International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# FG M2M

D1.1 – Version 1.0
(04/2014)

ITU-T Focus Group on M2M Service Layer

## M2M use cases: e-health

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. The ITU-T Focus Group on the M2M service layer (FG M2M) was established further to ITU-T TSAG agreement at its meeting in Geneva, 10-13 January 2012. ITU-T Study Group 11 is the parent group of FG M2M.

Deliverables of focus groups can take the form of technical reports, specifications, etc. and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

## SERIES OF FG M2M TECHNICAL REPORTS

Deliverable 0.1: M2M standardization activities and gap analysis: e-health

Deliverable 0.2: M2M enabled ecosystems: e-health

**Deliverable 1.1: M2M use cases: e-health**

Deliverable 2.1: M2M service layer: requirements and architectural framework

Deliverable 3.1: M2M service layer: APIs and protocols overview

*Attachments:*

- Spreadsheet on survey results on e-health M2M use cases (D11att1.xlsx)

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

# Deliverable D1.1 "M2M use cases: e-health"

## CONTENTS


1 Scope ..... 5

2 References ..... 5

3 Definitions ..... 5

3.1 Terms defined elsewhere ..... 5

3.2 Terms defined in this document ..... 5

4 Abbreviations and acronyms ..... 5

5 Conventions ..... 6

6 Summary of use cases ..... 7

7 Detailed use cases ..... 8

7.1 Remote patient monitoring/assisted living ..... 8

7.1.1 Legacy mass medical examination ..... 8

7.1.2 Travelling mass medical examination with BAN ..... 12

7.1.3 Remote patient monitoring ..... 17

7.1.4 Telehealth Counseling System ..... 19

7.1.5 Telehealth management system using NFC e-health device and smart phone ..... 22

7.1.6 Telehealth system for home care support ..... 25

7.1.7 Ambient Assisted Living (AAL) ..... 28

7.1.8 Easy Clinic ..... 34

7.2 Other use cases ..... 36

7.2.1 Personal healthcare data management ..... 36

Annex A: Contributed use cases outside the scope of the FG M2M ..... 39

A.1 Individual electronic health information: Electronic Health Record (EHR) ..... 39

A.1.1 Expert system for medical information/applications sharing ..... 39

Appendix I: Results of a survey to identify use cases of e-health services with M2M ..... 43

Bibliography ..... 44

# M2M use cases: e-health

## 1 Scope

The main objective of this deliverable is to describe use cases of e-health applications and services involving the usage of M2M technologies.

Annex A contains some contributed use cases outside of the scope of the FG M2M (that is, these uses cases do not necessarily involve the usage of M2M technologies).

## 2 References

[ITU-T FG M2M D0.2] ITU-T FG M2M Deliverable D0.2 “M2M enabled ecosystems: e-health”

NOTE - References for use cases on e-health are available in the Bibliography of this deliverable.

## 3 Definitions

### 3.1 Terms defined elsewhere

NOTE- Some definitions of terms used in this deliverable can be found in clause 3 of the D0.2 deliverable [ITU-T FG M2M D0.2]: e-health, EHR, PHR, m-health, Telehealth, Telemedicine, Remote patient monitoring/assisted living.

### 3.2 Terms defined in this document

None

## 4 Abbreviations and acronyms

This Deliverable uses the following abbreviations and acronyms:

| | |
|---|---|
| AAL | Ambient Assisted Living |
| API | Application Programming Interface |
| ACCP | Advanced Care Coordination Platform |
| BAN | Body Area Network |
| ECG | Electrocardiogram |
| EHR | Electronic Health Record |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications |
| HIS | Hospital Information System |
| IC | Integrated Circuit |
| ICT | Information and Communication Technology |
| ID | Identifier |
| ISDN | Integrated Services Digital Network |

| | |
|---|---|
| ITS | Intelligent Transport Systems |
| LAN | Local Area Network |
| LTE | Long Term Evolution |
| MVNO | Mobile Virtual Network Operator |
| NFC | Near-field Communication |
| NGN | Next Generation Network |
| PC | Personal Computer |
| PHR | Personal Health Record |
| PSTN | Public Switched Telephone Network |
| RFID | Radio Frequency IDentification |
| RPM | Remote Patient Monitoring |
| SOAP | Simple Object Access Protocol |
| SpO2 | Saturation of Peripheral Oxygen |
| WAN | Wide Area Network |
| WiMax | Worldwide Interoperability for Microwave Access |
| 3GPP | 3rd Generation Partnership Project |
| 3G | 3rd Generation |

## 5 Conventions

The use cases contained in this Deliverable are described using the following template.

| Title of use case | Description |
|---|---|
| Background information | NOTE – It also includes reference to the original FG M2M contribution(s). |
| Involved entities (and associated functional components) | The entities involved in the use case and the associated functional components of the e-health ecosystem. NOTE – In clause 7.1, the functional components are those involved in remote patient monitoring/assisted living service provision (see clause 7.1.1 of D0.2 [ITU-T FG M2M D0.2]). |
| Relevant services (and related application and service categories) | NOTE – In clause 7.1, the relevant services should be linked with the application and service categories as identified in the Deliverable D0.2 [ITU-T FG M2M D0.2]. |
| Use case description | NOTE – This description should possibly use the above identified involved entities, functional components and service categories |
| Information flow | NOTE – The information flow should possibly use the above identified involved entities, functional components and service categories. |
| High level diagram describing the use case | |
| Security threats | The risks of and among identified functional components to |

| | |
|---|---|
| | provide trustworthy and diverse services. NOTE – Security requirements derived from the threats should be described in the "Derived requirements for the e-health ecosystem" field. |
| Derived requirements for the e-health ecosystem | NOTE – Requirements should be written as much as possible in a clear way such that they can then be moved (re-used) into a requirements specific clause of the appropriate deliverable(s) and possibly identifying common requirements derived from the different use cases beyond those specific to each use case. |
| Other information specific to the use case | |

## 6 Summary of use cases

This clause provides a summary of the e-health use cases contained in this document.

| No. | Application category | Use case title | Summary |
|---|---|---|---|
| 1 | Remote patient monitoring / assisted living | Legacy mass medical examination | This use case deals with a person who undergoes a mass medical examination carrying an examination sheet. |
| 2 | Remote patient monitoring / assisted living | Travelling mass medical examination with BAN | This use case deals with a person who undergoes a travelling mass medical examination using BAN-configured medical devices. |
| 3 | Remote patient monitoring / assisted living | Remote patient monitoring | This use case deals with remote patient monitoring that typically involves patient information collection by sensor devices and transmission of this information through a wide area network. |
| 4 | Remote patient monitoring / assisted living | Telehealth Counseling System | This use case introduces Telehealth Counseling System that enables easy and convenient health management and tele-consultation using video phone. |
| 5 | Remote patient monitoring / assisted living | Telehealth management system using NFC e-health device and smart phone | This use case introduces Telehealth Management System using NFC e-health device and smart phone to upload health data. |
| 6 | Remote patient monitoring / assisted living | Telehealth system for home care support | This use case introduces Telehealth system for healthcare in the home using a system with glucose meter and pulse oximeter. |

| | | | |
|---|---|---|---|
| 7 | Remote patient monitoring / assisted living | Ambient Assisted Living (AAL) | This set of use case deals with AAL concerning the use of information technology to assist the elderly, or people who are handicapped in any way, in order to live a fully independent life. |
| 8 | Remote patient monitoring / assisted living | Easy Clinic | This use case aims to make the monitoring process of remote patients in general, and for elderly patients in particular simple and easy. It consists of sending the remote patient readings (Blood Pressure and Sugar Level) from the medical devices to the hospitals/ clinics through land line and broadband connection or using smart phone. |
| 9 | | Personal healthcare data management | This use case introduces the personal healthcare data management system for consumers.<br>Healthcare data are collected through the gateway device, and the data may be synchronized between the gateway device and the PHR server. Note that the PHR server provides a Web service API for end user access. |
| 10 | | Expert system for medical information/applications sharing | This use case deals with medical doctor or institute accessing an expert system for medical information/applications sharing. |

# 7 Detailed use cases

This clause contains the use cases identified by the FG M2M (use cases for e-health applications and services enabled by M2M technologies).

## 7.1 Remote patient monitoring/assisted living

### 7.1.1 Legacy mass medical examination

| | Description |
|---|---|
| Background information | (m2m-i-106, m2m-i-085r1, m2m-i-063)<br>Mass medical examinations including patient care at medical facilities, are conducted in a well-structured environment with the management of examination staff. Examinees can easily follow their instructions during the examination.<br>In most cases, mass medical examinations expect examinees line up in front of each medical instrument and the examination staff measures them one by one. Using a self-measurement system, examinees need not to wait in lines. This is applied to medical equipment which does not need qualified operators, such as X-ray photography, and reduces human intervention and recording errors.<br>When examinees finish all the required measurements, they have |

| | |
|---|---|
| | medical interviews by medical doctors on site or remotely and receive feedbacks, such as prescriptions, from the doctors.<br>This use case highlights a self-examination procedure at mass medical examinations, and describes information flow among examinees, examination staff, and medical doctors.<br>Mass medical examinations with healthcare screening are managed by a government or company who needs to take care of citizens' or employees' health. |
| Involved entities (and associated functional components) | Examinee ("Patients"), examination staff ("Caregivers"), medical doctor ("Caregivers"), medical devices ("Sensors") and management PC (coordinator) ("Gateways"), backend system ("Medical Information System"), PC connected to backend system ("Front End Tools") |
| Relevant services (and related application and service categories) | Medical examination services ("Remote patient monitoring/assisted living") |
| Use case description | 1. An examinee signs up an informed consent of the medical examination service and the examination staff registers him or her to the examination system.<br>2. The examinee receives an IC card or examination sheet with a bar code which is used for user identification at the local site. The examinee undergoes medical measurements as shown in Fig. 1. The number of examination items depends on the medical screening purpose.<br>3. The examinee sweeps his or her IC card on the reader of a sphygmomanometer for automatic local identification. The IC card reader detects the card. The examination system identifies and authorizes the examinee by the local ID in the card by the registered information in the system.<br>4. The examinee checks his/her name on the display of each measurement device, such as a sphygmomanometer and measures by the device. A blood pressure measurement in the examination service is shown in Fig.2 as an example of the procedure.<br>5. The device sends the measured data with the examinee's local ID wirelessly and securely to the management PC.<br>6. The PC receives and stores the data with the examinee's ID as a medical record.<br>(The management PC uploads the medical records to a backend system in a medical call center.)<br>7. The examinee receives a medical interview locally or remotely.<br>8. A medical doctor diagnoses the examinee by his/her records stored in the backend system and interview result.<br>(The medical doctor may prescribe medicines for the examinee depending on the records and medical interview.) |

