented correctly in FHIR:

I. Patient resource
II. Observation resource

Also users can register and log into the application in order to create new observation or browse previous ones.

I. Patient resource:

This resource covers "WHO" defined information about the patient, as FHIR describe it. This resource could be for human or animals, it contains all necessary information to support the administrative, financial and logistic procedures. Usually it should be created from health care provider so it has references to organization resource, in addition to other references. Patient UML diagram is shown in (Appendix 7.8), XML template is shown at (Appendix 7.5)

II. Observation resource

One of the central resources, used usually as a reference to diagnostic reports resources, contains the values with some metadata, and it also has a reference to patient resource. This resource is used in our case to transfer blood pressure data from smartphone device to aggregation server when participants measure their blood pressure, and from server to smartphone when users request viewing of their previous measurements. UML diagram is shown in (Appendix 7.8), XML template is shown at (Appendix 7.6)

[8] http://hapifhir.io/download.html

```java
Observation.Component component = new Observation.Component();
component.getCode().addCoding()
        .setSystem("http://loinc.org")
        .setCode("8462-4")
        .setDisplay("Diastolic blood pressure");
component.setValue(
        new QuantityDt()
                .setValue(Double.valueOf(diastolic))
                .setUnit(diastolicUnit)
                .setSystem("http://unitsofmeasure.org")
                .setCode("mm[Hg]"));
observation.addComponent(component);

component = new Observation.Component();
component.getCode().addCoding()
        .setSystem("http://loinc.org")
        .setCode("8462-4")
        .setDisplay("Systolic blood pressure");
component.setValue(
        new QuantityDt()
                .setValue(Double.valueOf(systolic))
                .setUnit(systolicUnit)
                .setSystem("http://unitsofmeasure.org")
                .setCode("mm[Hg]"));
observation.addComponent(component);
```

```java
public void onRun() throws Throwable {
    Response<ObservationsBundle> response = NetworkService
            .getInstance().getAPI().getObservationRequest(
                    AppRecord.get(AppRecord.AUTH_KEY, ""),
                    "json", "true")
            .execute();
    if(response.code()==200)
    EventBus.getDefault().post(response.body());
}
```

Figure 24 Top) Part of creating FHIR observation resource code using Java in Android, shows the assignment of Systolic and Diastolic blood pressure values, in addition to add LOINC Systolic and Diastolic pressure codes to ensure semantic interoperability, B) Parsing FHIR observation resource in Android using Java, shows how application check part of security measures be checking request token to determine if the request will parsed or ignored

4.4.1.1 User Registeration

When user makes new account, his data will be encoded in two different forms, the first one will contain FHIR patient information field such as first name, family name and age, but other information can't be included in this resource like password will be sent with normal data model, which can be normal JSON message. User credentials info are not part of health care standards that's why we provide two requests, one for interoperability, and other for registration processes. In this way any other implementation which uses FHIR standards will be able to read our application output data. Figure 25 A) shows how user information is used.

4.4.1.2 Send observation resource

To send measurement data, it is firstly converted to FHIR standard form using Hapi FHIR classes, then it will pass API client classes to create FHIR request out of FHIR observation resource. Figure 24 Top) shows observation creation code in the application, we can see how observation attributes are assigned, and how FHIR can use "LOINC" standard to integrate semantic interoperability.

4.4.1.3 View observation resources

Users can retrieve their previous observation, this starts when user sends request to see his observation, this request goes directly throw API, then server will respond with list of FHIR resources, after that API capture this data, parse it using FHIR classes and display it using Android view classes.

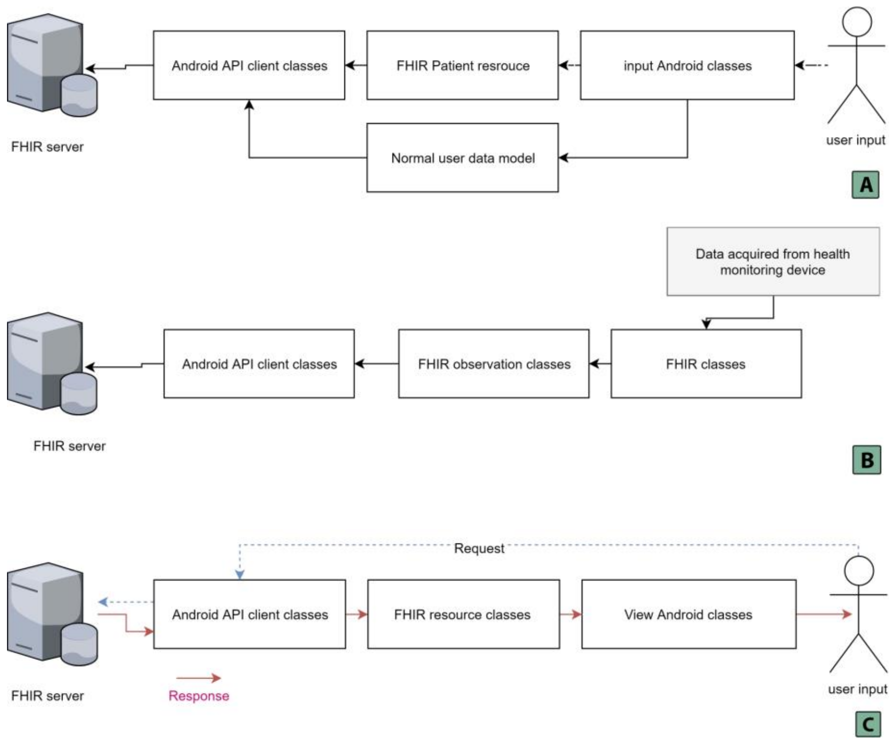


Figure 25 A) create new account dataflow in smartphone application, shows two data models are formed: Normal data model and FHIR patient resource, B) convert BLP data which had been acquired from Blood pressure monitoring device, to observation FHIR resource and send it via smartphone application and sent it to the server, C) retrieve previous user observations and display them in smartphone application

Figure 25 C) shows the data flow in the application, Figure 24 Bottom) shows part of parsing code using Java.

4.4.1.4 Final look

Registration page is the first page appears where users can make accounts in the first time, this is shown in Figure 26 B) and C), after registration confirmation email will be sent to user email to activate his profile, after activation users can log in their accounts using login in page, which shown in Figure 26 A). User can update his account, this is shown in Figure 27 A).

Main page displays last five records of systolic, diastolic and mean blood pressure of the user. Sliding menu can used to choose: create or view blood pressure measurement, update profile and online support, this is displayed in Figure 27 B) and C).

When user enters “My Observation” page, he can see all previous measurements, as Figure 28 A). To make new measurement, user should click “New Observation” button, and then, new page will be displayed to show device using instruction, and then user can connect smartphone to health monitoring device, this is can be shown in Figure 28 B) and C).

Finally users can send messages directly to user administrator, this to report bugs and problems, which is depicted in Figure *26* D).

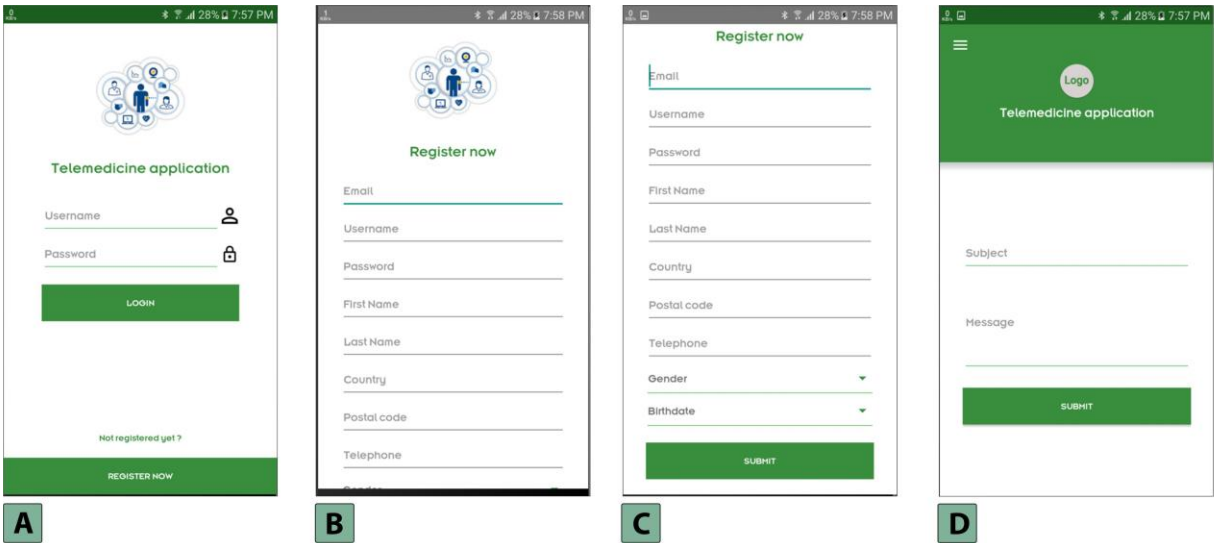


Figure 26 Smartphone application user interfaces, A) application log in page, B) C) user registration page, D) support users interface in the application

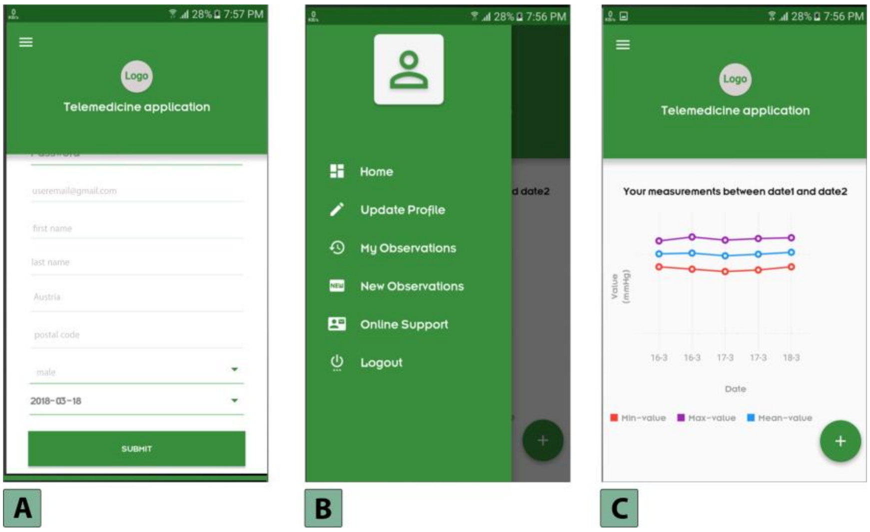


Figure 27 Smartphone application user interfaces: A) update user profile page, B) user menu items, C) home page

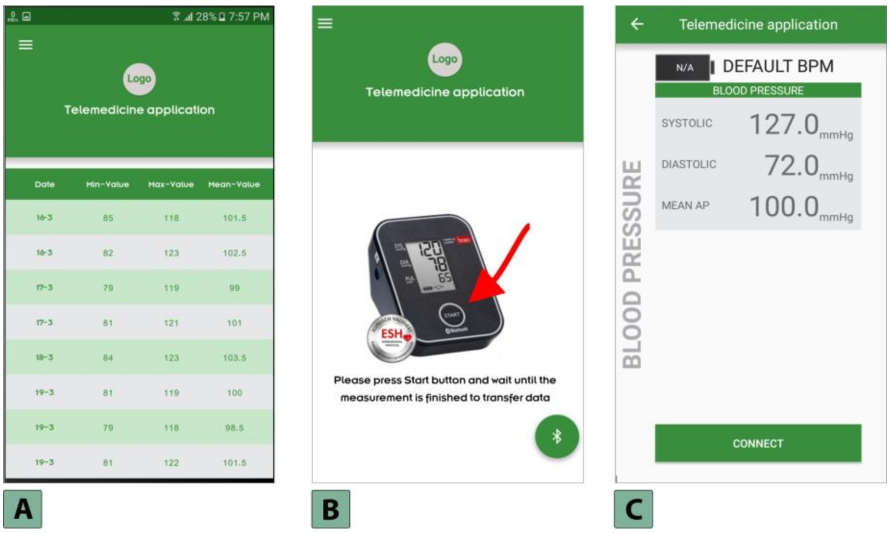


Figure 28 Smartphone application user interfaces: A) view previous observations, B) health monitoring device page before acquisition, C) health monitoring device page after acquisition

4.4.2 Server API side

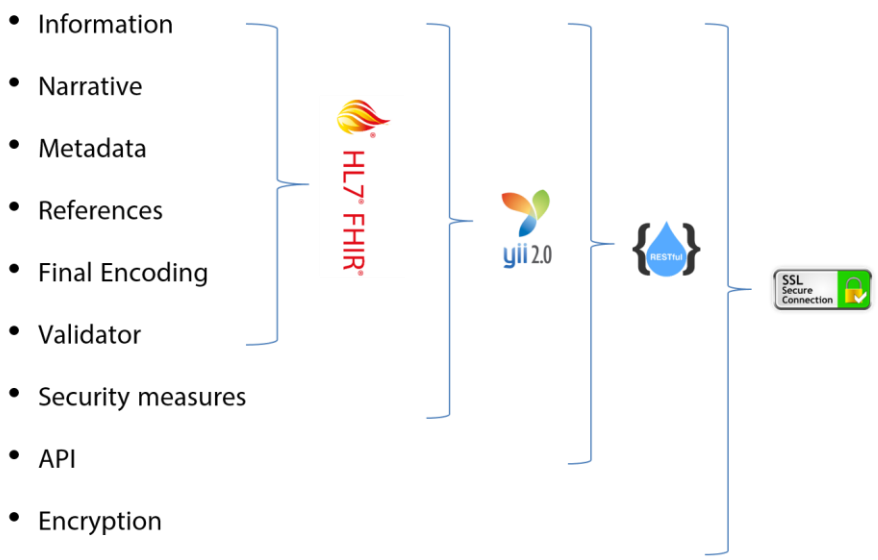


Figure 29 implementation approach of server API & backend. HL7 FHIR, Yii2 web framework, SSL and RESTful concept have been used to deliver this approach

In this task we aim to collect data from smartphone and offer an API to exchange data using RESTful and FHIR, additionally we should design and implement backend user interface to display related information and transactions[9].Figure 29 shows our solution parts, where HL7 FHIR is responsible for providing health interoperability and connection security is achieved using secure socket layer. Yii Web framework is used to implement FHIR concepts and integrate SSL, then all technologies combined works to offer RESTful API.

