सत्यमेव जयते

TECHNICAL REPORT

M2M ENABLEMENT IN

REMOTE HEALTH MANAGEMENT

TEC-TR-S&D-M2M-004-01

M2M HEALTH WORKING GROUP

ISO 9001:2008

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

RELEASE 1.0

MAY 2015

Revision History

Date	Release	Document No.	Description
12-05-2015	R1.0	TEC-TR-S&D-M2M-004-01	Technical Report on M2M enablement in Health Sector

Important Notice

Individual copies of the present document can be downloaded from **http://www.tec.gov.in**
Users of the present document should be aware that the document may be subject to revision or change of status.
Any suggestions/comments may please be sent to **m2mreports.tec@gov.in**

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

रवि शंकर प्रसाद
RAVI SHANKAR PRASAD

सत्यमेव जयते

मंत्री
संचार एवं सूचना प्रौद्योगिकी
भारत सरकार
MINISTER
COMMUNICATIONS & IT
GOVERNMENT OF INDIA

Message

I am glad to note that Telecommunication Engineering Centre is bringing out Technical Reports on M2M enablement in Transport, Health, Power and Safety & Surveillance sectors and a Report on M2M Gateway & Architecture.

M2M communications is going to change the way the humans live and control their surrounding as well as various social and economic sectors operate. It is expected to improve the efficiency of various sectors such as Automotive, Health, Power and Safety & Surveillance etc. by transmitting the information electronically and automation of information processing. It will help in providing quality sevices to our citizens.

I am confident that the Technical Reports will help in developing specifications/ standards to be used in India and opportunity of manufacturing wide variety of devices and other products in India. I congratulate TEC and all concerned for this commendable work which is very timely, and wish them success in all their endeavors.

(RAVI SHANKAR PRASAD)

Room No.: 105, Sanchar Bhawan, 20, Ashoka Road, New Delhi - 110001
Phone : 91-11-23739191, 23372177 Fax : 91-11-23723330

राकेश गर्ग
सचिव
RAKESH GARG
Secretary

सत्यमेव जयते

भारत सरकार
Government of India
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
Ministry of Communications &
Information Technology
दूर संचार विभाग
Department of Telecommunications

08th May 2015

Message

I am extremely happy to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a Technical Report on Gateway an Architecture of M2M communications.

2. While Government started the work of developing roadmap for M2M communications in India, TEC at the same time initiated the work of identifying technical requirements of Automotive, Health, Power, Safety and Surveillance sectors. As there has been active participation from stakeholder of each sector, the reports have taken into account the ground level status and requirement for M2M enablement.

3. India has to make strides in making its various sectors smart for which quick adoption of M2M is the necessary. These reports will help stakeholders in development and finalization of sectors specific plans for adoption of M2M.

4. I appreciate the efforts put in by Telecommunication Engineering Centre in bringing out these reports. I wish them success in all their endeavours.

(Rakesh Garg)
Secretary(Telecom)

संचार भवन, 20, अशोक रोड़, नई दिल्ली-110001 / Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001
Tel. : 011-23719898, Fax : 011-23711514, E-mail : secy-dot@nic.in

सत्यमेव जयते

सदस्य (प्रौद्योगिकी) एवं
पदेन सचिव, भारत सरकार
Member (Technology), Telecom Commission &
Ex-Officio Secretary to Govt. of India
Tel : 23372307 Fax : 23372353

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, २०, अशोक रोड़,
नई दिल्ली.११०००१
Government of India
Ministry of Communications & Information Technology
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road,
New Delhi-110001

Message

I am happy to note that Telecommunication Engineering Centre (TEC) is bringing out technical reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report of Gateway an Architecture of M2M communications. We are aware that adoption of M2M communication will inter-alia, lead to enhancement in the efficiency of various sectors of society and economy.

Need for improvement in efficiency in various socio-economic sectors has been felt for a long time and some efforts in this direction have also been made whereby M2M based systems have been deployed. However, the solutions which have been implemented are generally based on propriety platforms. However, to achieve smart processes and functioning in all the sectors, interoperability of devices/ platforms/ applications is necessary which entails adoption of open standards.