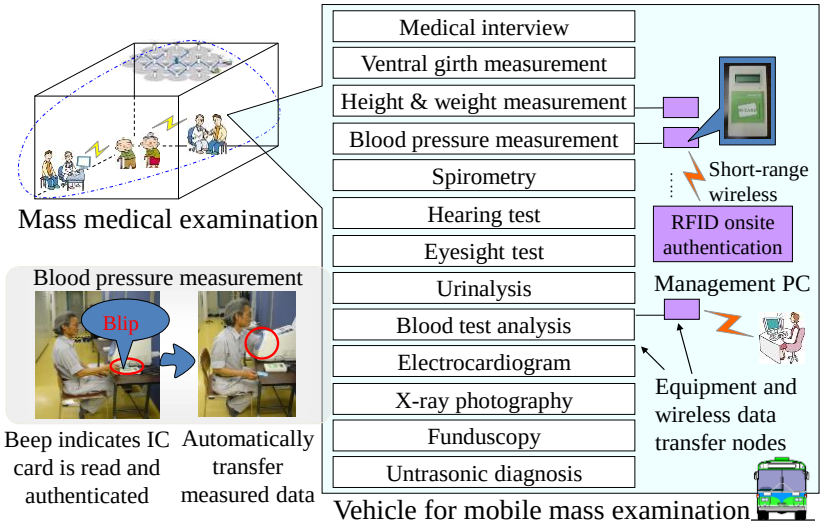
<table>
<tr>
<td></td>
<td>



Fig.1 An example of mass medical examination

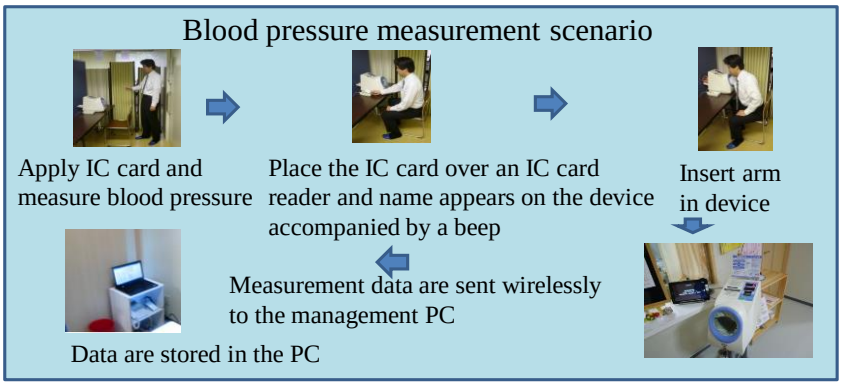
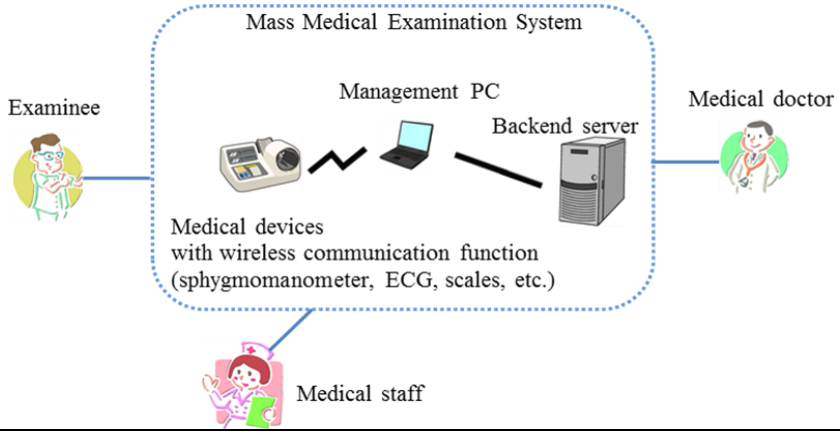



Fig.2 A self-measurement procedure
</td>
</tr>
<tr>
<td>Information flow</td>
<td>
The examination staff registers an examinee to the mass medical examination system and the examinee takes medical examinations by himself or herself.

The mass medical examination system handles the examinees' local IDs and stores their data measured by devices in the system.

The examinee receives medical interview by a medical doctor.

The medical doctor checks the examinees' medical records with the result of the interview whether further diagnosis is required.
</td>
</tr>
<tr>
<td>High level diagram describing the use case</td>
<td>


</td>
</tr>
</table>

| | |
|---|---|
| Security threats | Security threats:<br>Following security threats should be avoided and provided solutions should follow regulation requirements.<br>**Eavesdropping:**<br>− Communication between a device and the management PC<br>An attacker can eavesdrop on the communication and retrieve the vital data with environmental information. The device identification number and temporal user ID may be revealed. Privacy breach by analyzing data may be another risk.<br>− Communication between the management PC and the backend system<br>Privacy breach of personal information and medical records is a risk.<br>− Communication internally performed in a device, management PC or the backend system<br>Privacy breach of personal information and medical records is a risk.<br>**Interruption:**<br>− Communication between a device and the management PC, or the management PC and the backend system, or communication internally performed<br>Privacy breach of personal information and medical records is a risk. This prevents normal services by blocking message or sensed data sending.<br>**Hijacking:**<br>− Data transmitted between a device and the management PC, or the management PC and the backend system in a protocol<br>An attacker can hijack data and prevent normal data transfers.<br>− Data transmitted among internal protocol layers<br>An attacker can hijack data internally transmitted, breach privacy, and prevent normal services.<br>**Interference on wireless communication:**<br>− Interference and jamming between a device and the management PC (LAN) or between the management and the backend system (WAN)<br>**Data tampering:**<br>− Modifications of vital data collected from sensors<br>This causes unreliable medical records creation.<br>− Sensitive system information tampering<br>An attacker modifies sensitive system information, such as user ID and password, and behaves as a legal user. Unauthorized access causes privacy breaches and breaks trust relationships between examinees and medical doctors/ examination staffs.<br>− Control data tampering<br>An attacker modifies control data of LAN and performs unauthorized control of the network. This blocks normal services and leads to other attacks.<br>− Stored data tampering |

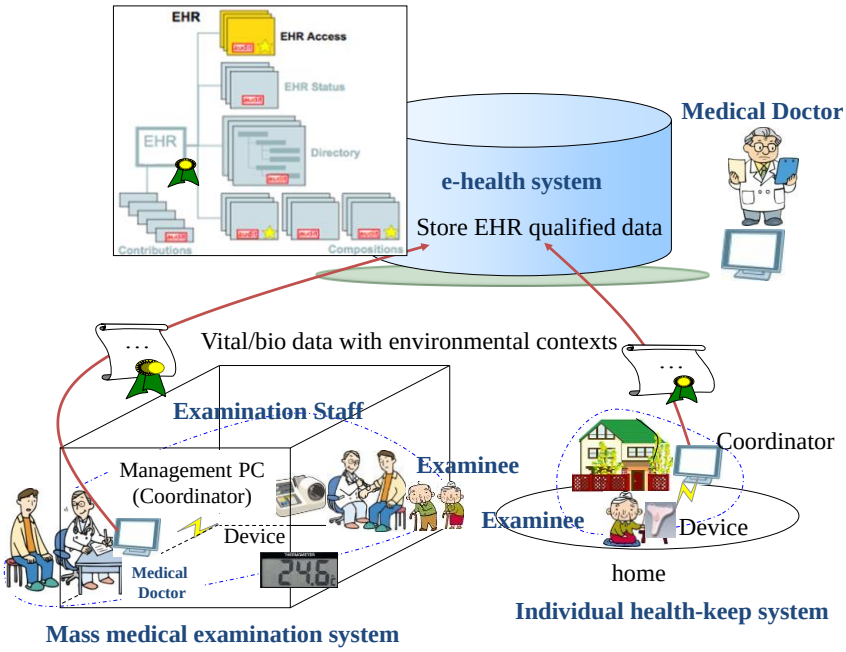
| | |
|---|---|
| | An attacker modifies stored data in a component of the system and prevents normal services and invites the breakdowns of trust relationships between examinees and medical doctors/examination staffs.<br>NOTE - Same threats as subsection 7.1.2 “Travelling mass medical examination with BAN”, except no threats by using BAN, since the legacy mass medical examination does not configure BAN. |
| Derived requirements for the e-health ecosystem | The mass medical examination system shall provide quality of service environment for examinees in terms of data relevancy and efficiency.<br>The mass medical examination system shall combine and store the examinees’ local ID with their medical records following the authorized security procedure.<br>The mass medical examination system shall provide measured data as medical records to a medical doctor.<br>Security and privacy requirements:<br>− Sensitive individual information is handled by established security mechanisms and privacy breach is avoided.<br>Note: The information contains personal information such as name, address, age, gender, medical history, family etc. and medical records including any vital data tagged with the person’s identification provided by examinees to the service provider.<br>− Medical records used in diagnosis are required to be securely protected. The guideline to deal with patient information depends on the policy and regulation of each country.<br>− When sharing personal information of examinees with medical doctors or staffs, it is managed according to his/her agreement on the usage.<br>− In multi-user environment, when sharing a medical device among examinees, measured data by the device corresponds to each examinee.<br>NOTE - Same as subsection 7.1.2. |
| Other information specific to the use case | |