4.4.2.1 System description

This system contains resources management interfaces which contain:

- **Patient control**: this part allows adding new patients, and contain all users' information.
- **Practitioner control**: contain all information about doctors and specialists.
- **Organization control**: this part controls health care facilities.
- **Diagnostic control**: contains information of medical diagnosis results which made by practitioner. Usually this contain references to the patient, practitioner, observation and organization resources.
- **Observation control**: contains all of medical observations, and results like blood pressure values in our case. Usually it have references to the patient, practitioner and organization resources.

Following actions: create, update, read, delete and browse history can be applied to each resource.

This part will provide tool for direct communication to other systems directly using FHIR and other one for direct parsing of any FHIR resource.

[9] Some parts of this chapter (Server API) have mentioned before in my colleague thesis [14], and repeated here to complete the meaning.

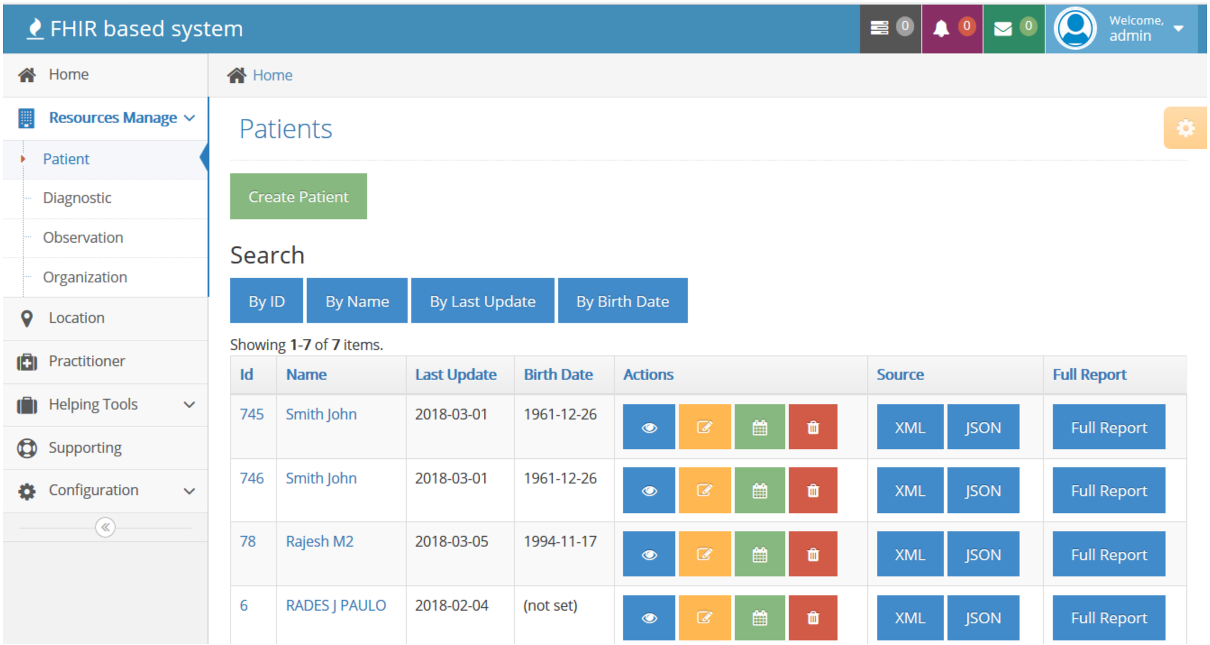


Figure 30 Screenshot of the backend shows patients resources management interface. Authorized system users can view, add, update, remove and browse patient resource history. The system also offers XML and JSON formats for exporting. "Full Report" button provide general view for all resources related to certain patient resource.

System administrator can have access using email and password, and other levels of authorization can be granted for other users such as supervisor or students to access to different levels in this backend.

4.4.2.2 HL7 FHIR resources

To implement this from FHIR point of view we should use the following resources:

I. Patient resource
II. Observation resource
III. Practitioner resource
IV. Organization resource
V. Diagnostic resource

The first two resources are used directly to transfer blood pressure from mobile device to the backend, but other resources are required as they have references between each other's to support control and analysis of this data.

Practitioner resource

This resource cover any individual who are working in health care service as part of their formal duties, they could be: physicians, dentists, pharmacists, nurses, therapists, medical technicians, laboratory scientists and others. This resource has relation to qualifications of the individual. This resource is used in the backend to assign observations performer. Practitioner UML diagram is shown in Appendix 7.9.

Organization resource

This resource is used to describe collection of people that have come together achieve an objective, as it described by FHIR website. This resource has reference normally to contact resource. It has been used in the system to check the organization that own certain resource such as observations or diagnostic repost. UML diagram is shown in Appendix 7.9.

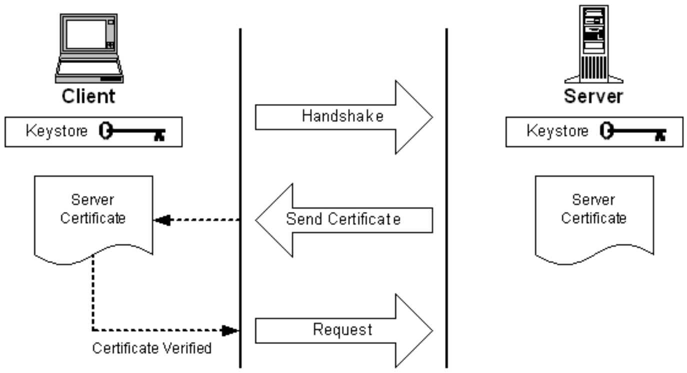


Figure 31 Secure Sockets Layer connection procedures. Starts from top when client starts Handshaking, then exchange certificates, and then verified connection can be established[10], all connection of the system went through secure socket layer.

Diagnostic resource

A diagnostic resource describe is the set of information that is provided by a diagnostic service when medical investigations are finished. This resource could be used in our system to provide the final diagnosis of patient, for example it could be hypertension diagnosis for a patient. UML diagram is shown in Appendix 7.9.

4.4.2.3 Data encryption SSL

HL7 FHIR is a health care data standard but it is doesn't deal with security aspects since it isn't part of health data problem itself. Thus we've used Secure Sockets Layer (SSL) which provides security over networks.

All connection through the API will pass throw this layer which encrypt outgoing requests data and decrypt ingoing response. This layer will provide two main points:

- Assure that parts are communicate directly to the server, not any other part.
- Ensuring that only the server can read what smartphone sends and smartphone can read what sends back.

And this occurs through three main steps:

- **Handshake** begins with the client sending a smartphone sends first message, which contains all required information needed in order to connect to the client via SSL, including the maximum SSL version supported. Then server responds with a first server message, which contains similar information required by the smartphone, then decision made about which version is supported in both parts.
- **Certificate Exchange**, after connection is established, the server proves its identity to the smartphone, using its SSL certificate. An SSL certificate consists of various segments of data, including the domain, the certificate's public key, the signature and validity dates. Smartphone checks if certificate is trusted by one of several Certificate Authorities.
- **Key Exchange**, the encryption of data exchanged by smartphone and server is using symmetric algorithm, using a single key for both encryption and decryption. To agree on the key, asymmetric encryption and the server's public/private keys are exchanges securely.

Figure 31 shows Secure Sockets Layer connection establishment steps.

[10] https://docs.oracle.com/cd/E57185_01/EALIS/ssl.html

4.4.2.4 Web development framework Yii2

In order to link previous technologies together, server-side programming framework should be used, in our case we chose Yii2 which is PHP web framework, provide group of features for integration, security and efficient friendly user interfaces.

Yii2 features for API implementation

Yii has been developed to contain modern classes which give the developers the possibility to generate different kinds of web services by using modern inheritance process between classes and combining between strong concepts like class mapping, data-types definition and using MVC pattern design.Yii as many web frameworks provide MVC concept which Simplify the development and separating the logical parts from user interfaces are the most important things which should be consider during the implementation steps for any software, because of that, Yii framework gained importance by following Model, View, and Controller pattern, which gives the possibility to manipulate anyone of thus technologies without effecting the rest. Parts of MVC pattern:

- Model: The responsible part for rules and logic and it has no relation with user interfaces.
- Controller: Controlling and managing the communication between users and model, and plays a small role in viewing step.
- View: Responsible for the visual part which users deal with, containing all interface elements.

Also, to control all processes during the development, Yii has main controller which collects the data from users beside the requests and after that divide the requests between system parts.

Three layers of input validation facilitate exploring and tracking errors which are very important in the software environment, based on this importance, Yii provides three levels of input validation starting with databases model constraints validation, then the controller rising exception errors and finally the user interface direct or indirect validation. This architecture gives the developers the possibility to control the developing process and monitoring the system, and prevent any not valid information to enter the system.

Since authentication and authorization play an important role in the system protection and managing the access to the system, Yii provides a wide range of user identity verification like email-password pairs, username-password pairs and two factors authentication, which build beside the other sorts of authentications for distributed systems like token a strong audit trail process. This is one of recommendations of FHIR development guideline, in Figure 32 the first left case which is recommended is integrated in Yii2.

Also Access Levels Control concept in essential when with sensitive data like medical data are processed which always requires a high level of authorization, any accessing to the system must be examined and monitored to know whether the user has the right to access. User access levels can be easily implemented in Yii2. This functionality alongside with Yii structure which gets advantages of MVC, active records and access level control, can offer impenetrable wall in front of hackers cutting the way for them to use any gab in the security process.

Most important, from designing perspective, Yii2 is an object-oriented framework which corresponds to the nature of FHIR as a resource-oriented framework, thus resources of FHIR can use Yii implicitly data models and MVC which the design pattern of Yii, to facilitate the implementation of RESTful API and the integration of FHIR classes. Furthermore Yii supports the extensibility and scalability by using modern concepts like as Name spaces, Autoloaders and composer-integration.

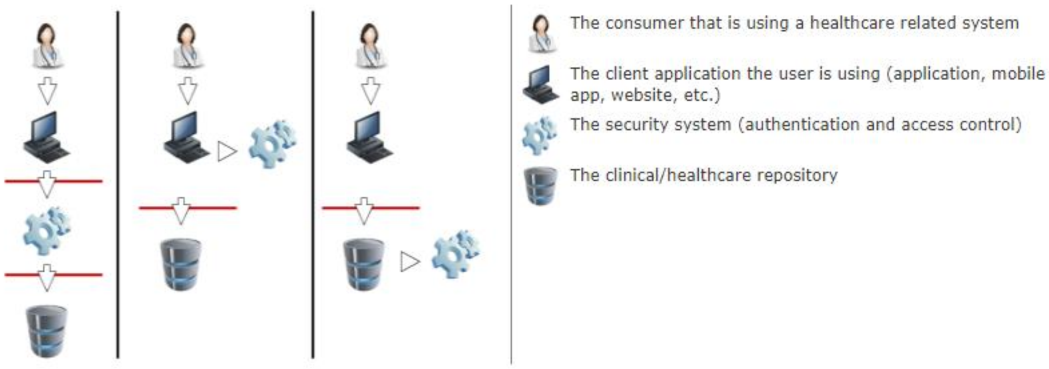


Figure 32 FHIR systems security cases for authentication and access control, first one left is recommended since all connections cross through security layer[11], to check security and users control level

To give Yii2 the ability to generate and parse FHIR resources, we integrate Dcarbone/PHP-FHIR[12] library, which is an open source PHP Classes. In this way we can receive XML messages and convert it to object in Yii2, then this object is easily processed, on the other hand we can generate XML resources starting from Yii objects.

[11] https://www.hl7.org/fhir/security.html
[12] https://github.com/dcarbone/php-fhir

4.4.2.4.1 Integrate FHIR with Yii2 in to perform requests and responds

Create/Edit a resource record

This is started when FHIR request is received, then Yii controller classes with receive the request and extract FHIR resources. Yii controller will communicate with FHIR parsing/generating classes to parse the resources and then assign them to suitable models, these Yii models are customized to adapt to FHIR resources structure, the final output of this step are Yii model objects which emulate FHIR resources structure and data types. When model objects are ready, they can be used by FHIR Database controller which adapt them to be sent to FHIR database system and validate them before sending, here they will be converted to FHIR resources again to be sent to FHIR database system if the database has external API or they can be encapsulated into query to be internal in Internal FHIR database. Figure 33 A) shows these relations and how FHIR requests are parsed and passed to FHIR database system.

This is corresponds in smartphone application to create and update patient requests, and create blood pressure observations. Figure 35 shows how data flows from smartphone to the server though Yii FHIR API.

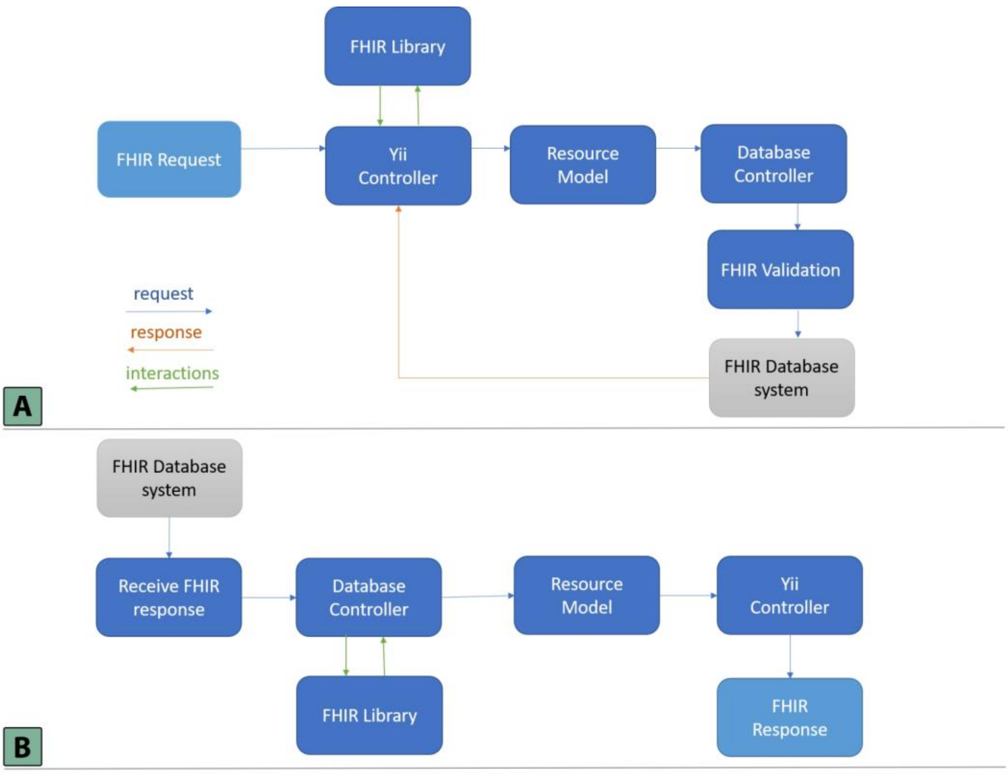
View/History of resource record

When FHIR database system sends FHIR response, Yii classes received it and pass it to certain classes depending on the type of database system, then move it to database controller classes which interact with FHIR parsing/generating libraries to parse it, then assign this parsed information to Yii data model, after that Yii controller will send this data as response, this data could be normal data output used in interfaces or could be FHIR resources ready to be sent through the API. Figure 33 shows these relations.