The technical reports of TEC are a good step in this direction and will certainly help various stakeholders to take preparatory steps in their respective sectors for future adoption of M2M communications.

S. S. Sirohi

(S.S. Sirohi)
Member (T)
8.5.2015.

सलाहकार (प्रौद्योगिकी)
Advisor (Technology)
Tel. : + 91-11-23718460
+ 91-11-23036317
Fax : + 91-11-23329525

सत्यमेव जयते

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, नई दिल्ली-110 001
Government of India
Ministry of Communications &
Information Technology
Department of Telecommunications
Sanchar Bhawan, New Delhi-110 001

A.K. Bhargava
Advisor, DoT

Message

I am pleased to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report on Gateway & Architecture of M2M communications.

TEC has taken timely action to take up the work of study and preparation of the Technical Reports in the Automotive, Health, Power, Safety and Surveillance sectors. The Reports have been prepared to be released along with the National M2M roadmap by virtue of relentless efforts of TEC and its Working Groups consisting of stake holders.

M2M communication is an opportunity for India not only to keep pace with the world but also to march ahead in development of specifications of new products consisting of Devices, Gateways and Platforms meeting the Indian requirements, though of course, in sync with the standards.

I appreciate the efforts of Telecommunication Engineering Centre specially its S&D Division and all the Working Groups for bringing out these technical reports in a very timely manner. I wish them success in all their endeavours.

(A.K. Bhargava)

AJAY KUMAR MITTAL
वरिष्ठ उप महानिदेशक
Sr. Deputy Director General
Tele : 23320252 Fax : 23329088
e-mail : srddg.tec@gov.in
www.tec.gov.in

सत्यमेव जयते

भारत सरकार
दूरसंचार विभाग
दूरसंचार इंजीनियरी केन्द्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली–110001
Government of India
Department of Telecommunications
Telecom Engineering Centre
Khurshid Lal Bhawan, Janpath, New Delhi-110001
ISO 9001:2008

FOREWORD

Telecommunication Engineering Centre (TEC) is an organ of Department of Telecommunications (DoT). It provides technical support to DoT. TEC develops technical specifications of products for use in telecom networks. It carries out technology studies and proactively takes up development of specifications based on such studies Development of specifications is a transparent process with active participation of stakeholders. Certification of telecom products is also one of its activities.

M2M Communication is an area which has rapidly attracted attention of world over, primarily due to its enormous potential in bringing about fundamental changes in the delivery and use of services in almost all sectors of economy and society and the quality of human life.

M2M systems have been in use for some time past, e.g. in automotive sector. However, the use of technology/devices/application is generally proprietary in nature as standards have started involving in the recent past. We are aware that variety of social and economic activities are interdependent and in today's digital world, it is possible to link them through networks and applications to achieve enhancement in efficiency and development of new services. This is possible only when there is interoperability among devices/networks/applications. This requires standardization and development of harmonized specifications.

Towards achieving this objective, TEC in consultation with stake holders from government, industry, standards bodies and sector users, took up study of four sectors to begin with namely Automotive, Health, Power, Safety and surveillance. Four working groups (WG), one for each were formed with the participation from stakeholders as mentioned above. As it is also necessary to work out architecture for M2M domain and also service delivery models, Gateway and Architecture WG was also formed. All the groups have overwhelming participation. Chairmen, Rapporteurs & Co-rapporteurs have been elected by the WGs themselves. Joint Working Group is chaired by Sr. Deputy Director General and Head TEC.

These groups have carried out use case studies and analysis for respective sectors. Beginning the year 2014, these groups have worked relentlessly. This can be gauged from the fact that there were about 50 conference calls and four Face to Face (F2F) meetings combined of all groups and lot of many interactions within the groups. Services and Development (S&D) Division of TEC coordinated and managed the entire activity of formation of working groups, holding meetings, preparation of the reports etc.