### 7.1.2 Travelling mass medical examination with BAN

| | Description |
|---|---|
| Background information | (m2m-i-106, m2m-i-085r1, m2m-i-063)<br>Traveling mass medical examinations are useful in both developed and developing countries. Equipment used for the examinations are transported by an examination vehicle. The vehicle visits a company or village and measuring devices are set up in rooms at a visited company or village. However, travelling examinations are prone to have a mismatching of examinees, and setting up a system requested by an examinees’ company or |

| | |
|---|---|
| | village may have difficulties in room limitations and ad-hoc wiring of devices. It is also important to know in which environment examinations are undergone. For example, room temperature data is required along with measured data. Some measured data is affected by environment.<br>In this circumstance, the systems expect not only immovable instruments located inside the vehicle, but also battery-operative medical devices in a temporal examination room. Thus, the examination needs to be done in a convenient way, and a wearable Body Area Network (BAN) measurement will be useful for easy-to-use and retrieving the body surroundings. There are various small sensors, such as a small SpO2 sensor consisting of a BAN. Users wear sensors near an examination room and the data are automatically sent to the management PC. Users are free to measure anytime anywhere as long as measurement context, such as environmental temperature, is automatically collected and sent with measured data.<br>If mass medical examinations are executed with self-performed health-checkups and have a wireless link to a medical center operating an e-health system, it will help both examinees and medical staffs, especially countries in short of medical doctors and staffs. Examinees can check their health conditions in a relaxed state and save time spent for commute-and-wait at a medical center for health checks, and medical doctors in the center also can work on thorough medical examinations and treatments.<br>Simple-and-easy health checkups are the first step for screening in Preventive Medicine. BANs deal with continuous data retrieval, such as the continuous measurement of SpO2 and body surroundings, and expects large data for each person. The M2M system can deal with these data and provides interfaces to various medical/healthcare analyses. BAN data are considered as a key component of preventive medicines.<br>This use case describes a flexible local data storing for health checkups using BANs for a travelling mass medical examination and it also describes the relationship between BANs and an e-health backend system from the view point of measured data.<br>Mass medical examinations with healthcare screening are managed by a government or company who needs to take care of citizens' or employees' health, |
| Involved entities (and associated functional components) | Examinee ("Patients"), examination staff ("Caregivers"), medical doctor ("Caregivers"), medical devices ("Sensors") and management PC (coordinator) ("Gateways") in Mass medical examination system, e-health system ("Medical Information System"), PC connected to e-health system ("Front End Tools") |
| Relevant services (and related application and service categories) | Mass medical examination services, individual healthcare services and e-health monitoring services ("Remote patient monitoring/assisted living") |

| | |
|---|---|
| Use case description | 1. An examinee signs up an informed consent of the medical examination and the examination staff registers him or her to the medical examination system.<br>2. The examinee receives an IC card or examination sheet with a bar code which is used for user identification at the examination site. The number of examination items depends on the screening purpose. This system expects not only legacy medical devices such as a weighing scale, but also easy-to-use emerging sensors in a BAN configuration.<br>3. The examinee sweeps his or her IC card on the reader of a sphygmomanometer for automatic local identification. The IC card reader detects the card. The system identifies and authorizes the examinee by the local ID in the card by the registered information in the system.<br>4. The examinee checks his/her name on the display of each measurement device, such as a sphygmomanometer and measures by the device.<br>5. The device sends the measurement data and the examinee's local ID wirelessly and securely to the management PC.<br>6. The management PC receives them. It also collects related supplementary environmental contexts affecting the examinee's measurement results, such as the room temperature. It stores the measurement data and the supplementary environmental contexts with the examinee's ID as a medical record in the PC. The PC is positioned as a data collector of medical devices.<br>7. The examinee receives a medical interview locally or remotely referencing the data.<br>8. After a medical interview, the management PC, which has also a role of the end node of an e-health system, prepares and uploads records following the data security requirements of the e-health backend system. Uploading may be performed via wide-area network, such as a cellular network.<br>9. The backend system stores the data as EHR qualified data.<br>10. Medical doctors diagnose examinees by looking at their records.<br>(Medical doctor may prescribe medicines for the examinees depending on the records and medical interviews.) |
| Information flow | The examination staff registers an examinee to the mass medical examination system and the examinee does medical examinations by himself or herself.<br>The mass medical examination system handles the examinees' local IDs and stores their data measured and corrected by the related supplementary environmental contexts in the system.<br>The mass medical examination system uploads medical records to the e-health backend system. |

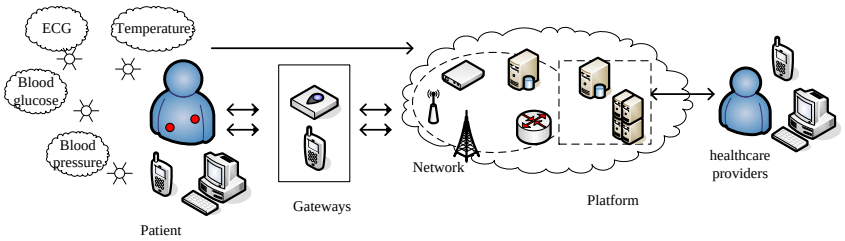
| | |
|---|---|
| | The examinee receives medical interview by a medical doctor.<br>The medical doctor checks examinees' medical records stored in the e-health system with the result of the interview. |
| High level diagram describing the use case |  |
| Security threats | Security threats:<br>Following security threats should be avoided and provided solutions follow regulation requirements.<br>**Eavesdropping:**<br>− Communication between a device and the management PC<br>An attacker can eavesdrop on the communication and retrieve the vital data with environmental information. The device identification number and temporal user ID may be revealed. Privacy breach by analyzing data may be another risk.<br>− Communication between the management PC and the backend system<br>Privacy breach of personal information and medical records is a risk.<br>− Communication internally performed in a device, management PC or the backend system<br>Privacy breach of personal information and medical records is a risk.<br>**Interruption:**<br>− Communication between a device and the management PC, or the management PC and the backend system, or communication internally performed<br>Privacy breach of personal information and medical records is a risk. This prevents normal services by blocking message or sensed data sending.<br>**Hijacking:**<br>− Data transmitted between a device and the management PC, or the management PC and the backend system in a protocol<br>An attacker can hijack data and prevent normal data transfers. |

| | |
|---|---|
| | − Data transmitted among internal protocol layers<br>An attacker can hijack data internally transmitted, breach privacy, and prevent normal services.<br>**Interference on wireless communication:**<br>− Interference and jamming between a device and the management PC (LAN and BAN) or between the management and the backend system (WAN)<br>**Data tampering:**<br>− Modifications of vital data collected from sensors<br>This causes unreliable medical records creation.<br>− Sensitive system information tampering<br>An attacker modifies sensitive system information, such as user ID and password, and behaves as a legal user. Unauthorized access causes privacy breaches and breaks trust relationships between examinees and medical doctors/ examination staffs.<br>− Control data tampering<br>An attacker modifies control data of LAN/BAN and performs unauthorized control of the network. This blocks normal services and leads to other attacks.<br>− Stored data tampering<br>An attacker modifies stored data in a component of the system and prevents normal services and invites the breakdowns of trust relationships between examinees and medical doctors/examination staffs. |
| Derived requirements for the e-health ecosystem | The mass medical examination system shall provide quality of service environment for examinees in terms of data relevancy and efficiency.<br>The mass medical examination system shall combine and store the examinees' local ID with their medical records linked to the related supplementary environmental contexts in a secure way.<br>The mass medical examination system shall provide measured data to a medical doctor for interview and prepare medical records satisfying the security requirements of data upload to the e-health backend system.<br>The e-health system shall handle medical records with related environmental contexts.<br>Security and privacy requirements:<br>− Sensitive individual information is handled by established security mechanisms and privacy breach is avoided.<br>NOTE - The information contains personal information such as name, address, age, gender, medical history, family etc. and medical records including any vital data tagged with the person's identification provided by examinees to the service provider.<br>− Medical records used in diagnosis are required to be securely protected. The guideline to deal with patient information depends on the policy and regulation of each country. |

| | |
|---|---|
| | − When sharing personal information of examinees with medical doctors or staffs, it is managed according to his/her agreement on the usage.<br>− In multi-user environment, when sharing a medical device among examinees, measured data by the device corresponds to each examinee. |
| Other information specific to the use case | BAN which is a key component of Preventive Medicine deals with continuous data retrieval, such as the measurement of percutaneous oxygen saturation rate (SpO2) and environmental temperature, and expects large data for each person. The M2M system deals with these data and provides interfaces to support medical/healthcare analysis.<br>An individual health-keep system having the same functions described in the mass medical examination system can work with the e-health system. Requirements for individual health-keep systems are the same as those for mass medical examination system. |

### 7.1.3 Remote patient monitoring

| | Description |
|---|---|
| Background information | (m2m-i-070, m2m-i-203)<br>Combined with advanced health-monitoring sensors, health-monitoring devices can play an important role in improving the lives of patients, particularly in the weaker sections of the society including disabled, elderly and chronically ill patients.<br>These health-monitoring devices offer great potential help for such patients who may be able to afford good healthcare without having to regularly visit their doctor. Both patient and doctor are able to get potential benefits from these technologies; doctors can focus more on priority tasks by saving time normally spent with consulting ill patients and patients can move about in their environment without having to make extensive trips to the doctor – especially if they reside in a remote location.<br>The following use case describes remote monitoring service suitable for non-emergency situations in a generalized way.<br>The remote patient monitoring has two relevant service models, B2C (e-health platform is owned by network operator) and B2B2C (e-health platform is owned by platform provider, who has a business agreement with network operator). |
| Involved entities (and associated functional components) | Patient (“Patients”), Healthcare providers (“Caregivers”), sensor devices (“Sensors”), Gateway (“Gateways”) , PC/Mobile (“Front End Tools”) |
| Relevant services (and related application and service categories) | Chronic disease management, Postoperative rehabilitation (“Remote patient monitoring/assisted living”) |