This is corresponds in smartphone application to retrieve previous Blood pressure observations of the user. Figure 35 shows hoe Request and retrieve FHIR resources from FHIR server through developed FHIR API are done.

Delete a Resource record

The controller will send Delete request to FHIR database server to delete a record, the returned response will be sent to FHIR Library to get the related PHP object from XML or JSON format and sent back to the controller which will show it on the UI.




```php
static function viewAction($resource, $id) {
    $parser = new \PHPFHIRGenerated\PHPFHIRResponseParser();
    $json_response = @file_get_contents(Yii::$app->params['fhir_url2'] . '/' . $resource . '/' . $id . '/_history');
    $object = $parser->parse($json_response);
    if (!isset($object->entry[0]->resource->$resource)) {
        $json_response = @file_get_contents(Yii::$app->params['fhir_url2'] . '/' . $resource . '/' . $id . '?_pretty=true');
        $object = $parser->parse($json_response);
        if (!isset($object->identifier)) {
            $text = explode('pre>', $json_response);
            $text = explode('</', $text[1]);
            return $text[0];
        }
        return $object;
    } else {
        return $object->entry[0]->resource->$resource;
    }
}
```

C

Figure 33 A) Create/Edit a resource record using Yii2 libraries, this starts with FHIR request from the smartphone or other parts, then pass to Controller which interact with FHIR libraries to parse the request, which become normal Yii data model. After that it passes through database controller then it will be validated and sent to FHIR database system, B) View resource using Yii2 libraries, this starts when FHIR database system sends FHIR resource, it passes database Controller and parsed to become normal Yii2 data model to pass then Yii controller and after that it becomes FHIR response C) parsing XML FHIR resource using Dcarbone and Yii2 in server API

4.4.2.4.2 Link user account to patient profile

We have designed MySQL database to allow Yii2 to manage authorization of the users, and provide login interface. Another important use of this data base is to link patient resource in FHIR to user account in Yii, this achieved by using “user_fhir_account” table, accordingly each user has FHIR patient resource and he is able to create, update and review his records. Figure 34 shows MySQL database structure and relations

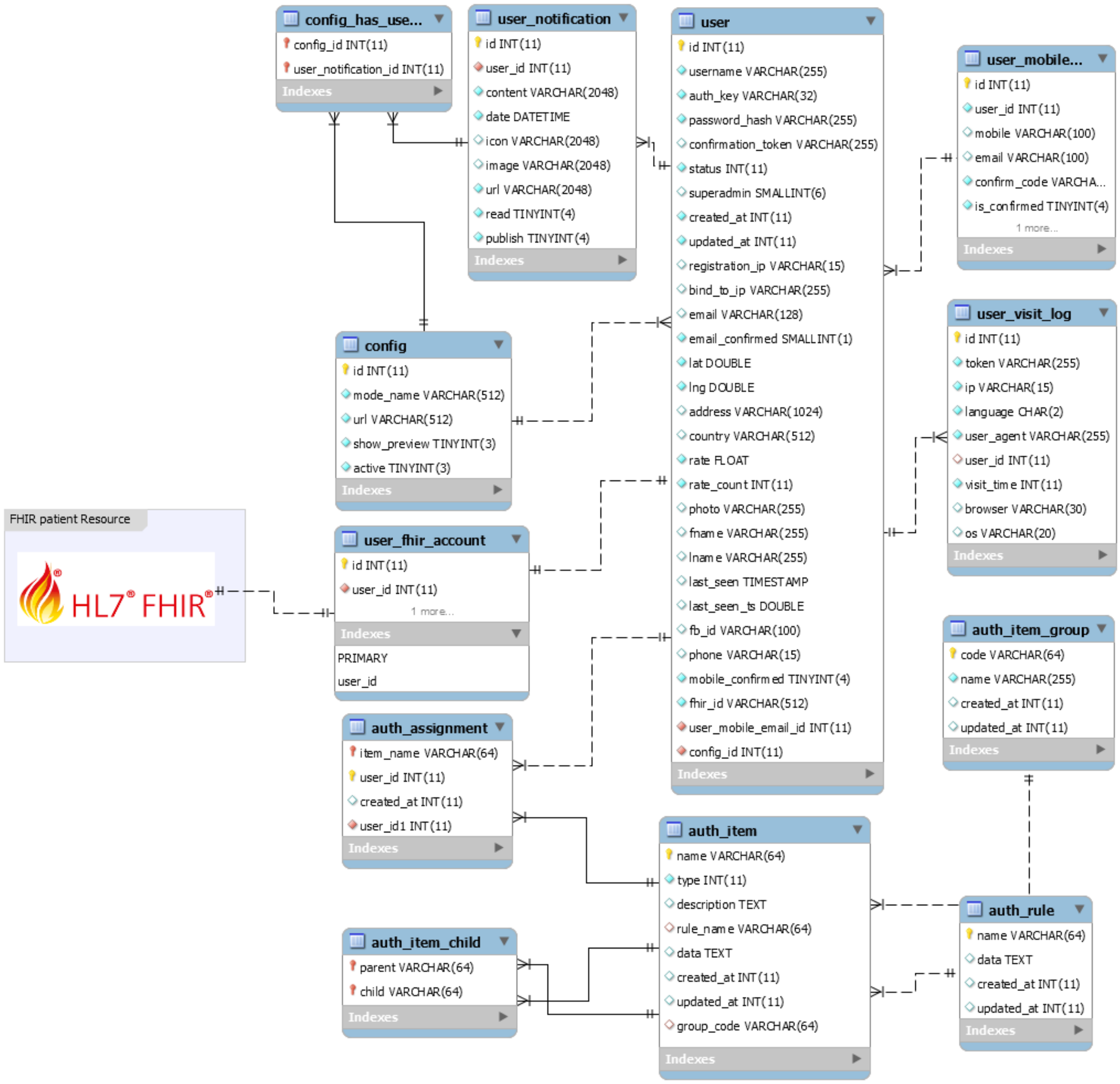


Figure 34 MySQL database Entity–relationship model which integrate Yii2 users model with FHIR patient resource through "user_fhir_account" table in the project. The ID of the patient resource is stored in this table and using this Yii active records model we can build relation that allows to call patient resource classes and functions directly from user classes, the programming result will be one object represent Yii user and FHIR patient

4.4.2.5 RESTful API

REpresentational State Transfer (REST), or RESTful web services is the layer -in our design- which benefits from all other technologies before. It has used here because HL7 FHIR committee recommend this, since it stateless and scalable, also RESTful API will offer Simplicity of a uniform Interface, and resistance of failure of the whole system in presence of on component has failed [50].

RESTful API URLs structure should be as the following:

VERB [base]/[type]/[id] {? -format=[mime-type]}&auth_key=AUTHKEY

Where: Verb: POST, GET, DELETE or PUT

Base: Service Base URL

Type: name of a resource type (e.g. “Patient”)

Id: resrouce ID

Mime-type: The Mime Type (e.g. “application/xml+fhir; charset=UTF-8”)

Auth key: is the key which used for authentication

Main actions in our system which the API will deliver are: create, update, read, delete and browse history. Full list of resource API action URL are

ACTION	VERB	URL
CREATING PATIENT PROFILE	POST	/Patient?_format=xml&auth_key=AUTH_KEY
UPDATING PATIENT PROFILE	POST	/Patient/ID?_format=xml&auth_key=AUTH_KEY
READING PATIENT PROFILE	GET	/ Patient/ ID?_format=xml&auth_key=AUTH_KEY
CREATING OBSERVATION	POST	/Observation?_format=xml&auth_key=AUTH_KEY
READ OBSERVATIONS	GET	/Observation?_format=xml&auth_key=AUTH_KEY
READING OBSERVATION	GET	/Observation/ ID?_format=xml&auth_key=AUTH_KEY

Table 1 Basic Interactions to exchange FHIR resources which are related to blood pressure measurements between smartphone application and server programming interfaces, other ordinary interactions are neglected here.

Create patient and observation resource

Here when the client, which in our case the smartphone send create or update request, this request is received by API layer then parsed with FHIR classes then use other classes to pass to server layer, at server layer validation occurs, if the resource is correct, then it is stored or updated, otherwise exception message will be generated and send back to the client. Figure 35 A) shows scheme of these processes.

Read patient and observation resources

Read request is made by client then it send directly to server passing API and auxiliary classes to the server, then server will respond with proper response to display requested resource or send warning message if the is not found or redistricted. Figure 35 B) shows schema of read resources.

History of observation resource

Client sends history request which is resolved by API layer then go to auxiliary classes, then goes to FHIR server. Server responds with proper respond. . Figure 35 B) shows resource history request.

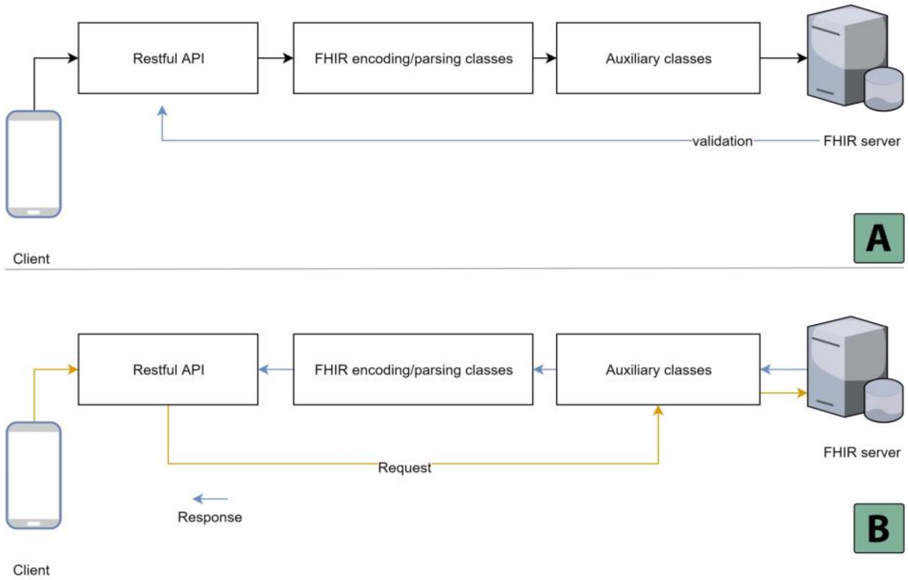


Figure 35 A) Create/update FHIR resources data flow from smartphone to the server though developed FHIR API. Validation is part of the process B) Request and retrieve FHIR resources from FHIR server through developed FHIR API

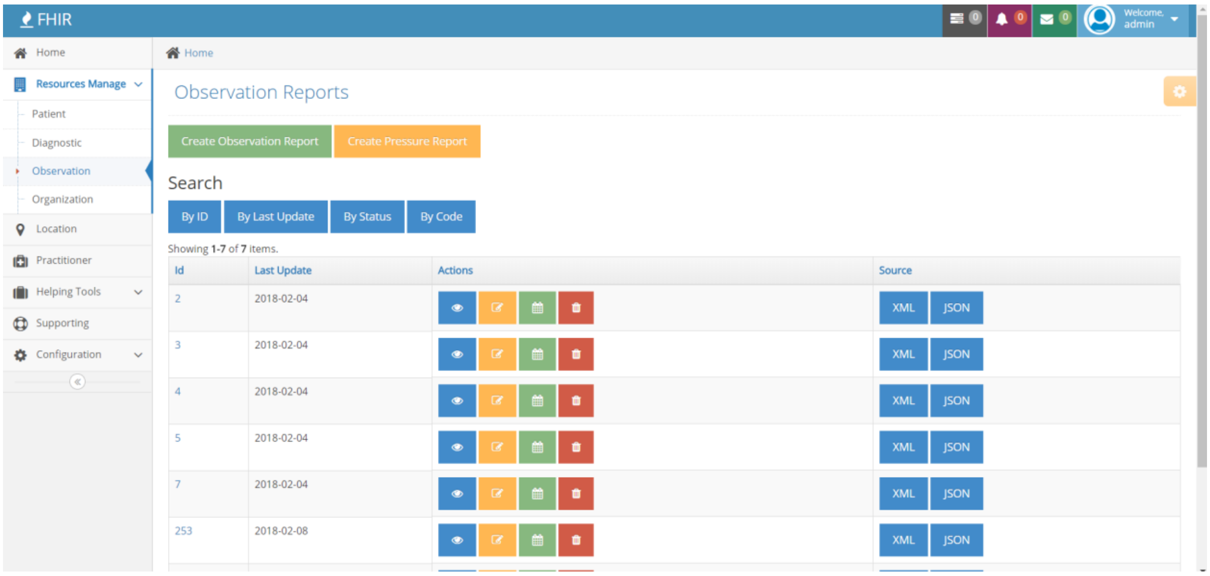
4.4.2.6 Final look

The final step is to integrate user interfaces, we have been keen to deliver user friendly interfaces to simplify the usage even for non-experts users. The next pictures show only the system parts for observations management, since it related to our acquired measurements display, similar interfaces are generalized for all resources[13].

Figure 36 Top) shows UI where system administrator can get a list of all observations on the system with a few extra options, like search options by different fields, view, edit, delete, history of an observation and the downloadable XML or JSON file that represent the selected observation. The Figure 36 Bottom) displays the page where admin can create new observations. This page contains the observation needed fields, which includes choosing patient, a practitioner and other data.

The administrator can view the details of each observation in the system. Any information related to the observation is shown in this page, including links to the related patient or practitioner, in addition to Blood pressure and heart rate information. The ability to visualize some sorts of data is provided also as seen in Figure 37. Admins can view last edit date and view some extra options like updating the observation, history or delete it if it isn't connected to any other resource. Admin can edit the data in an observation by changing the content of any field, each time an observation is edited a history record will be created, this list of history record can be accessed by the admin and reviewed at any time (the history list or details for each one), this is shown in Appendix 7.10 . Admin can access a patient full report and review all the patient's history, observations and diagnostic reports. All related patient information can be found in this page.

[13] Some backend User Interfaces have mentioned before in my colleague thesis [14], and repeated here to complete the meaning.