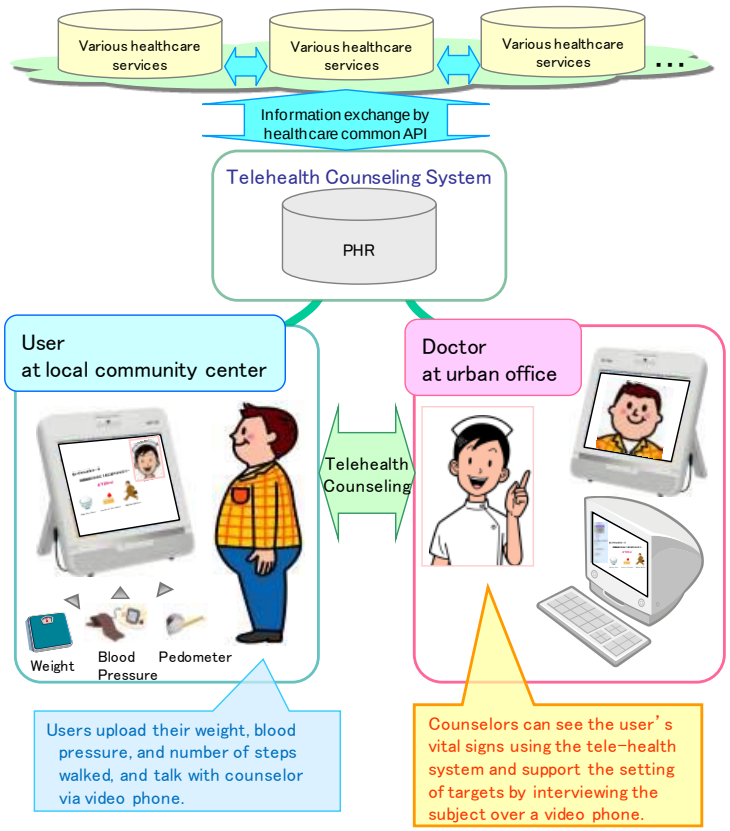
| | |
|---|---|
| Use case description | Remote patient monitoring typically involves patient information collection by sensor devices and transmission of this information through a wide area network. |
| Information flow | 1. A patient can obtain his biological signs (e.g., Electro Cardio Gram, temperature, blood glucose, blood pressure) through body-embedded sensor devices, wearable sensor devices, or sensor devices around him. Besides, motion information (e.g., walking, running, fallen down) of the user and other context information (e.g., monitoring time, position) may also be gathered by related devices.<br>2. Gathered information will be uploaded to an e-health platform, by direct connection into the network or by wireless gateways between the network and the patient environment. If information collected through the short-range wireless network (Bluetooth, Zigbee, etc) is transmitted to a gateway, then it will be uploaded by the gateway through a wide area network (such as Second Generation, Third Generation, Long Term Evolution, etc).<br>3. An e-health platform is responsible for data processing, addressing fragmentation of various Health Information systems, providing effective devices management and other service support functions (e.g., authentication, traffic control, and B2B administration). This platform can be provided by a network operator or a 3rd platform provider.<br>4. Healthcare providers (e.g., clinicians, health care assistants, family members, fitness coaches) can have access to personal data of monitored patient via web/PC/mobile and make feedbacks about the patient's health situation.<br>5. The patient himself can also have access to his personal data and review his feedbacks via web/PC/mobile. |
| High level diagram describing the use case |  |
| Security threats | The following potential security threats should be considered:<br>– Eavesdropping<br>The personal medical data may be captured by unauthorized roles via eavesdropping of the information flow.<br>– Data tampering<br>The personal medical data may be tamperred by unauthorized users or attackers.<br>– Interference on communication link<br>During the transmission between devices and gateways or |

| | |
|---|---|
| | network access points, the personal medical data may be unsuccessfully transmitted due to unexpected interference. The reliability and the integrity of the data may also be affected.<br>– Hijacking<br>The medical service may be hijacked by attackers, and the fake e-health platform may be exposed to users so that unexpected service may be provided to users.<br>– Physical damages<br>The medical data stored in the e-health platform may be lost due to physical damages of the databases.<br>– Impact on body<br>The medical sensor devices, especially the body-embedded devices, may affect the users' body due to electromagnetic factors or other factors. |
| Derived requirements for the e-health ecosystem | – The device must be easy to use and secure.<br>– The device must be managed, such as updating software, configuration, etc, remotely.<br>– If data collected by sensor devices is uploaded without a gateway, these sensor devices must have wide area communication capability.<br>– The network must provide different prioritized treatment for data transmission. Emergency data are often required a higher priority.<br>– The platform is recommended to addressing data interoperability between e-health systems. |
| Other information specific to the use case | |

### 7.1.4 Telehealth Counseling System

| | Description |
|---|---|
| Background information | (m2m-i-106, m2m-i-088, m2m-i-074)<br>The Telehealth Counseling System is used as a Telehealth consultation service, that provides a communication service by video phone between citizens (e.g. elderly people) in rural areas and health professionals (e.g. medical doctors) in urban areas, and includes e-health device (e.g. blood pressure monitor, weight scale and pedometer) to be used by citizens at home or local community center, and an easy service to upload their data.<br>The purpose of the Telehealth Counseling System is to provide counseling to patients remotely using video phone and easy data uploads from e-health device. |

| | |
|---|---|
| Involved entities (and associated functional components) | Users (”Patients”), e-health device (“Sensors”),Video phone (“Gateways”), PHR system (“Medical Information System”), PC (“Front End Tools”), Doctors (“Caregivers”) |
| Relevant services (and related application and service categories) | Remote health counseling, Health data management (“Remote patient monitoring/assisted living”) |
| Use case description | Users:<br>– (Walk with pedometer and go to local community center)<br>– Login to Telehealth Counseling System with pedometer ID<br>– Upload the pedometer data<br>– Measure and upload weight data<br>– Measure and upload pressure monitor data<br>– See the data on video phone<br>– Receive counseling from doctors through video phone<br>e-health device:<br>– Pedometer sends its internal ID and number of steps walked to the video phone that has an interface with the e-health device<br>– Weight scale and blood pressure monitor send their data to the video phone that has an interface with the e-health device<br>Video phone:<br>– Sends data to a PHR system automatically<br>– Shows data upon user’s request<br>PHR system:<br>– Receives and stores user data from video phone<br>– Returns data on request from video phone<br>Doctors:<br>– See user data on PC<br>– Provide counseling to users through video phone |
| Information flow | 1. A user living in a rural area wears a pedometer in daily life.<br>2. Once a week, users gather at a local community center to upload their health data to a PHR system.<br>3. A user logs onto the system using his/her pedometer ID, and uploads the data of number of steps walked.<br>4. After that, the user measures his/her own blood pressure and weight, and uploads data to the database of the PHR system. Users can see their data just uploaded with their previously measured health data.<br>5. Doctors in urban areas can see the user data from their office.<br>6. Once a month, users and doctors have a health counseling appointment. They can see the same data through the video |

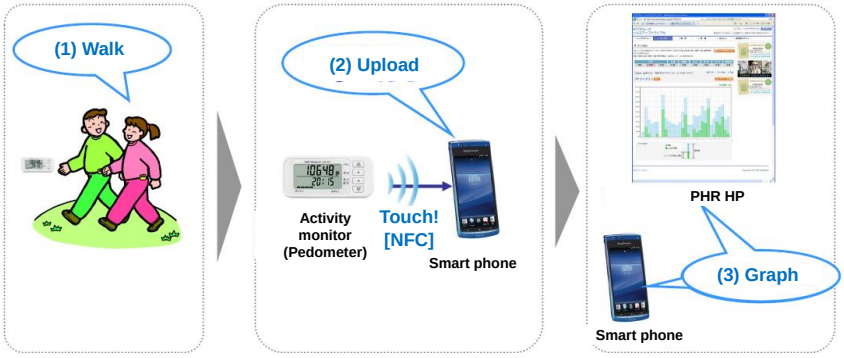
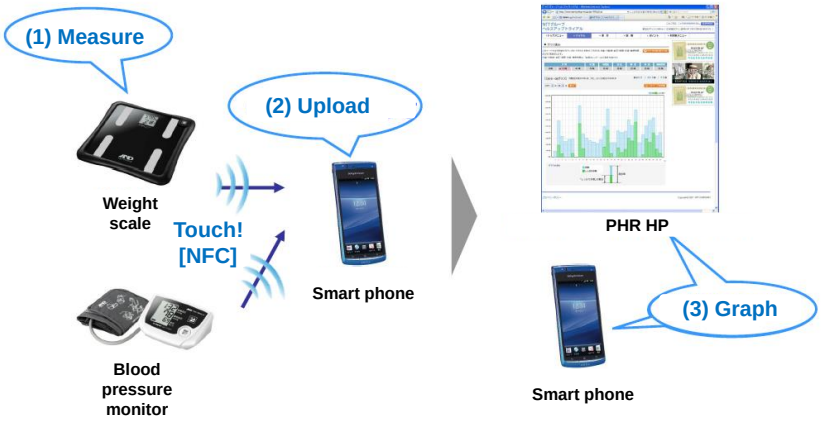
| | |
|---|---|
| | phone on the system. |
| High level diagram describing the use case |  |
| Security threats | [Users]<br>– N/A<br>[e-health device]<br>– Exposing measured data to other users on health devices<br>– Exposing stored data on a lost/stolen health device<br>– Exposing stored data by using a lost/stolen pedometer ID<br>[Video phone]<br>– Exposing stored data by using a lost/stolen video phone<br>– Reporting inaccurate results from healthcare device (falsification)<br>– Stealing user identity using a registered video phone (data upload from unregistered e-health device)<br>– Stealing of ID, password, and health data<br>[PHR system]<br>– Stealing user identity using a registered server<br>– Exposing PHR data to unregistered third parties (User/Web Service)<br>– Stealing user identity for accessing PHR data<br>– Loosing stored PHR data (includes overwriting data) |

| | |
|---|---|
| | – Other security measures including anti-virus<br>[Doctors]<br>– N/A |
| Derived requirements for the e-health ecosystem | – e-health device should have a function to transfer electronic data automatically to a video phone.<br>– e-health device should have an interface such as Bluetooth and NFC etc to upload health data from e-health device to a video phone.<br>– A video phone should receive vital data from various types of e-health device (at least two types of equipment, e.g. blood pressure monitor and weight scale).<br>– A video phone should have a function to transfer electronic data automatically to a PHR system.<br>– A PHR system shall receive data from a gateway and store data in a database.<br>– A PHR system should exchange health data with other PHR systems.<br>– Telehealth system should have a high security function such as digital certification, client authentication, or data encryption.<br>– Telehealth system should have a personal identification function such as identification and authorization by ID and password.<br>– Telehealth system should manage the unique IDs of health devices.<br>– Telehealth system shall have a wired or wireless communication network.<br>– Telehealth system should use health data set that has already been standardized. |
| Other information specific to the use case | |