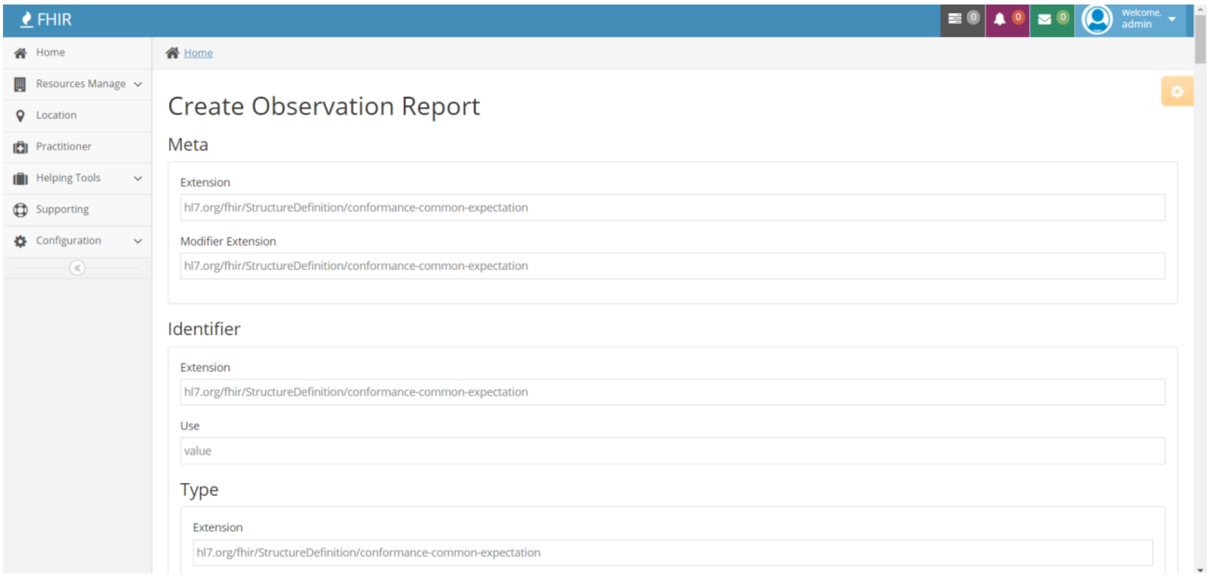


Figure 36 Top) Part of Backend UI for observations management, Authorized system users can view, add, update, remove and browse history of observation resources. The system also offers XML and JSON formats for exporting. Searching among observation is included also, Bottom) Part of backend UI to create observations, this form can be used by doctors to enter the values directly in the system, and this interface contains all possible required field to generate FHIR observation resources.

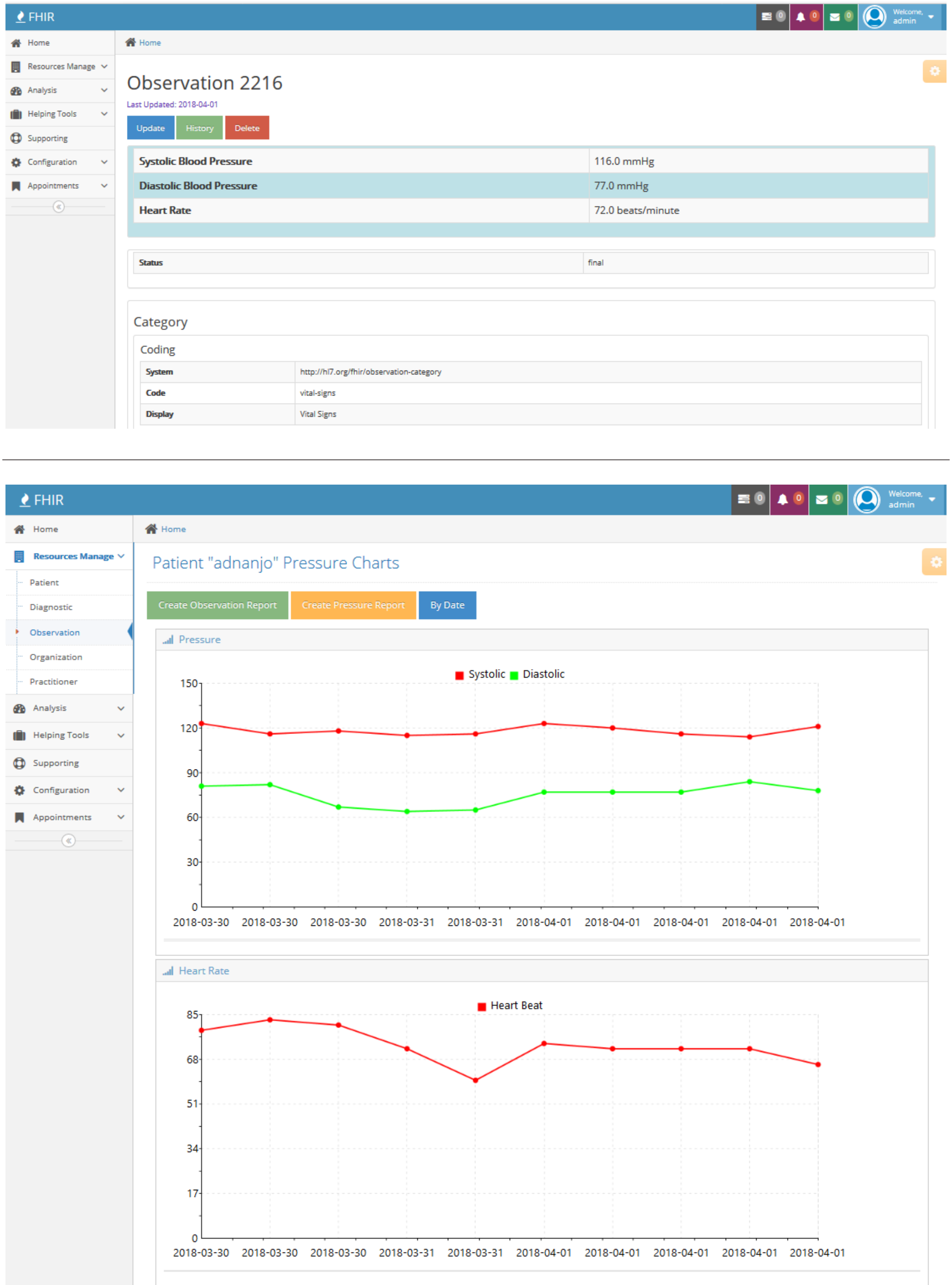


Figure 37 Top) Part of UI for observation resource view. This page is used to view any retrieved observation resource, providing detailed information and Meta data and references. The image shows the values of Systolic, Diastolic blood pressure and heart rate which has been acquired from health monitoring, Bottom) User interface to visualize blood pressure and heart rate values which have been stored in the server, these values has been acquired from health monitoring device and transmitted according to FHIR.

4.5 Other concerns

4.5.1 User privacy and security issues

Since health interoperability standards doesn't provide guidelines about where to store data and how to protect user privacy, users privacy concerns is an issue. Patient' information usually stored in servers which could be prone to cyber-attacks, or other forms of privacy violation. We have find the following suggestions to mitigate this issue

- Store information in local servers connected to local network in the location of health care facilities.
- Prevent external access to the local network, and when external connection is required it should occurs across server API through proxies.
- Also servers should be dedicated only for information storage and exchange to prevent any possible threats.
- All connection should be encrypted with certificate with high key length from trusted authorities.
- Servers must do periodical backup for all data, backups should be stored on external storage to prevent data lose in case of system failure.

Some studies recommended also to use hardware encryption [51] beside software encryption, this could provide additional protection, but as usual this is a trade-off between the performance-costs and security measures.

Cloud computing services are being very common. They can provide a good alternative of normal dedicated databases servers, as they get the advantages of separating virtual machines and firewalls easily arranged backup in addition to physical protection [52], but they still lack being in healthcare facility geographical domain, which poses question about data privacy.

4.5.2 Non-expert user problem

Health information systems are used by IT non-experts such as patients, doctors or hospitals staff, that could lead to some mistakes during data entry and usage, this human factor couldn't be excluded completely, but we can ease this problem by using easy friendly interfaces and forms, put hints and clarifications to describe any ambiguous value or field, these alongside with little training for system users should be sufficient to get rid of most of errors.

5. Testing and evaluation

This chapter discusses testing of the first 3 tasks of the project (all tasks are clarified in chapter 1.2), other tasks concerning analysis platform has been tested before by my colleague as part of his thesis [14], so this test focuses on correct delivery of data and check functionality of the system to transfer data between health monitoring device and smartphone, then between smartphones and server, besides to check user interfaces in server backend and smartphone application.

Since health interoperability can't be explicitly tested in this project, the correct transmission and functions are the proof that the interoperability standards are implemented correctly and applications has been built according to these considerations. On the other hand, the collected data will be used to test a case of physiological measurements about blood pressure variation using statistical hypothesis and tests.

5.1 System testing and Evaluation

5.1.1 Method

Ten participants have to measure their Systolic and Diastolic blood pressure twice a day, once in the morning and once in the afternoon for five days, using health monitoring device and their smartphones. The participants are placed at different places in Vienna city, Austria and using different ISPs to access the internet. All participants use Android-operated smartphones, Android versions higher than 5.xx.

Each participant logs in the application in his smartphone using username and password and using new observation button, transfers data from health monitoring device to the server, as shown in Figure *28*. The aims of this test are to test the functionality of the system during time span and different requests, and check the application on different smartphones to assure correct data delivery from health monitoring device to the server, then use this collected data in a physiological measurement test of blood pressure changing during the day.

5.1.2 Results

After five days, we are able to see that all measurements which have delivered to smartphone were transferred correctly to the server but some measurements were interrupted due to problems with device cuff placement, and then the device shows error message and stops the measurement. Participants were able to see their previous records on the application, and no participant express problem with using the applications interfaces. System administrator was able to see participants' profiles and blood pressure observations information in the backend and all FHIR resources and integrated semantic interoperability parts.

5.1.3 Discussion

Based on the results we can conclude that data are transferred correctly from health monitoring device to smartphones and then to the server. There were some interruptions because of wrong use of health monitoring device but this is considered outside data transfer domain, even though this highlights the suggestion to train people how to telemedicine devices.

Since participants' data were stored correctly in FHIR server, they were able to see their previous observation and system admin was able to view those results, and thus these data are correct and ready to be used for another part of the project and for physiological measurements test.

5.2 Physiological Measurements and Evaluation

5.2.1 Introduction

The circadian clock in the human body is essential to maintain internal cycles of metabolism and physiological functions. Blood pressure changes during the day are one of the cycles which are subject to the circadian clock. Abnormal blood pressure variation has always been associated with more likelihood of many health problems including obstructive sleep apnea [53] [54], kidney disease [55] and others.

Many studies have shown that the blood pressure changing pattern is closely related to sleep-wake cycle, suggesting that the systolic and diastolic blood pressure is increasing in the early morning, reaching highest values in the middle of the day and then start to decrease gradually [56] [57].

If we consider that the collective measurement process of blood pressure itself has improved recently to provide more potentials to study blood pressure variation during the day hours based on modern personal health monitoring devices, which allows the transmission of the vital data to main aggregation reservoir. In this context, this test propose was to analyze the data collected from participants using blood pressure monitoring device which transfer the data to the main server, to determine if SBP Systolic blood pressure and DBP Diastolic is blood pressure different in the early morning in comparison to late evening.

5.2.2 Method & Measurements

Nine males and one female volunteer (mean age is 29 ±2 years; ages between 27-31 years) participated in this test. All volunteers had no physical illness nor family history of hypertension and they don't work in jobs requiring muscular effort, working in offices jobs or students. Neither of them use drugs or take regular medication and beverages containing caffeine are not allowed for one hour before the test to exclude caffeine factor [58]. All of the volunteers are residents of Vienna city.

Participants have a regular schedule for sleeping and waking, the measurements are done twice a day for five days, once in the morning between 9-10 am and once in the evening between 8-10 pm, all measurements are acquired using "**BosoMedicus System** Wireless upper arm blood pressure monitor" from the bare upper arm.

Before taking a measurement each participant had to sit comfortably for the blood pressure measurement, supporting his back and arms and placed his feet flat on the floor, relax for 5 minutes. For measurement, each participant had to grasp the end of the cuff that feeds through the metal ring and wrap it around the outside of the arm as shown in Figure 38,then starts the measurement with the start button. The pump starts to inflate the cuff and the he rising cuff pressure is displayed as a

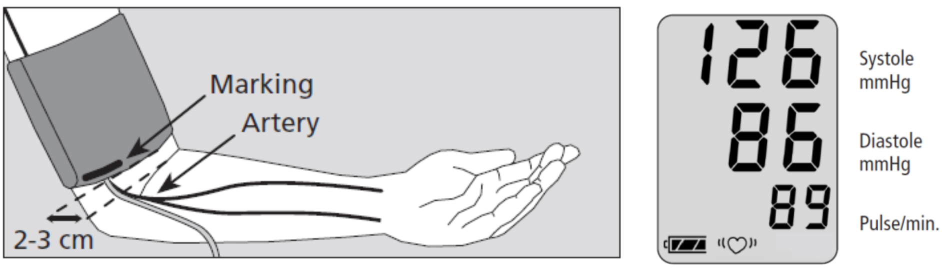


Figure 38 Right) Cuff position during blood pressure measurement, correct measurement should be taken two cm above the elbow, Left) health monitoring device output after measurement showing systolic and diastolic pressure values.

digital numerical value and in the form of a bar on the left edge of the device screen. When the proper pressure is achieved, the device switches the pump off and releases the air slowly from the cuff. During the measurements, participants shouldn't move. After each measurement, each participant had to use a smartphone application to transfer device output data to the aggregation server using an internet connection.

We formed our statistical test hypotheses as to the following. Null Hypothesis $\mathbf{H_0}$, there is no difference between Systolic and Diastolic blood pressure measurements of the participants in the morning and in the evening. Alternative Hypothesis $\mathbf{H_1}$, Systolic and Diastolic blood pressure measurements of the participants in the morning are different in comparison to measurements of the evening [56]. If the results rejected the Null hypothesis, then we can accept that there is a significant difference between morning and evening measurements at the certain level of significance.

Because the data is for the same participants in the morning and evening, so these datasets are related to each other, we can use T-test for matched pairs. For T-test for matched pairs the differences of datasets are normally distributed should be fulfilled as a prerequisite. To check this condition, we used Shapiro-Wilk test of the differences. Then T-test matched pairs two-tailed test is carried out to check the Null hypothesis.

5.2.3 Results

The results of Shapiro-Wilk tests of datasets difference has shown that all both differences of Systolic-diastolic in morning-evening are following a normal distribution with a level of significance more than 5%, then the prerequisite of paired samples T-test is a full field, this is shown in Table 2 A.

The results of paired T-test for two samples in Table 2 A shows clearly that there is a significant difference in the means between the morning and evening measurements in both systolic and diastolic blood pressure groups for 95% confidence interval. Median and standard deviation box plot of each participant measurements show changes in the difference between morning and evening measurements for each participant, but still provides clear visual confirmation about the differences in the whole group, which has been found also in box plots of all participants which are shown in Figure 39.

	Statistic	*Degree of freedom*	*Sig.*
Diastolic pressure morning-evening difference	.975	50	.378
Systolic pressure morning-evening difference	.973	50	.312

A)

	Paired Differences					t	df	Sig. (2-tailed)
				95% Confidence Interval of the Difference				
	Mean	Std. Deviation	Std. Error Mean	Lower	Upper			
SBP Morning - Evening	-8.28	5.41366	.76561	-9.81	-6.74	-10.81	49	.000
DBP Morning - Evening	-7.64	4.81393	.68079	-9.00	-6.27	-11.22	49	.000

B)

Table 2 A)Shapiro-Wilk tests of datasets difference of Systolic and Diastolic blood pressure in the morning and evening, showing normally distribution, B) Two paired samples T-test results of morning and evening has shown clear difference between the mean values of both groups.

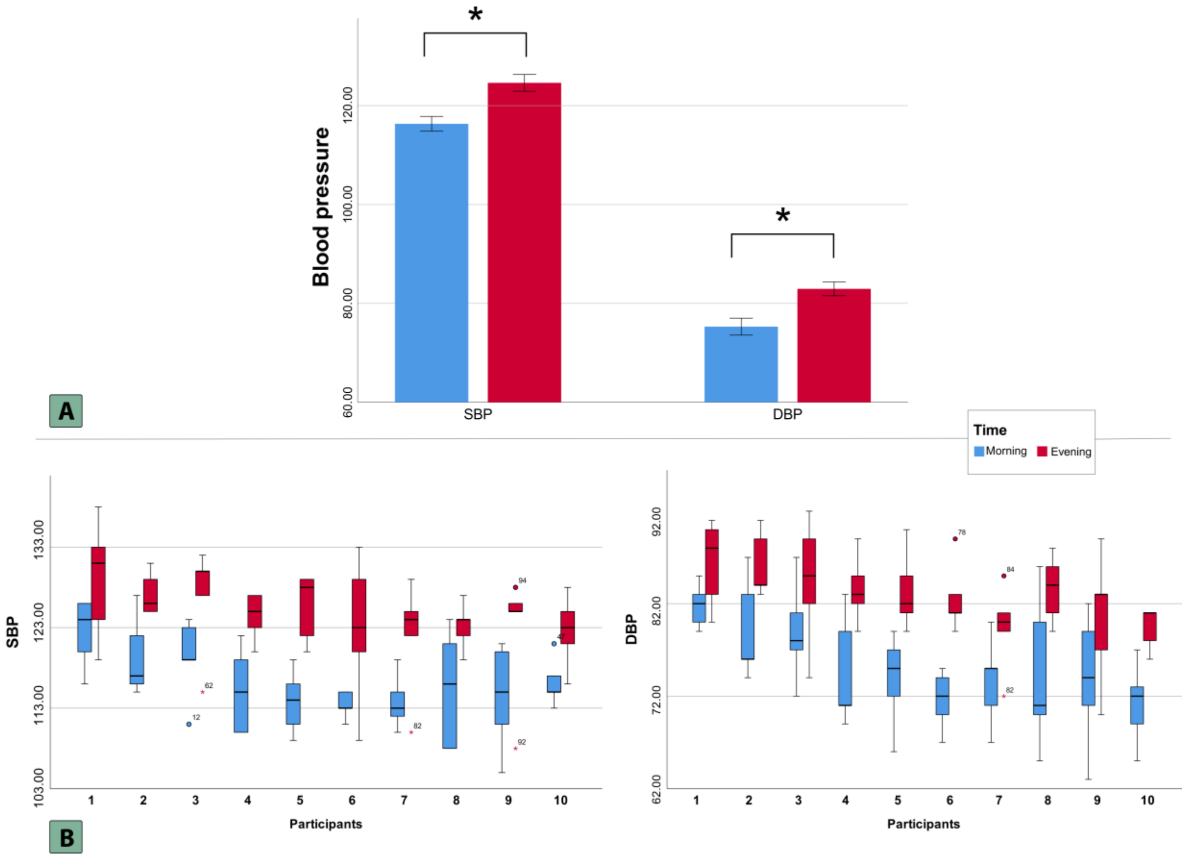


Figure 39 A) Box plots of whole participants groups for systolic and diastolic blood pressure showing clear distinct between means of the morning and evening measurements, The statistical differences between the bars are indicated by asterisks "" based on paired samples t-test with 0,95 confidence interval, B) Box plot of each participant for Systolic and diastolic blood pressure in the morning and evening. Each participant has different blood pressure difference between morning and evening.*

5.2.4 Discussion

The results confirmed the studies about the difference between blood pressure measurements in the morning and evening [56] [57], which varies according to each participant. All participant measurements have shown higher values for systolic and diastolic blood pressure in the evening. The measurements method introduced to all participant at the beginning, but during the course of the test measurements were done by the participant themselves with little guidance when needed, thus we can't proof the complete correctness of all measurements. Even though the system was able to receive all patients' data in semi-real time and make it available for analysis, this capacity will be combined with environmental data retrieval in the second part of the project to detect any possible relations between human body vital data and some environmental parameters in Vienna city. This concept can be generalized on larger scale to collect big amount of patients' detailed vita data without the restriction of location and time, and feed it to machine learning algorithms to address medical issues facing us at the present time such as predictive therapy [59] and computer aided lesions detection [60], therefore we think that the process of remotely collecting of patients data looks very promising for future applications as it is consistent with the current and future trends to invest information systems as data source of all daily life activities.

6. Conclusion

Health interoperability problem between telemedicine system parts has been presented in this work, therefore a theoretical concept of healthcare information model and sublayers have been discussed. Each layer in this model requires specific tools and implementation approach in real-world, thus the implementation of these layers are covered within work chapters, starting from basic information collection stage to transmission stages, to function interfaces between healthcare information system components which allows the interoperability.

Initially, the work started with the acquisition and analyzing of incoming vital signs via Bluetooth Low Energy from health monitoring devices, especially healthcare BLE profiles, then moved to focuses particularly on blood pressure and heart rate signs, to show how data can be extracted and processed before sending via mobile applications to a central aggregation server.

The process of transmission to the central server was executed using HL7 FHIR standards through secure socket layer. Accordingly, this thesis presented a detailed study HL7 FHIR and rationale behind this choice, then went into details about the structure of this protocol and its 'resources', and how they were adapted and functioned to convert the acquired data and send it to the main server. The implementation of FHIR has extended to link other semantic standards and proposed some methods to complement FHIR to offer implementation supports health interoperability between the parts of the system at the structural, syntactic and semantic levels.

On the other end of the project, the server receives the data, analyzes and decrypts it, the study covered theoretical and practical parts of building programming application interfaces APIs to obtain server software component which can receive and store healthcare data for later processing.

These concepts have been successfully implemented and tested, accordingly it can be considered that the work has provided a holistic view of the construction of an interoperable telemedicine system to collect vital signs via Bluetooth low energy and other standards from health monitoring devices and transmit it to the central aggregation server.

Although other studies have been presented in the context of Health interoperability, most have ignored the extension of the system to acquire healthcare data health monitoring devices. Besides, this work provides overview of the flow of healthcare data across different layers in software environments in smartphones and servers. This study still lacks the test on a large scale, to check the ability to withstand a large number of requests at one time and ensure the stability of the system. Additional works in future can be done to provide software for IOS phones and connect more monitoring devices, such as the blood glucose monitoring devices and portable ECGs.

The objectives set at the beginning of the work were achieved and ensured by the delivery of data from the Blood pressure monitoring device to the server. One of the physiological hypotheses was tested based on this data and carried out successfully.

7. Appendices

7.1 Health care BLE profiles

Health care, Sports and fitness and related services profiles:

- BLP (Blood Pressure Profile) — for blood pressure measurement.
- HTP (Health Thermometer Profile) — for medical temperature measurement devices.
- GLP (Glucose Profile) — for blood glucose monitors.
- CGMP (Continuous Glucose Monitor Profile)
- BCS (Body Composition Service)
- CSCP (Cycling Speed and Cadence Profile) — for sensors attached to a bicycle or exercise bike to measure cadence and wheel speed.
- CPP (Cycling Power Profile)
- HRP (Heart Rate Profile) — for devices which measure heart rate
- LNP (Location and Navigation Profile)
- RSCP (Running Speed and Cadence Profile)
- WSP (Weight Scale Profile)
- ESP (Environmental Sensing Profile)
- UDS (User Data Service)
- HOGP (HID over GATT Profile) allowing Bluetooth LE-enabled Wireless mice, keyboards and other devices offering long-lasting battery life.
- Proximity sensing
- FMP — the "find me" profile
- PXP — the proximity profile
- Alerts and time profiles
- Time profile
- The Battery Service

7.2 GATT health related services and characteristics UUID

List of GATT identified UUID for health propose [61]

Name	Assigned Number
Aerobic Heart Rate Lower Limit	0x2A7E
Aerobic Heart Rate Upper Limit	0x2A84
Aerobic Threshold	0x2A7F
Age	0x2A80
Alert Category ID	0x2A43
Alert Category ID Bit Mask	0x2A42
Alert Level	0x2A06
Alert Notification Control Point	0x2A44
Alert Status	0x2A3F
Anaerobic Heart Rate Lower Limit	0x2A81
Anaerobic Heart Rate Upper Limit	0x2A82
Anaerobic Threshold	0x2A83
Battery Level	0x2A19
Battery Level State	0x2A1B
Battery Power State	0x2A1A
Blood Pressure Feature	0x2A49
Blood Pressure Measurement	0x2A35
Body Composition Feature	0x2A9B
Body Composition Measurement	0x2A9C
Body Sensor Location	0x2A38
Current Time	0x2A2B
Cycling Power Control Point	0x2A66
Cycling Power Feature	0x2A65
Cycling Power Measurement	0x2A63
Cycling Power Vector	0x2A64
Date of Birth	0x2A85
Date Time	0x2A08
Day Date Time	0x2A0A
Day of Week	0x2A09
Descriptor Value Changed	0x2A7D
Device Name	0x2A00
Email Address	0x2A87
Fat Burn Heart Rate Lower Limit	0x2A88
Fat Burn Heart Rate Upper Limit	0x2A89
Firmware Revision String	0x2A26
First Name	0x2A8A
Fitness Machine Control Point	0x2AD9
Fitness Machine Feature	0x2ACC
Fitness Machine Status	0x2ADA
Five Zone Heart Rate Limits	0x2A8B
Gender	0x2A8C
Glucose Feature	0x2A51
Glucose Measurement	0x2A18
Glucose Measurement Context	0x2A34
Heart Rate Control Point	0x2A39
Heart Rate Max	0x2A8D
Heart Rate Measurement	0x2A37
Height	0x2A8E
Hip Circumference	0x2A8F
Indoor Bike Data	0x2AD2

Indoor Positioning Configuration	0x2AAD
Intermediate Cuff Pressure	0x2A36
Intermediate Temperature	0x2A1E
Language	0x2AA2
Last Name	0x2A90
Manufacturer Name String	0x2A29
Maximum Recommended Heart Rate	0x2A91
Measurement Interval	0x2A21
Model Number String	0x2A24
New Alert	0x2A46
Peripheral Preferred Connection Parameters	0x2A04
Peripheral Privacy Flag	0x2A02
Pollen Concentration	0x2A75
Position 2D	0x2A2F
Position 3D	0x2A30
Position Quality	0x2A69
Pressure	0x2A6D
Pulse Oximetry Control Point	0x2A62
Reconnection Address	0x2A03
Reconnection Configuration Control Point	0x2B1F
Record Access Control Point	0x2A52
Scientific Temperature Celsius	0x2A3C
Sensor Location	0x2A5D
Serial Number String	0x2A25
Service Changed	0x2A05
Service Required	0x2A3B
Software Revision String	0x2A28
Sport Type for Aerobic and Anaerobic Thresholds	0x2A93
System ID	0x2A23
Temperature	0x2A6E
Temperature Celsius	0x2A1F
Temperature Fahrenheit	0x2A20
Temperature Measurement	0x2A1C
Temperature Type	0x2A1D
Three Zone Heart Rate Limits	0x2A94
Time Accuracy	0x2A12
Time Broadcast	0x2A15
Time Source	0x2A13
Time Update Control Point	0x2A16
Time Update State	0x2A17
Time Zone	0x2A0E
Training Status	0x2AD3
UV Index	0x2A76
VO2 Max	0x2A96
Waist Circumference	0x2A97
Weight	0x2A98
Weight Measurement	0x2A9D
Weight Scale Feature	0x2A9E

7.3 Health monitoring device technical specification

Measurement principle	oscillometric
Measurement range	Systolic: 60 to 279 mmHg Diastolic: 40 to 200 mmHg Pulse: 40 to 180 per minute
Cuff pressure	0 to 299 mmHg
Memory store	30 measurements
Display	LCD
Operating conditions	environmental temperature +10°C to +40°C Relative humidity 15 to 85% Air pressure 800 hPa to 1060 hPa
Power supply	DC 6 V (4 x 1.5 V Mignon IEC LR 6 alkaline manganese batteries) Alternative special option: DC 6 V power supply unit, Order No. 410-7-150
Typical battery life	500 measurement cycles (Depending on inflation pressure and frequency of use).
Weight	250 g without batteries
Dimensions (WxHxD)	96 mm x 68 mm x 130 mm
Classification	Medical device with internal energy source (in battery operation) / class II (in power supply unit operation), continuous operation mode
Clinical test	Accuracy complies with the requirements of ISO 81060 Part 2
Bluetooth	Bluetooth Version 4.0
Maximum deviation of pressure measurement	± 3 mmHg or 2% of the reading
Maximum deviation of pulse rate display	± 5 %
Applicable standards	DIN EN ISO 80601-2-30 „Medical electrical equipment - Part 2-30: Particular requirements for the basic safety and essential performance of automated type non-invasive sphygmomanometers“.
Wireless Communication	VZ (MURATA Manufacturing Co. Ltd.) Bluetooth Ver.4.OLE BLP Frequency band: 2402-2480 MHz Maximum RF output power: 1.6dBM

7.4 Blood pressure device parsed output

VI. Generic Access (0x1800)
   - Device Name [R] (0x2A00)
   - Appearance [R] (0x2A01)
   - Peripheral Privacy Flag [R W] (0x2A02)
   - Reconnection Address [W] (0x2A03)
   - Peripheral Preferred Connection Parameters [R] (0x2A04)