### 7.1.5 Telehealth management system using NFC e-health device and smart phone

| | Description |
|---|---|
| Background information | (m2m-i-106, m2m-i-088, m2m-i-072)<br>This Telehealth management use case uses near-field communication (NFC) e-health device including a pedometer, weight scale, and blood pressure monitor, along with a smart phone to upload user health data, to evaluate health management programs. |

| | |
|---|---|
| Involved entities (and associated functional components) | Users (”Patients”), e-health device (“Sensors”), Smart phone (”Gateways”), PHR system (“Medical Information System”), Doctors (“Caregivers”), PC (“Front End Tools”) |
| Relevant services (and related application and service categories) | Remote health counseling, Health data management (“Remote patient monitoring/assisted living”) |
| Use case description | Users (employees):<br>– (walk with pedometer in daily life)<br>– Measure weight and blood pressure manually<br>– Upload number of steps walked, weight, and blood pressure by NFC touch interfaces between e-health device and smart phone<br>– See their own vital data on smart phone<br>e-health device:<br>– Measure user’s vital data<br>– Send the data to a smart phone by a NFC touch interface between e-health device and smart phone<br>Smart phone:<br>– Sends data to a PHR system automatically<br>– Shows the data on a smart phone by request of the user<br>PHR system:<br>– Receives and stores data from a smart phone<br>– Returns data on request from a smart phone |
| Information flow | 1. A participating user who works at the company has a smart phone, pedometer, weight scale, and blood pressure monitor.<br>2. In advance, the user installs software for the trial to the smart phone and logs in to the software using his/her ID and password provided by the trial secretary.<br>3. The user walks with the pedometer attached and uploads the pedometer data by touching the smart phone and pedometer whenever the user likes.<br>4. The user measures weight and/or blood pressure at home or at the working place and uploads the data by a touch interface on the smart phone, weight scale, and/or blood pressure monitor.<br>5. The user can see his/her graph of data including past measured health data on the smart phone or PC.<br>6. (Over a period of time) the doctor examines user’s measured vital data along with blood test results and evaluates them. |

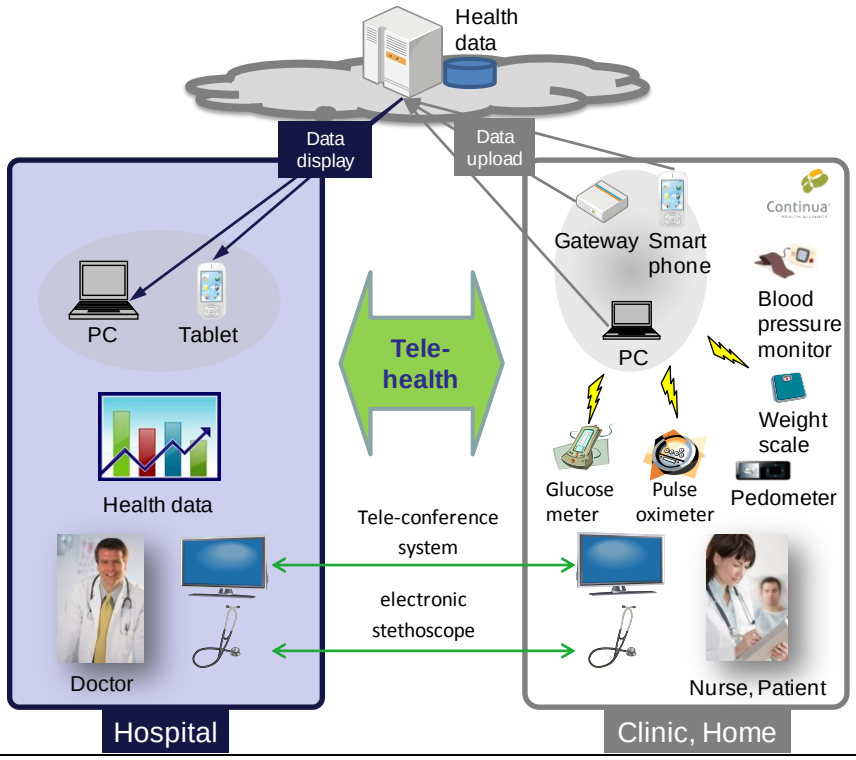
| | |
|---|---|
| High level diagram describing the use case |  <br>  |
| Security threats | [Users]<br>– N/A<br>[e-health device]<br>– Exposing measured data to other users on health devices<br>– Exposing stored data on a lost/stolen health device<br>[Smart phone]<br>– Exposing stored data by using a lost/stolen smart phone<br>– Report inaccurate results from a healthcare device (falsification)<br>– Stealing user identity using registered smart phones (data upload from unregistered e-health device)<br>– Stealing of ID, password, and health data<br>[PHR system]<br>– Stealing user identity using a registered server<br>– Exposing PHR data to unregistered third parties (User/Web Service)<br>– Stealing a user identity for accessing PHR data<br>– Loosing stored PHR data (includes overwriting data)<br>– Other security measures including anti-virus.<br>[Doctors] |

| | |
|---|---|
| | – N/A |
| Derived requirements for the e-health ecosystem | – e-health device should have a function to transfer electronic data automatically to a smart phone.<br>– e-health device and a smart phone should have an interface such as Bluetooth and NFC etc to upload health data from e-health devices to the smart phone.<br>– A smart phone should receive vital data from various types of e-health device (at least two types of equipment, e.g. blood pressure monitor and weight scale).<br>– A smart phone should have a function to transfer electronic data automatically to a PHR system.<br>– A PHR system shall receive data from a gateway and store the data in the database.<br>– A PHR system should exchange health data with other PHR systems.<br>– Telehealth system should have high security functions, including digital certification, client authentication, or data encryption.<br>– Telehealth system should have a personal identification function such as identification and authorization by ID and password.<br>– Telehealth system should manage the unique IDs of health devices.<br>– Telehealth system shall have a wired or wireless communication network.<br>– Telehealth system should use a health data set that has already been standardized. |
| Other information specific to the use case | |

### 7.1.6 Telehealth system for home care support

| | Description |
|---|---|
| Background information | (m2m-i-106, m2m-i-088, m2m-i-071)<br>Telehealth system for home care support is used to reduce the amount of commuting by both doctors and patients to and from hospital by uploading health data. |
| Involved entities (and associated functional components) | Users (“Patients”), e-health device (“Sensors”), Upload gateway/PC (“Gateways”), PHR system (“Medical Information System”), Nurses at clinic (”Caregivers”) , Doctors at hospital (”Caregivers”), PC for health professionals (“Front End Tools”), Tablet PC for users (“Front End Tools”) |
| Relevant services (and related application and service | Remote health counseling, Health data management (“Remote patient monitoring/assisted living”) |

| | |
|---|---|
| categories) | |
| Use case description | Users (patients):<br>– (walk with pedometer in daily life)<br>– Manually measure weight, blood pressure, glucose level with glucose meter and SpO2 with pulse oximeter<br>– Upload number of steps walked, weight, blood pressure, glucose level, and SpO2 to an upload gateway/PC semi-automatically<br>– See their own vital data on tablet PC<br>e-health device:<br>– Send data to an upload gateway/PC after measurement by users<br>Upload gateway/PC:<br>– Send data from e-health device to a PHR system automatically<br>PHR system:<br>– Receive and store the data from an upload gateway/PC<br>– Return data on request from users, nurses, and doctors<br>Nurses:<br>– See user data from clinic<br>– See user data from user's home<br>– Give advice to users under doctor's guidance<br>Doctors:<br>– See user data from hospitals<br>– Give advice to nurses<br>PC for Professionals:<br>– Shows user data<br>Tablet PC for Users:<br>– Shows user data |
| Information flow | 1. A user with chronic diseases who lives away from a hospital walks with a pedometer to improve his/her condition in daily life.<br>2. Once a day, the user uploads the data of number of steps walked.<br>3. The user measures his/her blood pressure, weight, glucose level, and SpO2 and uploads the data to a PHR system.<br>4. The user sees his/her data with past measured health data in the PHR system.<br>5. A nurse sees user data from clinic or user's home remotely.<br>6. A doctor sees user data from the hospital remotely. |

| | |
|---|---|
| | 7. A nurse provides health support including advice and instruction under a doctor's guidance. |
| High level diagram describing the use case |  |
| Security threats | [Users]<br>– N/A<br>[e-health device]<br>– Exposing measured data to other users on health devices<br>– Exposing stored data on a lost/stolen health device<br>[Upload gateway/PC]<br>– Exposing stored data by using a lost/stolen PC<br>– Report inaccurate results from healthcare device (falsification)<br>– Stealing user identity using a registered upload gateway and PC (data upload from unregistered e-health device)<br>– Stealing of ID, password, and health data<br>[PHR system]<br>– Stealing user identity using a registered server<br>– Exposing PHR data to unregistered third parties. (User/Web Service)<br>– Stealing user identity for accessing PHR data<br>– Loosing stored PHR data (includes overwriting data)<br>– Other security measures including anti-virus<br>[Doctors] |

| | |
|---|---|
| | N/A |
| Derived requirements for the e-health ecosystem | – e-health device should have a function to transfer electronic data automatically to an upload gateway/PC.<br>– e-health device and an upload gateway/PC should have an interface such as Bluetooth and NFC to upload health data from e-health device to an upload gateway/PC.<br>– An upload gateway/PC should receive vital data from various types of e-health device (at least two types of equipment, e.g. blood pressure monitor and weight scale).<br>– An upload gateway/PC should have a function to transfer electronic data automatically to a PHR system.<br>– A PHR system shall receive data from an upload gateway/PC and store data in a database.<br>– A PHR system should exchange health data with other PHR systems.<br>– Telehealth system should have a highly security function such as digital certification, client authentication, or data encryption.<br>– Telehealth system should have a personal identification function such as identification and authorization by ID and password.<br>– Telehealth system should manage the unique IDs of health devices.<br>– Telehealth system shall have wired or wireless communication network.<br>– Telehealth system should use health data set that has already been standardized. |
| Other information specific to the use case | |