- Generic Attribute (0x1801)
  - Service Changed [I] (0x2A05)
  - Client Characteristic Configuration (0x2902)

- Blood Pressure (0x1810)
  - Blood Pressure Measurement [I] (0x2A35)

- Client Characteristic Configuration (0x2902)
  - Blood Pressure Feature [R] (0x2A49)
  - Date Time [R W] (0x2A08)

- Device Information (0x180A)
  - Manufacturer Name String [R] (0x2A29)
  - Model Number String [R] (0x2A24)
  - Serial Number String [R] (0x2A25)
  - Hardware Revision String [R] (0x2A27)
  - Firmware Revision String [R] (0x2A26)
  - Software Revision String [R] (0x2A28)
  - System ID [R] (0x2A23)
  - IEEE 11073-20601 Regulatory Certification Data List [R] (0x2A2A)

- Battery Service (0x180F)
  - Battery Level [R] (0x2A19)

- Unknown Service (233bf000-5a34-1b6d-975c-000d5690abe4)
  - Unknown Characteristic [R W] (233bf001-5a34-1b6d-975c-000d5690abe4)

7.5 HL7 FHIR patient resource XML template

```xml
<Patient xmlns="http://hl7.org/fhir">
 <!-- from Resource: id, meta, implicitRules, and language -->
 <!-- from DomainResource: text, contained, extension, and modifierExtension -->
 <identifier><!-- 0..* Identifier An identifier for this patient --></identifier>
 <active value="[boolean]"/><!-- 0..1 Whether this patient's record is in active use -->
 <name><!-- 0..* HumanName A name associated with the patient --></name>
 <telecom><!-- 0..* ContactPoint A contact detail for the individual --></telecom>
 <gender value="[code]"/><!-- 0..1 male | female | other | unknown -->
 <birthDate value="[date]"/><!-- 0..1 The date of birth for the individual -->
 <deceased[x]><!-- 0..1 boolean|dateTime Indicates if the individual is deceased or not --></deceased[x]>
 <address><!-- 0..* Address Addresses for the individual --></address>
 <maritalStatus><!-- 0..1 CodeableConcept Marital (civil) status of a patient --></maritalStatus>
 <multipleBirth[x]><!-- 0..1 boolean|integer Whether patient is part of a multiple birth --></multipleBirth[x]>
 <photo><!-- 0..* Attachment Image of the patient --></photo>
 <contact>  <!-- 0..* A contact party (e.g. guardian, partner, friend) for the patient -->
  <relationship><!-- 0..* CodeableConcept The kind of relationship --></relationship>
  <name><!-- 0..1 HumanName A name associated with the contact person --></name>
  <telecom><!-- 0..* ContactPoint A contact detail for the person --></telecom>
  <address><!-- 0..1 Address Address for the contact person --></address>
  <gender value="[code]"/><!-- 0..1 male | female | other | unknown -->
  <organization><!--  0..1 Reference(Organization) Organization that is associated with the contact --></organization>
  <period><!-- 0..1 Period The period during which this contact person or organization is valid to be contacted relating to this patient --></period>
 </contact>
 <animal>  <!-- 0..1 This patient is known to be an animal (non-human) -->
  <species><!-- 1..1 CodeableConcept E.g. Dog, Cow --></species>
  <breed><!-- 0..1 CodeableConcept E.g. Poodle, Angus --></breed>
  <genderStatus><!-- 0..1 CodeableConcept E.g. Neutered, Intact --></genderStatus>
 </animal>
 <communication>  <!-- 0..* A list of Languages which may be used to communicate with the patient about his or her health -->
  <language><!-- 1..1 CodeableConcept The language which can be used to communicate with the patient about his or her health --></language>
  <preferred value="[boolean]"/><!-- 0..1 Language preference indicator -->
 </communication>
 <generalPractitioner><!-- 0..* Reference(Organization|Practitioner) Patient's nominated primary care provider --></generalPractitioner>
 <managingOrganization><!-- 0..1 Reference(Organization) Organization that is the custodian of the patient record --></managingOrganization>
 <link>  <!-- 0..* Link to another patient resource that concerns the same actual person -->
  <other><!-- 1..1 Reference(Patient|RelatedPerson) The other patient or related person resource that the link refers to --></other>
  <type value="[code]"/><!-- 1..1 replaced-by | replaces | refer | seealso - type of link -->
 </link>
</Patient>
```

7.6 HL7 FHIR Observation resource XML template

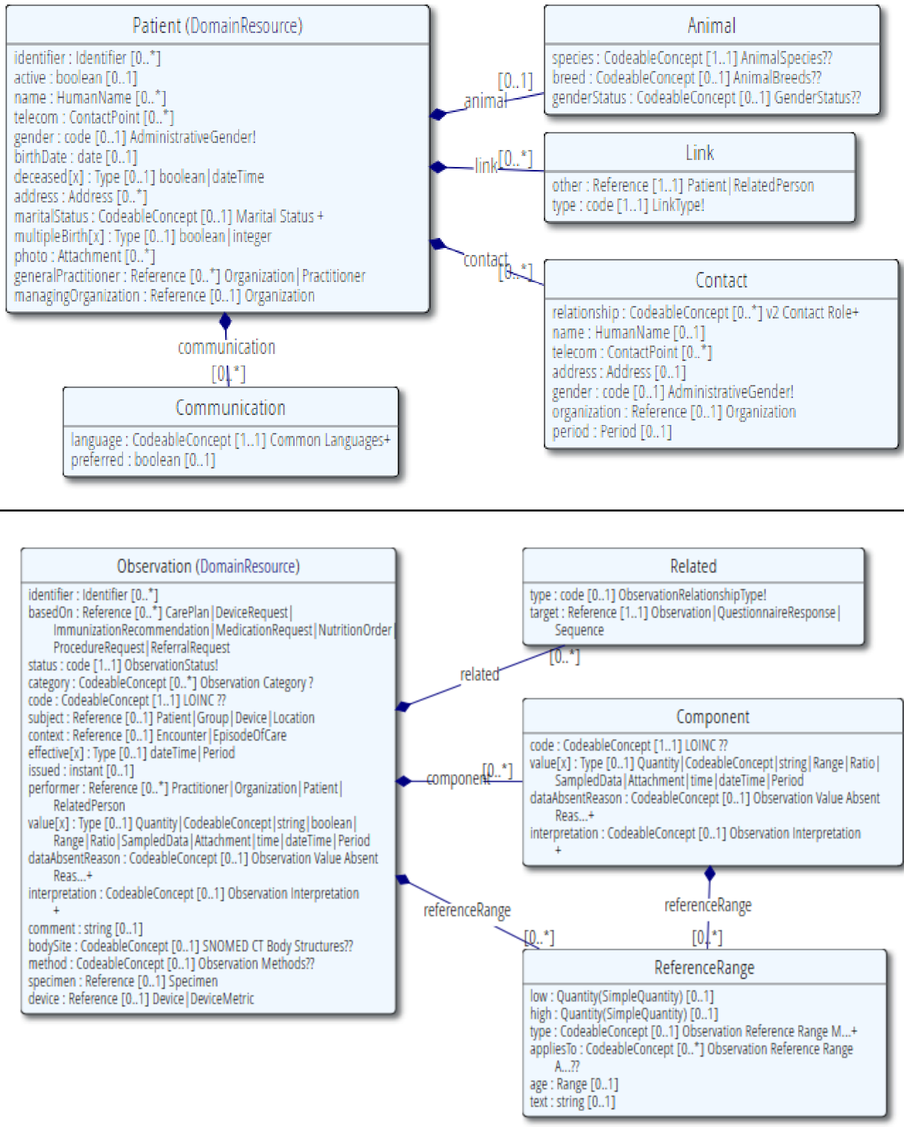
```
<Observation xmlns="http://hl7.org/fhir">
 <!-- from Resource: id, meta, implicitRules, and language -->
 <!-- from DomainResource: text, contained, extension, and modifierExtension -->
 <identifier><!-- 0..* Identifier Business Identifier for observation --></identifier>
 <basedOn><!-- 0..* Reference(CarePlan|DeviceRequest|ImmunizationRecommendation|
   MedicationRequest|NutritionOrder|ProcedureRequest|ReferralRequest) Fulfills plan, proposal or order --
></basedOn>
 <status value="[code]"/><!-- 1..1 registered | preliminary | final | amended + -->
 <category><!-- 0..* CodeableConcept Classification of  type of observation --></category>
 <code><!-- 1..1 CodeableConcept Type of observation (code / type) --></code>
 <subject><!-- 0..1 Reference(Patient|Group|Device|Location) Who and/or what this is about --></subject>
 <context><!-- 0..1 Reference(Encounter|EpisodeOfCare) Healthcare event during which this observation is
 made --></context>
 <effective[x]><!-- 0..1 dateTime|Period Clinically relevant time/time-period for observation --></effect
ive[x]>
 <issued value="[instant]"/><!-- 0..1 Date/Time this was made available -->
 <performer><!-- 0..* Reference(Practitioner|Organization|Patient|RelatedPerson) Who is responsible for t
he observation --></performer>
 <value[x]><!--  0..1 Quantity|CodeableConcept|string|boolean|Range|Ratio|
   SampledData|Attachment|time|dateTime|Period Actual result --></value[x]>
 <dataAbsentReason><!--  0..1 CodeableConcept Why the result is missing --></dataAbsentReason>
 <interpretation><!-- 0..1 CodeableConcept High, low, normal, etc. --></interpretation>
 <comment value="[string]"/><!-- 0..1 Comments about result -->
 <bodySite><!-- 0..1 CodeableConcept Observed body part --></bodySite>
 <method><!-- 0..1 CodeableConcept How it was done --></method>
 <specimen><!-- 0..1 Reference(Specimen) Specimen used for this observation --></specimen>
 <device><!-- 0..1 Reference(Device|DeviceMetric) (Measurement) Device --></device>
 <referenceRange>  <!-- 0..* Provides guide for interpretation -->
  <low><!--  0..1 Quantity(SimpleQuantity) Low Range, if relevant --></low>
  <high><!--  0..1 Quantity(SimpleQuantity) High Range, if relevant --></high>
  <type><!-- 0..1 CodeableConcept Reference range qualifier --></type>
  <appliesTo><!-- 0..* CodeableConcept Reference range population --></appliesTo>
  <age><!-- 0..1 Range Applicable age range, if relevant --></age>
  <text value="[string]"/><!-- 0..1 Text based reference range in an observation -->
 </referenceRange>
 <related>  <!-- 0..* Resource related to this observation -->
  <type value="[code]"/><!-- 0..1 has-member | derived-from | sequel-to | replaces | qualified-by | inter
fered-by -->
  <target><!-- 1..1 Reference(Observation|QuestionnaireResponse|Sequence) Resource that is related to thi
s one --></target>
 </related>
 <component>  <!-- 0..* Component results -->
  <code><!-- 1..1 CodeableConcept Type of component observation (code / type) --></code>
  <value[x]><!-- 0..1 Quantity|CodeableConcept|string|Range|Ratio|SampledData|
    Attachment|time|dateTime|Period Actual component result --></value[x]>
  <dataAbsentReason><!--  0..1 CodeableConcept Why the component result is missing --></dataAbsentReas
on>
  <interpretation><!-- 0..1 CodeableConcept High, low, normal, etc. --></interpretation>
  <referenceRange><!-- 0..* Content as for Observation.referenceRange Provides guide for interpretation o
f component result --></referenceRange>
 </component>
</Observation>
```

7.7 HL7 FHIR DiagnosticReport resource structure

Structure

Name	Flags	Card.	Type	Description & Constraints
DiagnosticReport			DomainResource	A Diagnostic report - a combination of request information, atomic results, images, interpretation, as well as formatted reports Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
identifier	Σ	0..*	Identifier	Business identifier for report
basedOn		0..*	Reference(CarePlan | ImmunizationRecommendation | MedicationRequest | NutritionOrder | ProcedureRequest | ReferralRequest)	What was requested
status	?! Σ	1..1	code	registered | partial | preliminary | final + DiagnosticReportStatus (Required)
category	Σ	0..1	CodeableConcept	Service category Diagnostic Service Section Codes (Example)
code	Σ	1..1	CodeableConcept	Name/Code for this diagnostic report LOINC Diagnostic Report Codes (Preferred)
subject	Σ	0..1	Reference(Patient | Group | Device | Location)	The subject of the report - usually, but not always, the patient
context	Σ	0..1	Reference(Encounter | EpisodeOfCare)	Health care event when test ordered
effective[x]	Σ	0..1		Clinically relevant time/time-period for report
effectiveDateTime			dateTime	
effectivePeriod			Period	
issued	Σ	0..1	instant	DateTime this version was released
performer	Σ	0..*	BackboneElement	Participants in producing the report
role	Σ	0..1	CodeableConcept	Type of performer Procedure Performer Role Codes (Example)
actor	Σ	1..1	Reference(Practitioner | Organization)	Practitioner or Organization participant
specimen		0..*	Reference(Specimen)	Specimens this report is based on
result		0..*	Reference(Observation)	Observations - simple, or complex nested groups
imagingStudy		0..*	Reference(ImagingStudy | ImagingManifest)	Reference to full details of imaging associated with the diagnostic report
image	Σ	0..*	BackboneElement	Key images associated with this report
comment		0..1	string	Comment about the image (e.g. explanation)
link	Σ	1..1	Reference(Media)	Reference to the image source
conclusion		0..1	string	Clinical Interpretation of test results
codedDiagnosis		0..*	CodeableConcept	Codes for the conclusion SNOMED CT Clinical Findings (Example)
presentedForm		0..*	Attachment	Entire report as issued

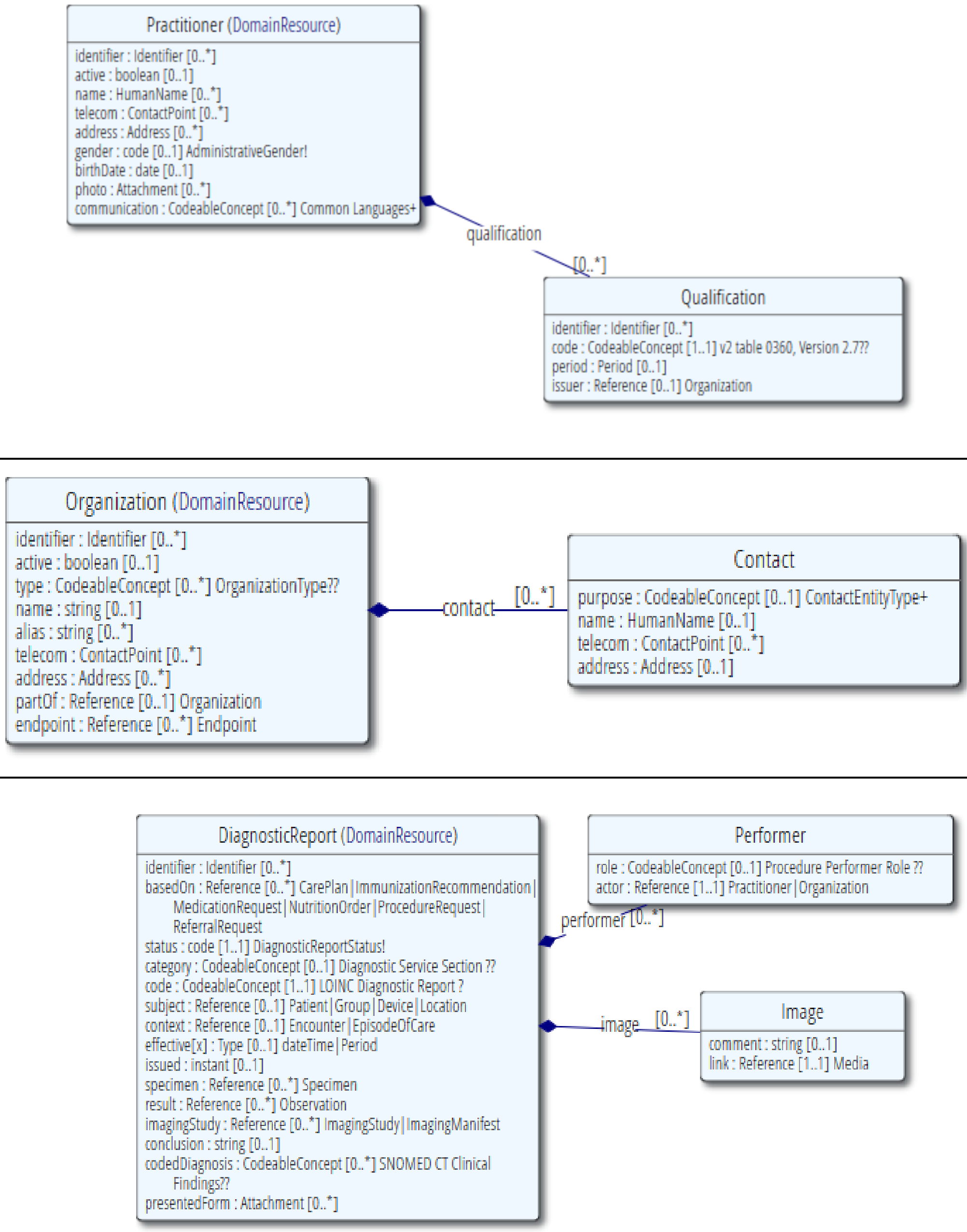
7.8 HL7 FHIR Patient, Observation resources UMLs



UML diagrams Top) FHIR Patient Resource [14] shows all characteristics in addition to links to other resources. Patient Resource is used to store participants' information, Bottom) FHIR Observation Resource[15], this resource is used to transmit blood pressure values from smartphone to the server

[14] https://www.hl7.org/fhir/patient.html
[15] https://www.hl7.org/fhir/observation.html

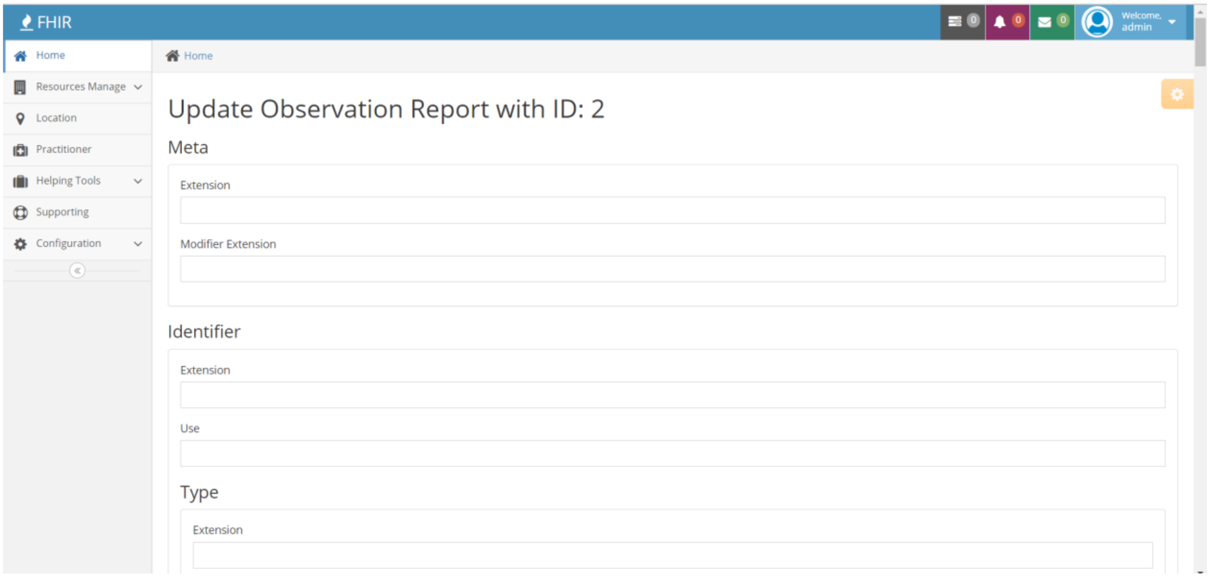
7.9 HL7 FHIR Practitioner, Organization and DiagnosticReport resources UMLs

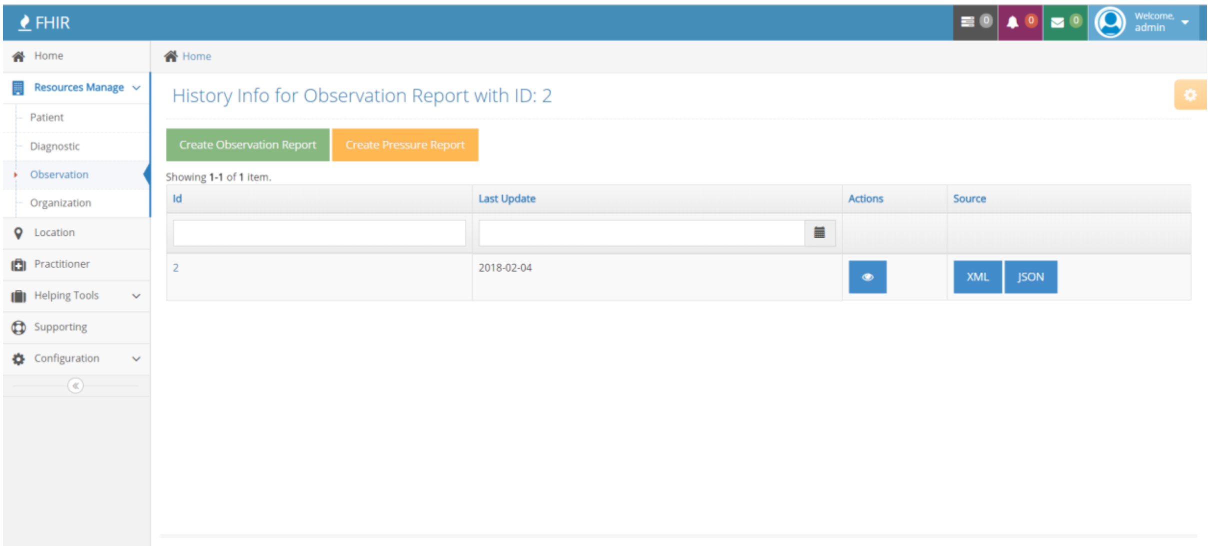


***Top**) practitioner[16], **Middle**) organization[17], **Bottom**) diagnostic report[18]*

[16] https://www.hl7.org/fhir/practitioner.html
[17] https://www.hl7.org/fhir/organization.html
[18] https://www.hl7.org/fhir/diagnosticreport.html

7.10 User interface for observation update and history





Top) backend UI for observation update, in this page admins can edit resources, athough the change will take place, but the records retains the old values for reference, Bottom) backend UI for observation resources history, in which admin can see any modification that happens on certain resource even if the resource is deleted.

8. Bibliography

[1] U. Nations, "World Population Ageing 2017 Highlights," Department of Economic and Social Affairs, New York, 2017.

[2] S. A. Tabish, "Lifestyle diseases: consequences, characteristics, causes and control," *Journal of Cardiology & Current Research,* 2017.

[3] S. AUSTRIA, "Chronische Krankheiten und Gesundheitsprobleme 2014," STATISTICS AUSTRIA Federal Statistical Office, Vienna , 2014.

[4] T. A. T. Association, "Telemedicine, Telehealth, and Health Information Technology, an ATA Issue Paper," The American Telemedicine Association , 2006.

[5] WHO, "TELEMEDICINE Opportunities and developments in Member States," World Health Organization, Geneva, Switzerland, 2010.

[6] B. W. A. B. Amber K. Sabbatini, "The cost of observation care for commercially insured patients visiting the emergency department.," *The American journal of emergency medicine.,* 2018.

[7] M. M. Hofmarcher, "Austria Health system review," The European Observatory on Health Systems and Policies, 2013.

[8] G. W. Beeler, "HL7 Basic Overview," HIMSS, 2015.

[9] IBM, "IBM X-Force® Research 2016 Cyber Security Intelligence Index," IBM , 2016.

[10] U. GE Healthcare, "Big Data, Analytics & Artificial Intelligence," General Electric Company, San Francisco, California, 2016 .

[11] D. B. Neill, "Using Artificial Intelligence to Improve Hospital Inpatient Care," *IEEE Intelligent Systems,* pp. 92 - 95, 2013 .

[12] E. Strickland, "AI Predicts Heart Attacks and Strokes More Accurately Than Standard Doctor's Method," *IEEE Spectrum's biomedical engineering blog,* 2017.

[13] M. U. o. Vienna, "Data Interface Dex / App Info," Medical University of Vienna, Vienna, 2016.

[14] M. Alakraa, *Development of an Interoperable Exchange, Aggregation and Analysis Platform for Health and Environmental Data,* Vienna: Fachhochschule Technikum Wien, 2017.

[15] IEEE, "610-1990 - IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries," no. IEEE, 1991.

[16] HIMSS, HIMSS Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations, vol. 3rd, Chicago, IL: HIMSS, 2013.

[17] J. Sensmeier, "HIMSS dictionary of healthcare information technology terms , acronyms , and organizations Statement of Responsibility : foreword by Joyce Sensmeier," no. Fourth edition. , 2017.

[18] U. N. L. o. Medicine, "Fact Sheet Unified Medical Language System," [Online]. Available: https://www.nlm.nih.gov/pubs/factsheets/umls.html. [Accessed 16 3 2018].

[19] U. N. L. o. Medicine, "U.S. National Library of Medicine," U.S. National Library of Medicine MeSH, [Online]. Available: https://www.nlm.nih.gov/mesh/meshhome.html. [Accessed 16 3 2018].

[20] T. N. O. B. Lee Peters, "Terminology Status APIs - Mapping Obsolete Codes to Current RxNorm, SNOMED CT, and LOINC Concepts.," *Studies in Health Technology and Informatics,* vol. 245, 2017.

[21] L. A. Robert H Dolin, "Approaching semantic interoperability in Health Level Seven," *The National Center for Biotechnology Information NCBI,* pp. 99-103, 2011.

[22] D. Collins, Creating a quality assurance program for long-term care., LTCS Books , 2016.

[23] O. W. Inc, "Bluetooth Low Energy IoT: A Market Dynamics Report," ON World Inc, September 2017.

[24] I. STANDARD, "802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," IEEE STANDARD.

[25] H.-B. L. R. K. C. Li, "Performance Evaluation of IEEE 802.15.4 for Wireless Body Area Network (WBAN)," *IEEE International Conference on Communications Workshops,* 2009.

[26] S. Movassaghi, M. Abolhasan, J. Lipman and D. Smith, "Wireless Body Area Networks: A Survey," in *IEEE Communications Surveys and Tutorials. IEEE*, 2014.

[27] FDA, "Batteries in Medical Devices - Technologies, Use and Maintenance," U.S. Department of Health and Human Services, 2014.

[28] E. T. W. Z. H. C. E. M. W. H. R. P. I. C. Xenofon Fafoutis, "BLE or IEEE 802.15.4: Which Home IoT Communication Solution is more Energy-Efficient?," *Research Gate,* May 2016.

[29] B. (c), "Master Table of content & compliance, BLUETOOTH SPECIFICATION Version 4.0 [Vol 0]," 30 June 2010. [Online]. Available: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737. [Accessed 13 May 2017].

[30] P.-G. Dharma, A. R. Pratama and A. Lazovik, “Building, Comparison of energy consumption in Wi-Fi and bluetooth communication in a Smart,” *Computing and Communication Workshop and Conference (CCWC), IEEE,* vol. 7th Annual, 2017.

[31] B. g. s. interest, "BLUETOOTH ® 4.1 FREQUENTLY ASKED QUESTIONS," Blutooth group speical interest, 2013.

[32] i. s. association, "INTERNET OF THINGS RELATED STANDARDS," [Online]. Available: http://standards.ieee.org/innovate/iot/stds.html.

[33] A. Inc., "iOS Device Compatibility Reference," 2017. [Online]. Available: https://developer.apple.com/library/content/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/DeviceCompatibilityMatrix/DeviceCompatibilityMatrix.html.

[34] S. D. ,. T. V. PrithviRaj Narendra, "BLE and IEEE 802.15.4 in the IoT: Evaluation and Interoperability Considerations," SICS Swedish ICT, Uppsala University Sweden, 2016.

[35] J. T. N. P. Konstantin Mikhaylov, "Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI," *Journal of Sensor and Actuator Networks,* 2013.

[36] JoakimLindh, "Bluetooth® low energy Beacons, Application Report," Texas Instruments Incorporated, Dallas, Texas, 2016.

[37] T. I. inc., Texas Instruments CC2540/41 Bluetooth® Low Energy Sample Applications Guide v1.3.1, Texas Instruments inc., 2012-2013.

[38] Aislelabs, "The Hitchhikers Guide to iBeacon Hardware: A Comprehensive Report by Aislelabs (2015)," Aislelabs, 4 May 2015. [Online]. Available: http://www.aislelabs.com/reports/beacon-guide/. [Accessed 12 May 2017].

[39] B. SIG, "Security, Bluetooth Low Energy," [Online]. Available: https://www.bluetooth.com/~/media/files/specification/bluetooth-low-energy-security.ashx?la=en. [Accessed 11 May 2017].