### 7.1.7 Ambient Assisted Living (AAL)

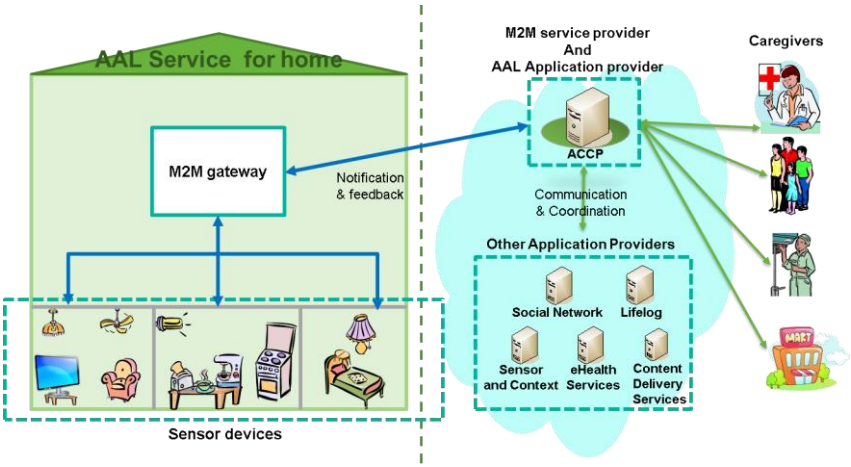
NOTE – the current table includes multiple use cases for Ambient Assisted Living.

| | Description |
|---|---|
| Background information | (m2m-i-017), (m2m-i-062), (m2m-i-174)<br>AAL (Ambient Assisted Living) is a use case to assist the elderly, or people who are handicapped in any way, to live a fully independent life. Technology is seen as one possibility for shaping our future in times of demographic change and living longer. It is seen as a possible means to keep ourselves healthy and active for even longer.<br>There are several scenarios of AAL service; depending on the user's symptoms and condition, AAL scenarios correspond to each situation. |

| | |
|---|---|
| | The AAL has two relevant service models, B2C (ACCP can be owned by network operators) and B2B2C (ACCP owned by MVNO provider and network operators). |
| Involved entities (and associated functional components) | AAL-user (“Patient”); sensor devices, M2M gateway (“Gateways”); WAN; Advanced Care Coordination Platform (ACCP) (“M2M service provider”) and (“Application service provider”); Front End Tools; Caregiver, Family living remotely, Trainee (“Caregivers”) |
| Relevant services (and related application and service categories) | Elderly person support service (“Remote patient monitoring/assisted living”) |
| Use case description | 1. Bath overflows avoidance<br>When the AAL-user puts hot water in a bathroom, family living remotely confirms water-level and stops. The AAL-user establishes the water level which stops. When the water-level sensor measures the water-level reaches the volume of hot water established by AAL-user, the sensor notifies ACCP via the M2M gateway. The hot water is stopped by ACCP and warns to AAL-user. The family of AAL-user can remotely check the event on the website and advice to AAL-user.<br>2. Close window if it rains<br>Some windows can be motorized to open or close for ventilation. System reacts to storm warning or moisture sensor.<br>When the wind-level measured by anemometer reaches the high level, windows in the house are opened and closed automatically by motors. And thermometer and hygrometer can measured as same as the anemometer can.<br>3. Emergency call button<br>User can push a button on his neck-cord when in an emergency situation.<br>AAL-user can press the emergency button embedded in the device (ex. necklace like). The device with emergency button needs to communicate with ACCP inside and outside location so that this device can access multiple wired and wireless broadband networks (ex. Wi-Fi, WiMAX, 3GPP, NGN). The caregiver and family living remotely can suitable dispose for AAL-user (ex. calling ambulance, rushing to user’s location), when they are warned by ACCP.<br>4. Opening and locking doors after user leaves<br>Electronic lock activates if AAL-user exits the house, opens upon return. AAL-user can see the door webcam and remotely open it. Door video can be shown if user cannot reach door. Caregiver can also access.<br>The biometrics sensor embedded in a door can recognize the |

| | |
|---|---|
| | AAL-user by AAL-user's biometrics information, the door is locked automatically when AAL-user goes out, and the door is opened automatically when AAL-user comes back by using biometrics sensor (fingerprint, the voiceprint, retina and facial authentication). This event of the door opening and closing is noticed to ACCP via M2M gateway, Caregiver and family living remotely can check AAL-user's event and give the AAL-user advices.<br>5. Pot boils over and smoking food alert in kitchen<br>Fluid sensor at stove causes alert, ACCP switches stove off.<br>The liquid sensor embedded in a stove detects a pot heated and the liquid which overflowed a pot and notifies this situation to ACCP via M2M gateway. And the sensor monitors the situation of power meter of an oven. When the ACCP detects the bad situation, ACCP sends signal to switch-off the oven. Caregiver and family living remotely can check the event on website.<br>6. Smoking alert (gentle)<br>Smoke sensor in the home can warn if sensor detects too much smoke.<br>7. When a smoking sensor measures abnormal-smoking-level, the sensor devices can notify ACCP of the situation via M2M gateway. ACCP can alarm to the AAL-user and can alarm to Caregiver or the family living remotely who can make emergency call.<br>8. Retrieving/bringing objects<br>A nursing robot with tray for holding drinks or food-tray, can be steered to bedside remotely by AAL-user.<br>A nursing robot that can be controlled remotely is operated by family living remote location. The nursing robot can bring something to drink and eat to the AAL-user who is in the bedroom and.<br>9. Fall-down alert<br>User falling and lying prone generates alert to Caregiver<br>When monitoring cameras and temperature sensors measure the abnormal situation, the sensor devices notices this situation to ACCP via M2M gateway. When the ACCP judges the situation of the AAL-user falling down, ACCP alarms to caregiver or family living remotely.<br>10. Inactivity alert<br>ACCP creates the profile of AAL-user's usual behavior. As example of the profile, ALL-user usual turns on a pot every morning, turn off a light every night, and so on. The sensors always monitor the profiled situation of AAL-user's activity and notice information to ACCP. When the ACCP detects abnormal situation rather than the normal situation, ACCP |

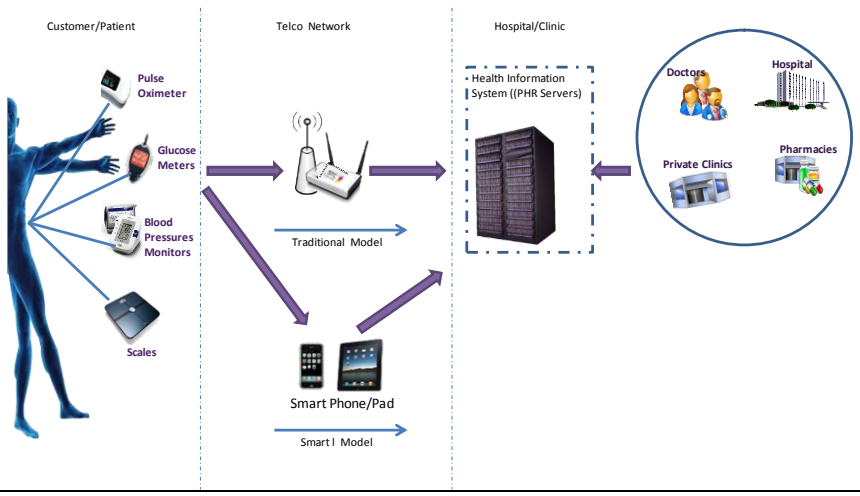
| | |
|---|---|
| | notices this situation to Caregiver or family living remotely.<br>11. Recover dementia people after missing location<br>AAL-user's location from mini mobile phone device and GPS can be seen by Caregiver. ACCP can also be set to send alert.<br>The small communication device with GPS device carried by dementia people notifies the location of AAL-user to ACCP. The device needs to communicate with ACCP inside and outside location so that this device can access multiple wired and wireless broadband networks (ex. Wi-Fi, WiMAX, 3GPP, NGN). The caregiver and family living remotely can suitable dispose for AAL-user with correct location of AAL-user, when they are warned by ACCP.<br>12. Flexible and tailored on-demand services<br>AAL scenario can be created flexibly and tailored by Caregiver or AAL-user. For example, regarding a case of morning scenario: step 1: the coffee machine can detect that this coffee machine is switched on by AAL-user and notice this detection to M2M gateway; step 2: M2M gateway can start a breakfast preparation scenario in getting the detection from the coffee machine. According to a breakfast preparation scenario, the blind in bedroom can be lifted automatically. |
| Information flow | 1. Monitoring<br>Some kind of sensors (temperature, moisture, lights/emergency call switch on/off, electronic lock door, smoke etc.) can obtain measurement results or status on equipment embedded sensor devices and also sends these parameters or status to M2M gateway through the wired or short range wireless local network.<br>2. Interpretation<br>M2M gateway can interpret what kind of sensor sent information and identify the user and gather the parameters or status information and assemble this information into specified data format. M2M gateway uploads this information to an Advanced Care Coordination Platform (ACCP) through the wired network (NGN, ISDN, PSTN etc.) or wireless network (GSM, 3G, LTE, WiMAX etc.).<br>3. Identity Management<br>ACCP can accept the monitored information by several M2M gateways and can manage the user identification.<br>4. Distributed Access Control<br>The information related with one user can be uploaded to an ACCP from several M2M gateways through the most suitable access network (wired/wireless). The ACCP can connect and control the distributed access network. |