[40] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD, 2004.

[41] J. Schang, "Enabling secure portable medical devices with TI's MSP430 ™MCU and wireless technologies," Texas Instruments Incorporated , Dallas, Texas, 2013.

[42] D. R. L. Brown, "Standards for Efficient Cryptography SEC 1: Elliptic Curve Cryptography," Certicom Corp, 2009.

[43] K. S. L. C. John Padgette, "Guide to Bluetooth Security, Recommendations of the National Institute of Standards and Technology," Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD, 2017.

[44] H. orgnization, "HEALTH LEVEL SEVEN® INTERNATIONAL The Worldwide Leader in Interoperability Standards," [Online]. Available: https://www.hl7.org/documentcenter/public_temp_A1B27B76-1C23-BA17-0C9A85E34211D8ED/calendarofevents/himss/2011/HL7%20Organizational%20Backgrounder%20and%20Standards%20Descriptions.pdf. [Accessed 15 3 2018].

[45] HL7, "What is the CDA?," 2010. [Online]. Available: https://www.hl7.org/documentcenter/public_temp_A07215E2-1C23-BA17-0C761334D1C45D52/calendarofevents/himss/2010/presentations/HIMSS2010%20cda.pdf.

[46] H. Deutschland, "HL7 RIM – das Referenzinformationsmodell," [Online]. Available: http://hl7.de/themen/hl7-v3-rim-das-referenzinformationsmodell/. [Accessed 15 11 2017].

[47] R. S. Frank Oemig, Healthcare Interoperability Standards Compliance Handbook: Conformance and Testing of Healthcare Data Exchange Standards, Springer, 2016.

[48] N. Digital, "The Interoperability Toolkit," NHS Digital, 2018. [Online]. Available: https://digital.nhs.uk/interoperability-toolkit.

[49] N. K. O. Y. F. N. N. N. J. H. N. T. S. T. S. M. S. F. F. T. N. T. T. K. H. H. S. T. N. Y. K. K. W. H. T. S. Kimura M, "SS-MIX: a ministry project to promote standardized healthcare information exchange.," *Methods of Information,* 2011.

[50] R. T. Fielding, "Network-based Application Architectures," UNIVERSITY OF CALIFORNIA, IRVINE, CALIFORNIA, IRVINE, 2000.

[51] M. K. B. M. Mustafa Canim, "Secure Management of Biomedical Data With Cryptographic Hardware," *IEEE Trans Inf Technol Biomed,* vol. 16, no. 1, pp. 166 - 175, 2011.

[52] P. M. ,. M. H. L. J. S. D. K. P. R. Arnon Rosenthal, "Cloud computing: A new business paradigm for biomedical information sharing," *Journal of Biomedical Informatics,* vol. 43, p. 342–353, 2010.

[53] F. Thürk and E. Kaniusas, "Physiological unbalance during dry static apneas: Effects of preceding preparations," in *Medical Measurements and Applications Proceedings (MeMeA), 2013 IEEE International Symposium on*, 2013.

[54] N. D. X. Z. N. W. B. S. R. Z. X. X. Z. W. Y. G. Z. H. H. M. Jing Xu, "Nocturnal blood pressure fluctuation and associated influential factors in severe obstructive sleep apnea patients with hypertension.," *Sleep Breath,US National Library of Medicine National Institutes of Health,* 2018.

[55] N. K. a. U. D. I. Clearinghouse, "High Blood Pressure and Kidney Disease," National Kidney and Urologic Diseases Information Clearinghouse, 2014.

[56] P. v. d. B. P. L. a. E. V. C. Jean-Paul Degaute, "Quantitative analysis of the 24-hour blood pressure and heart rate patterns in young men.," *Hypertension,* Vols. 18-2, pp. 199-210, 1991 .

[57] D. B. ,. Y. Z. ,. M. Z. ,. C. E. ,. R. A. Sebastián Lluberas a, "Sleep-Wakefulness Variations in Arterial Stiffness: Assessment Using Ambulatory Recording of Arterial Pulse Transit Time," *Rev Esp Cardiol.,* vol. 61, 2008.

[58] Y. Kawano, "Diurnal blood pressure variation and related," *Hypertension Research,* vol. 34, p. 281–285, 2011.

[59] D. G. S. C. M. M. T. K. D. M. J. L. S. A. L. U. F. M. P. K. Yue Jiao, "Development and testing of prediction models for end stage kidney disease patient nonadherence to renal replacement treatment regimens utilizing big data and healthcare informatics," *Bioinformatics and Biomedicine (BIBM), 2015 IEEE International Conference on,* 2015.

[60] K. H. J. L. R.-Á. S. O. S. F. G. K. M. A. R. R.-O. L. K. M. A. R. J. Cristina Soguero-Ruiz, " Support Vector Feature Selection for Early Detection of Anastomosis Leakage From Bag-of-Words in Electronic Health Records," *IEEE Journal of Biomedical and Health Informatics ,* vol. 20, no. 5, pp. 1404 - 1415, 2016.

[61] B. SIG, "GATT Characteristics," Bluetooth SIG, [Online]. Available: https://www.bluetooth.com/specifications/gatt/characteristics. [Accessed 15 3 2018].

List of Figures

Figure 1 Structure of the project shows vital data acquisition and the transmission to smartphone and the server, also shows big data resource collection and analysis platform [reformed from original project picture] 13
Figure 2 Compatibility focuses on small number of entities, in contrast inoperability provides communications between all entities. Health information systems nowadays are seeking the transition from compatibility to interoperability. 15
Figure 3 Interoperability pyramid layers: foundational layer at the base assure the basics for mutual technical ground, structural & syntactic layer at the middle provide the same content structure and syntax and semantic layer at the tope to assure correct understanding of the meanings 16
Figure 4 Semantic interoperability of blood pressure and heart rate measurements, using SNOMED CT and LOINC. Site of acquisition is determined according to SNOMED CT at the right arm, while vital value and category of the measurements provided according to LONIC, these values can be integrated later with structural level of health interoperability to offer full interoperability implementation. 17
Figure 5 Proposed data representation and transmission model design. Basic information at the core followed by other complementary layers, some layer designed for security and privacy protection. 18
Figure 6 shows A) communication interfaces of different systems, provide the ability of interoperability, B) communication interface layers, where information are transferred from non-interoperable systems below to other inoperable systems on the top 19
Figure 7 A) Transfer data from health monitor device to smartphone using Bluetooth Low Energy, b) BLE hub concept for medical purposes, where sensors wireless tranmissters form network of connections 21
Figure 8 Left) Energy consumption measurement result with 100 and 200 of beacons data for both BLE (a) and Wi-Fi (b) [30], Right) BLE vs. IEEE 802.15.4 data rate Kbit/s [34], both charts shows the superiority of Bluetooth low energy. 22
Figure 9 Bluetooth Low Energy architecture showing physical and virtual layers, image adapted from [35], smartphone application development deals usually with tope three layers: Apps, GAP and GATT. 23
Figure 10 Connection types based on GAP configuration. Left) Broadcasting: where there is or broadcaster and one or more observer. Right) Connection: one central and one peripheral [36]. The case on right is usually used in health care where device has Peripheral role to send data to the device has Central role which could be Computer, Smartphone or other. 24
Figure 11 BLE GATT structure. Each profile contains characteristics which is used to store information, different profiles could have links to each other, this is can be used to transmit healthcare data as predefined segments called “BLE healthcare and fitness profiles” 25
Figure 12 GAP and GATT BLE profiles and services in “Boso Medicus” blood pressure device output to the smartphone. Blood pressure measurements are shown in Blood pressure profile (0x1810), while other profiles transfer other kinds of data such as battery level, times of measurements and device manufacturing information 27
Figure 13 Blood pressure profile (BLP) consists of segments, each segment has its own interpretation. From left: Flags used to determine the unit of the measurements (Kpa or mmHG) and to determine which of next segments has values or empty, Blood Pressure Measurement Value is used to pass the value of Systolic, Diastolic and mean arterial pressure, Time Stamp used to pass time of the measurements, Pulse Rate used to pass heart rate and User ID can be used to assign ID for specific user or can be empty. This segments has redundant sequences can be used for future updates, this helps to provide backward compatibility of BLP. 28

Figure 14 The Android software stack, shows basic OS layers, API layers and software development layer. Any application should cross different layers in order use smartphone hardware resources... 29
Figure 15 Top) Information flow from health monitoring device to user interface throw smartphone application, shows GATT and BLP programming classes which have been developed to extract values from GATT and BLP profiles, Bottom) Systolic, Diastolic and mean blood pressure parsing using Java during Android App development, code shows how UUIDs are used to determine BLP profile and other service 30
Figure 16 A) Health monitoring device location estimation using 2 smartphones and one PC located differently in the space which violate users' privacy, B) Establish new "pairing" process is the first step to intercept communication between already connected devices, this is used in Man in the middle attack. 32
Figure 17 Overview of the various standards developed by HL7 [14], among them version 2x is the most ubiquitous one [8]. FHIR the most recent and still in development stages. 34
Figure 18 HL7 v3 HL7 Reference Information Model (RIM) [46], shows the interaction between parts of the concept where **Entity** can represent organization or person such as doctor or hospital, **participation** describes the involvement of an entity in an act such as diagnostic exam performer , **Role** and **Role Relationship** define who can play certain roles to apply actions in the system, **Act and Act Relationship** determine the type of the action that entities can play such as diagnostic report.. 34
Figure 19 A) Description of HL7 version 2.xx structure. Segments are separated by delimiter and composite delimiter used to form sub segments which contains the values, B) Standard schema for Clinical Document Architecture template contains all mandatory header attributes 35
Figure 20 Top) FHIR standard resource parts. Each resource has its own data (Standard Data), identity and metadata. Also it could have human readable part and reference to other resources , Bottom) FHIR Resource DiagnosticReport UML diagram. DiagnosticReport resource contains set of information that is provided by a diagnostic service when medical investigations are finished. It has the ability to integrate SNOMED CT and LONIC to offer the semantic interoperability of the clinical finding. Also it has relation with Performer and Image Resources. 37
Figure 21 FHIR resources layers and sub groups, this method of grouping has adapted by FHIR committee based on common sense groupings or patterns describing expected structures and/or behaviors amongst resources in the same category 38
Figure 22 Example of DiagnosticReport FHIR resource in XML format for abdominal ultrasound report, contains human readable part at the top as HTML form, Patient resource reference and other metadata. Ultrasound image is linked through reference to Image resource. 39
Figure 23 Tools which are proposed to build Application based on health interoperability FHIR standard in Android smartphones. Hapi FHIR libraries are integrated in Android Java libraries to implement HL7 FHIR, then all used to provide secure API using RESTful architecture and secure socket layer encryption........ 41
Figure 24 Top) Part of creating FHIR observation resource code using Java in Android, shows the assignment of Systolic and Diastolic blood pressure values, in addition to add LOINC Systolic and Diastolic pressure codes to ensure semantic interoperability, B) Parsing FHIR observation resource in Android using Java, shows how application check part of security measures be checking request token to determine if the request will parsed or ignored 42
Figure 25 A) create new account dataflow in smartphone application, shows two data models are formed: Normal data model and FHIR patient resource, B) convert BLP data which had been acquired from Blood pressure monitoring device, to observation FHIR resource and send it via smartphone application and sent it to the server, C) retrieve previous user observations and display them in smartphone application 43

Figure 26 Smartphone application user interfaces, A) application log in page, B) C) user registration page, D) support users interface in the application 44
Figure 27 Smartphone application user interfaces: A) update user profile page, B) user menu items, C) home page 44
Figure 28 Smartphone application user interfaces: A) view previous observations, B) health monitoring device page before acquisition, C) health monitoring device page after acquisition 44
Figure 29 implementation approach of server API & backend. HL7 FHIR, Yii2 web framework, SSL and RESTful concept have been used to deliver this approach 45
Figure 30 Screenshot of the backend shows patients resources management interface. Authorized system users can view, add, update, remove and browse patient resource history. The system also offers XML and JSON formats for exporting. "Full Report" button provide general view for all resources related to certain patient resource. 46
Figure 31 Secure Sockets Layer connection procedures. Starts from top when client starts Handshaking, then exchange certificates, and then verified connection can be established, all connection of the system went through secure socket layer 47
Figure 32 FHIR systems security cases for authentication and access control, first one left is recommended since all connections cross through security layer, to check security and users control level 49
Figure 33 A) Create/Edit a resource record using Yii2 libraries, this starts with FHIR request from the smartphone or other parts, then pass to Controller which interact with FHIR libraries to parse the request, which become normal Yii data model. After that it passes through database controller then it will be validated and sent to FHIR database system, B) View resource using Yii2 libraries, this starts when FHIR database system sends FHIR resource, it passes database Controller and parsed to become normal Yii2 data model to pass then Yii controller and after that it becomes FHIR response C) parsing XML FHIR resource using Dcarbone and Yii2 in server API 51
Figure 34 MySQL database Entity–relationship model which integrate Yii2 users model with FHIR patient resource through "user_fhir_account" table in the project. The ID of the patient resource is stored in this table and using this Yii active records model we can build relation that allows to call patient resource classes and functions directly from user classes, the programming result will be one object represent Yii user and FHIR patient 52
Figure 35 A) Create/update FHIR resources data flow from smartphone to the server though developed FHIR API. Validation is part of the process B) Request and retrieve FHIR resources from FHIR server through developed FHIR API 54
Figure 36 Top) Part of Backend UI for observations management, Authorized system users can view, add, update, remove and browse history of observation resources. The system also offers XML and JSON formats for exporting. Searching among observation is included also, Bottom) Part of backend UI to create observations, this form can be used by doctors to enter the values directly in the system, and this interface contains all possible required field to generate FHIR observation resources. 55
Figure 37 Top) Part of UI for observation resource view. This page is used to view any retrieved observation resource, providing detailed information and Meta data and references. The image shows the values of Systolic, Diastolic blood pressure and heart rate which has been acquired from health monitoring, Bottom) User interface to visualize blood pressure and heart rate values which have been stored in the server, these values has been acquired from health monitoring device and transmitted according to FHIR. 56
Figure 38 Right) Cuff position during blood pressure measurement, correct measurement should be taken two cm above the elbow, Left) health monitoring device output after measurement showing systolic and diastolic pressure values. 59

Figure 39 A) Box plots of whole participants groups for systolic and diastolic blood pressure showing clear distinct between means of the morning and evening measurements, The statistical differences between the bars are indicated by asterisks “*” based on paired samples t-test with 0,95 confidence interval, B) Box plot of each participant for Systolic and diastolic blood pressure in the morning and evening. Each participant has different blood pressure difference between morning and evening...61