| | |
|---|---|
| | 5. Communication & Coordination<br>ACCP can obtain and analysis the parameters or status information sent by M2M gateway in order to analysis the result of the monitoring. And ACCP can communicate with other Application provided by other providers (ex. e-health application, Lifelog application, that is typically to capture their entire lives, or large portions of their lives as digital data with computer devices, Social Network application etc.) and can coordinate with other Application.<br>6. Feedback<br>ACCP can get the analyzed result from Caregivers and can obtain the feedback from other Application providers. ACCP can integrate the instructions according to this feedback and can send to M2M gateway. ACCP can also send to Front End Tools for Caregivers or Patients.<br>7. Analysis<br>M2M gateway can receive the instructions integrated by ACCP through the network. And M2M gateway can analyze the received instructions for the user. Front End Tools can also receive the instructions and Caregivers or Patients can analyze the received instructions.<br>8. Service<br>M2M gateway can identify the activity detection by analyzing the received instructions and can send the instruction to the suitable object (ex. lights, windows, oven, etc.) that can directly provide the service to the users. |
| High level diagram describing the use case |  |
| Security threats | The following potential security threats should be considered:<br>– **Eavesdropping:**<br>The personal location and behavior data may be captured by unauthorized roles via eavesdropping of the information flow.<br>– **Interruption:**<br>Communication between sensor devices and M2M gateway, |

| | |
|---|---|
| | or M2M gateway and ACCP<br>Privacy breach of personal information, user's location and behavior date is a risk. This prevents normal services by blocking message or sensed data sending.<br><br>– **Hijacking:**<br>Data transmitted between sensor devices and M2M gateway, or M2M gateway and ACCP in a protocol<br>An attacker can hijack data and prevent normal data transfers.<br>Data transmitted among internal protocol layers<br>An attacker can hijack data internally transmitted, breach privacy, and prevent normal services. |
| Derived requirements for the e-health ecosystem | 1. Identity Management<br>– ACCP must manage identification (e.g. sensor device identification, M2M gateway identification, user identification, service identification, group identification)<br>– ACCP must manage identities for privacy data (e.g. user personal data)<br>– M2M gateway must manage identification (e.g. sensor device identification, user identification)<br>2. Distributed Access Control<br>– ACCP must control multiple distributed wired access networks (NGN, ISDN, PSTN etc.) or wireless networks (GSM, 3G, LTE, WiMAX etc.): ACCP must have a function to connect several authentication access network domains dynamically according to traffic situation or connectivity.<br>3. Advanced Platform<br>– ACCP should have capabilities of Reliability, Efficiency, Security, Privacy, Trust, Flexibility<br>4. Plug & Play of sensor devices<br>– Sensor devices must have easy user interface and have a function of Plug and Play to connect easily to M2M gateways.<br>5. Remote Installable Software<br>– ACCP must have a capability to manage software in sensor devices and M2M gateways and update software remotely.<br>6. Communication and collaboration with other applications<br>– Data managed in ACCP should be standardized for other semantic services (Smart meter service, ITS service, etc.) in order to share data for collaboration with other applications. |
| Other information specific to the use case | |

### 7.1.8 Easy Clinic

| Easy Clinic | Description |
|---|---|
| Background information | (m2m-i-075), (m2m-i-174)<br>This use case introduces the remote patient monitoring service for consumer/ user using his/her landline or smart phone.<br>The solution aims to make the monitoring process of patients in general, and for elderly patients in particular simple and easy to send the readings to the hospitals/clinics and doesn't need specific IT skills. |
| Involved entities (and associated functional components) | e-health devices ("Sensors"), Modem/Smart phone ("Gateways"), PHR server ("Medical Information System"), Doctors ("Caregivers") |
| Relevant services (and related application and service categories) | Remote monitoring service ("Remote Patient Monitoring/Assisted Living") |
| Use case description | Easy Clinic service is applied through 2 different Models :<br>Traditional/classical model: using the medical devices and a landline equipped with a modem and Internet connection, where Blood Pressure and Sugar Level readings are sent through their built in Modems to the PHR servers in Hospitals/Clinics once a day/week depending on the configuration defined.<br>Smart/Advanced model: Blood Pressure and Sugar Level devices send data to Smart devices which send them to the PHR servers in Hospitals/Clinics using wireless networks (GPRS, 3G, 4G). |
| Information flow | 1. In the Traditional model, readings are sent to the hospital/Clinic PHR servers periodically once a day/a week (depending on the predefined configuration).<br>2. In the Smart model readings are sent to the Smart devices where they will be transferred to the Hospital/Clinic PHR servers.<br>The measured data are stored in the patients' account in the PHR servers, and made available to the doctors, and authorized people only. |

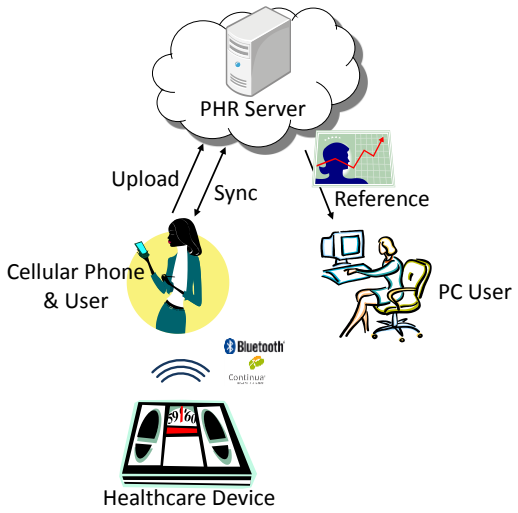
| | |
|---|---|
| High level diagram describing the use case |  |
| Security threats | One of the challenges of the remote patient monitoring is to ensure that the data transmitted from e-health devices to doctors and clinicians are secure enough. The following are the main aspects that should be considered:<br>– Confidentiality<br>– Integrity<br>– Authenticity<br>– Availability<br>– Access<br>– Reliability<br>Privacy issues derive from multidisciplinary fields such as e-health devices, Network, bioinformatics, Hospitals, Health Information Systems (HIS), etc. :<br>– Misuse of Patient Medical Information by unauthorized individual (Eavesdropping or information theft)<br>– Data Leakage (Prescription / Readings)<br>– Patient's data manipulation |
| Derived requirements for the e-health ecosystem | – Broadband connection should be available in the Patient home.<br>– The e-health devices and gateway device (Modems, Smart phones) should support common protocol to transfer the measured data by the e-health device.<br>– The e-health devices should have rich User Interface easy to use by the patient.<br>– The PHR Server should have Web-based API for accessing to PHR.<br>– The gateway device should support scheduled upload on uploading measured data to PHR Server.<br>– Authorized users and specially patient's doctors should have easy and full access to PHR servers. |

| | |
|---|---|
| Other information specific to the use case | – Remote Patient Monitoring use cases are facing difficulties in justifying their business cases.<br>– The investment required should be studied well and supported by eco-system stakeholders.<br>– Telcos need to be well prepared in selling e-health solutions and in particular Remote Patient Monitoring solutions, and they have to strongly cooperate with health care people such doctors, nurses to increase the adoption rate of these kind of new solutions. |

## 7.2 Other use cases

### 7.2.1 Personal healthcare data management

| | Description |
|---|---|
| Background information | (m2m-i-086, m2m-i-055)<br>This use case introduces the healthcare data management service for the user using his/her cellular phone.<br>Since the user may not have high level of IT skills, it is important to use cellular phone as the gateway to ease operating healthcare device, and collecting healthcare data to the PHR Servers.<br>On the other hand, the user may require PHR Servers to show various kinds of views. |
| Involved entities (and associated functional components) | Cellular phone user (“Patients”), Healthcare devices (“Sensors”), Cellular phone (“Gateways”), PHR Server (“Medical Information System”), PC/Cellular phone(“Front End Tools”), Tablet PC for users (“Front End Tools”) |
| Relevant services (and related application and service categories) | health data management |
| Use case description | Between (cellular phone’s) user and cellular phone:<br>– In this scenario, the cellular phone provides rich user interface (UI) for controlling healthcare device(s), and for viewing PHR records on PHR Server.<br>Between cellular phone and healthcare device:<br>– The phone collects the measured data by healthcare device (i.e. weight scale, blood pressure meter, etc.) over Bluetooth connectivity.<br>Between cellular phone and PHR Server:<br>– The cellular phone will upload the measured data to the PHR Server over mobile phone network.<br>– The cellular phone will access to the PHR records through Web applications. |
| Information flow | 1. The user invokes agent application on cellular phone. |

| | |
|---|---|
| | 2. The user turns on the healthcare device.<br>3. The phone discovers a healthcare device, and will establish the connection to the device.<br>4. The user uses the healthcare device.<br>5. The healthcare device sends measured data to the cellular phone.<br>6. The cellular phone forwards the measured data to the PHR Server.<br>7. The phone may store the data for future reference.<br>8. The PHR Server stores the measured data binding to the user's account information.<br>9. The user can access the measured data on the PHR Server through the UI on the phone. |
| High level diagram describing the use case |  |
| Security threats | [Confidentiality]<br>– Exposing PHR data on PHR Server to unauthorized entities<br>– Exposing measured data on Healthcare device to other users<br>[Integrity]<br>– Identity spoofing on Server or Gateway Server<br>– Identity Spoofing on user authentication for accessing to PHR data<br>– Reporting inaccurate measured data from device<br>[Availability]<br>– Loosing stored PHR data<br>– Exposing stored measured data on lost/stolen device |
| Derived requirements for the e-health ecosystem | – The healthcare device and gateway device (cellular phone) should support common protocol (such as Health Device Profile of Bluetooth) to transfer the measured data by the healthcare device.<br>– The gateway device should have rich UI to ease user's |

| | |
|---|---|
| | operation.<br>– The PHR Server should have Web-based API for accessing to PHR.<br>– The gateway device should support scheduled upload on uploading measured data to PHR Server.<br>– The behavior of the gateway device should be controlled by the PHR Server (e.g. scheduled upload timing, server selection, etc.)<br>– The API on the PHR should expose PHR data according to the access control rule. |
| Other information specific to the use case | |

# Annex A:

## Contributed use cases outside the scope of the FG M2M

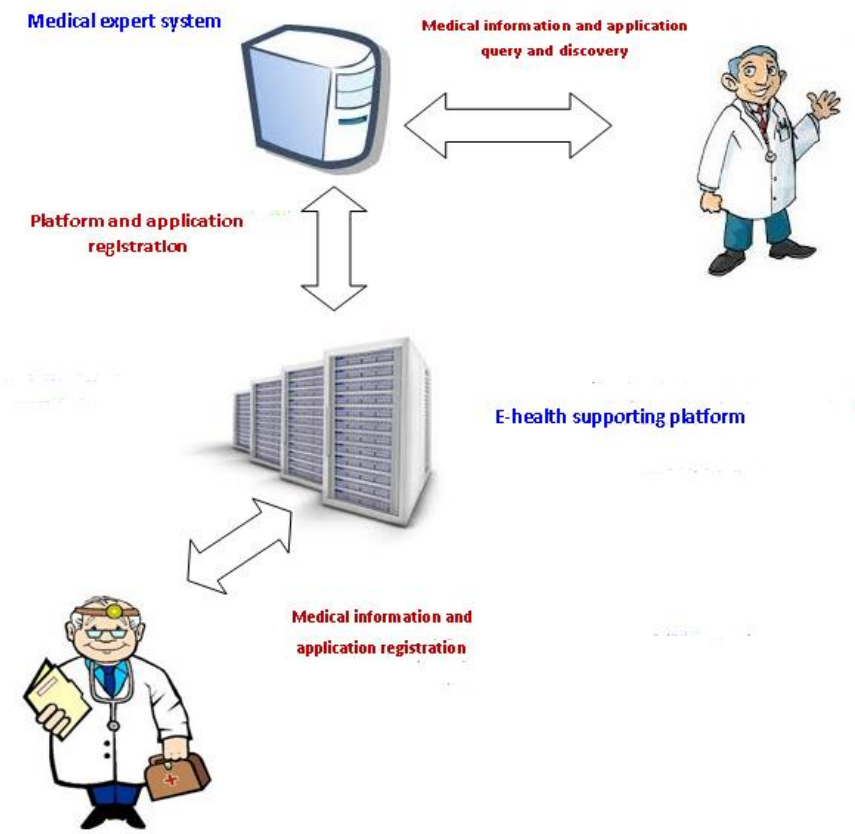
NOTE – "Outside the scope of the FG M2M" means that these uses cases do not necessarily involve the usage of M2M technologies.

## A.1 Individual electronic health information: Electronic Health Record (EHR)

### A.1.1 Expert system for medical information/applications sharing

| | Description |
|---|---|
| Background information | (m2m-i-112, m2m-i-090r1)<br>In e-health scenarios, to achieve the goal of medical information sharing (e.g. in order that a doctor can get the past medical cases from experienced doctors for reference), a mechanism is required, through which medical institutes/doctors could register/save related medical cases to some specific entities for the accessibility of other institutes or doctors.<br>Entities mentioned above are usually called "expert system". The expert system contains valuable resources for more efficient treatment of patients.<br>Medical doctors or medical institutes, who need medical information/applications and/or past medical cases from experienced doctor, use the expert system for information reference to work out better treatment solution. |
| Involved entities (and associated and related application and service functional components) | Medical expert system/e-health supporting platform ("Medical Information System"), Medical doctor ("Caregivers") |
| Relevant services (and related application and service categories) | Medical examination services, medical diagnosis |
| Use case description | 1: e-health supporting platforms register themselves with medical information/applications to the expert system, a platform with the responsibility of medical information/applications registration and discovery.<br>2: Expert system accepts registration request from e-health supporting platforms and then creates resource(s) (i.e. representing the registered e-health supporting platforms), e.g. corresponding database, and stores locally the description information of the specific e-health supporting platform which is contained in the registration request, and replies with acknowledgement message to activate the medical information/applications registration.<br>3: After receiving the reply from expert system, e-health supporting platforms send to expert system the medical information/applications registration request which includes the list of medical information/applications that the specific e-health |

| | |
|---|---|
| | supporting platform supports.<br>4: Expert system accepts the medical information/applications registration request and creates resource(s) and stores this information co-related with the registered e-health supporting platforms in order that other medical doctors or institutes can discover these medical information/applications through these stored information.<br>5: Other medical doctors or institutes can interrogate the expert system with query criteria (e.g. telemedicine application X operated by hospital Y) by using the service terminal. Expert system checks the locally stored description information of the medical information/applications to determine whether the request could be satisfied. If specific description information matches the query criteria, expert system replies with the description information about the medical information/applications and additionally the specific e-health supporting platforms supporting the service. With the provided information, the requesting medical doctors or institutes can access the e-health supporting platform and correspondingly use the medical information/applications. |
| Information flow | e-health supporting platforms register themselves with self description information and medical information/applications description information.<br>Expert system acknowledges the registration request from e-health supporting platforms and replies with success message.<br>Medical doctors or institutes query the expert system for medical information/applications of interest. |

| | |
|---|---|
| High level diagram describing the use case |  |
| Security threats | Security threats that need to be avoided:<br>– Unauthorised doctors or medical institutions initiate medical information and application registration to e-health supporting platform. Only those doctors or medical institutions that subscribed medical information and application sharing service are permitted to successfully register to e-health supporting platform for further process.<br>– Unauthorised e-health supporting platform initiates platform and application registration to medical expert system, especially when they belong to different owners. The medical expert system shall have security control over the registration of e-health supporting platform and applications. The medical expert system only accepts the registration of the e-health supporting platform and applications from the authorised/subscribed e-health supporting platfroms.<br>– Unauthorised doctors or medical institutions initiate medical information and application query and discovery request to medical expert system. Only those doctors or medical institutions that subscribed to medical expert system are permitted to get requested medical information and application. |
| Derived requirements for the e-health ecosystem | The system shall provide a mechanism for medical information/applications sharing.<br>The system shall provide a mechanism allowing medical doctors or institutes to register their recommended medical |

| | |
|---|---|
| | information/applications.<br>The system shall provide a mechanism allowing medical doctors or institutes to enquiry and discover past medical information/applications.<br>The system shall provide a secure mechanism for subscription, authorisation, and authentication for the registration, query and discovery of medical information and application.<br>The system shall provide a mechanism that allows mutual authentication between the e-health supporting platform and medical expert system. |
| Other information specific to the use case | |

# Appendix I:

## Results of a survey to identify use cases of e-health services with M2M

The objectives of this survey on e-health use cases are the identification of which use cases of those addressed by the ITU-T FG-M2M correspond to use cases of "e-health services with M2M" (e-health services enabled by M2M), as well as the identification of general use cases of e-health services contained in documents from other SDOs, according to those identified in the FG M2M Deliverable D0.1 [b- ITU-T FG M2M D0.1].

NOTE - The use cases actually contained in the present document are not sufficient in terms of relevant use cases for developing countries. Therefore, use cases for developing countries (in particular from mHealth Alliance) contained in Deliverable D0.1 [b- ITU-T FG M2M D0.1] have been also analyzed in the survey.

The results of the survey are described in the attached spreadsheet "D11att1.xlsx".

The survey comprises three main components: 1) e-health services set (columns A-H), 2) e-health M2M suitability (column I) and 3) e-health related use cases (columns J-Y).

1) Set of e-health services

The set of e-health services used for this survey is based on examples of common e-health service and application components as identified in the National eHealth Strategy Toolkit 2012 published by the WHO and ITU (see [b-WHOITU toolkit]).

2) e-health M2M suitability

The e-health applications and services with M2M are characterized by the usage of the so-called "e-health M2M framework" feature as described in clause 7 of Deliverable D0.2 [ITU-T FG M2M D0.2]. The usage of this feature indicates that the e-health application or service under consideration uses at least a capability per layer of the capabilities located in each of the four layers identified in the IoT reference model [b-ITU-T Y.2060]: "Application layer", "Service support and Application support layer", "Network layer" and "Device layer".

3) e-health related use cases

The use cases described in this document and in D0.1 (use cases from other groups or organizations) [b- ITU-T FG M2M D0.1].

The following process is used to generate the survey results.

Each use case (component 3) is at first analyzed to identify if it involves one or more of the e-health services (component 1).

For each use case involving one or more of the e-health services, the related e-health services are analyzed according to the e-health M2M framework feature (component 2): the e-health services matching the e-health M2M framework feature constitute "e-health M2M services". Consequently, the related use cases can be considered as use cases of e-health services with M2M.

The use cases whose related e-health services don't match the e-health M2M framework feature are just considered as use cases of e-health services.

NOTE - It is for further study if the above process can be used as a general method for other use cases not considered in this survey and for future use cases.

## Bibliography

[b-ETSI Use cases] ETSI (2013-09), *Machine to Machine Communications (M2M); Use cases of M2M applications for eHealth*, ETSI TR 102 732 V1.1.1

[b-epsos Use cases] epsos (2012), *Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription, D1.4.1 EED SERVICES including use cases for all services, Use-cases description*

[b-GSMA reference] GSMA (2011), *Connected Mobile Health Devices: A Reference Architecture, Version 1.0*

[b-ITU-T Y.2060] ITU-T Recommendation Y.2060 (2012), *Overview of the Internet of Things*

[b-ITU-T Y.2065] ITU-T Recommendation Y.2065 (2014), *Service and capability requirements for e-health monitoring services*

[b- ITU-T FG M2M D0.1] ITU-T FG M2M Deliverable D0.1 (2014), *M2M standardization activities and gap analysis: e-health*

[b-mHealth Alliance Evidence] mHealth Alliance (2013), *mHealth and MNCH: State of the Evidence*

[b-mHealth Alliance Leveraging] mHealth Alliance (2012), *Leveraging Mobile Technologies to Promote Maternal & Newborn Health: The Current Landscape & Opportunities for Advancement in Low-resource Settings*

[b-UN Health info] United Nations Foundation (2011), *mHealth Alliance and Vodafone Foundation, Health information as Health Care*

[b-UN mHealth for Dev] United Nations Foundation and Vodafone Foundation (2008), *mHealth for Development, The Opportunity of Mobile Technology for Healthcare in the Developing World*

[b-UN Wireless] United Nations Foundation and Vodafone Group Foundation (2008), *Wireless Technology for Social Change: Trends in Mobile Use by NGOs*

[b-WHOITU toolkit] WHO and ITU (2012), *National eHealth Strategy Toolkit*

_____

Printed in Switzerland
Geneva, 2014