The reports contain use cases in the sectors & their technical analysis, key challenges in implementation and the way forward. Suggestions for way forward those have emerged, require action by various stake holders as well as by TEC and the Working Groups. TEC and the Working Groups will continue further work and it is planned to bring out next release of Technical Report after further study as early as possible.

I express my sincere thanks to all the Chairmen, Rapporteurs and Co-rapporteurs and members of the Working Groups as well as the participating stakeholders as organization and as persons whose enthusiastic support and untiring efforts have made it possible to bring out these detailed reports.

Ultimate aim is to identify the areas for development of standards, harmonize Indian standards with international standards and development of product specifications ensuring interoperability. India being a big market for M2M, there is enormous potential of manufacturing devices and networking products for M2M in India. Let us all join hands to become part of the 'Make in India' programme of the Government of India.

I hope that the report will provide guidance to the stakeholders to plan standardized deployments in the concerned sectors. I also hope that the stake holders will provide their continued support to TEC to carry out further work in M2M domain. We will be enriched in our work through valuable suggestions from any quarter.

(A.K.Mittal)
Sr. Deputy Director General & Head
Telecom Engineering Centre

Contents

List of Contributors i
Executive Summary iii
1. Introduction 1
2. What is M2M Communication? 3
3. Conceptual description of M2M communication in Health Monitoring 4
4. Typical M2M application in Healthcare 5
5. M2M Healthcare Use Cases 6
5.1. Remote Patient Monitoring (RPM) 6
5.2. Rural Health 7
5.3. Patient Identification 10
5.4. Assisted Living 11
5.5. Smart Wearable Devices 12
5.6. Ambulance Management System/Mobile Care 13
5.7. Video Conferencing 15
5.8. Medical Assets tracking 16
5.9. Clinical Monitoring 18
5.10. Radiology data transfers 18
5.11. Remote Drug Delivery 18
5.12. Remote Robotic Surgery 18
5.13. Laboratory Information System 19
5.14. Summary of Use Cases 19
6. Communication Technologies 21
7. International Organizations working on Health standards 23
7.1. ISO Standards 23
7.2. HL7 (http://www.hl7.org/implement/standards/) 23
7.3. DICOM (http://medical.nema.org/Dicom/about-DICOM.html) 23
7.4. Personal Connected Health Alliance (PCHA) 24
7.5. Continua Health Alliance 24
7.6. ITU- International Telecommunication Union 25
7.7. Electronic Health Record Standards for India 26
7.8. BIS Standards for Health 26
8. Key Challenges 28
9. Way forward 28
10. References 29
11. Annexure 1 30

11.1. Use case Remote Patient Health Monitoring 30
11.2. Use Case Ambulance Patient Monitoring System 43
11.3. Use Case: Video Conferencing System 54
11.4. Use Case Remote Drug Delivery System 61
12. Abbreviations 69

Figures

Figure 1: Proportion of population aged 60 or above, World and developed regions, 1950-2050 1
Figure 2: M2M Concept 3
Figure 3: M2M framework for Health Monitoring 4
Figure 4: Global Healthcare M2M Connection by Region; 2013-2023 (Machina Research; 2014) [10]. 5
Figure 5: Remote Patient Monitoring Concept 6
Figure 6: Remote Health Monitoring Architecture by CONTINUA HEALTH ALLIANCE (Source: ITU-T TECHNICAL PAPER HSTP-H810, JULY 2014) 25
Figure 7: Remote Patient Monitoring [source: ITU-T Focus Group on M2M Service Layer Document [3] 26
Figure 8 : Information Flow In Remote Patient Monitoring 32
Figure 9 : Remote Patient Monitoring Concept 32
Figure 10: Remote Patient Monitoring Concept 35
Figure 11 : Remote Patient Monitoring [source: ITU-T Focus Group on M2M Service Layer Document [3] 36
Figure 12: Video Conferencing Illustration 56
Figure 13: Remote Drug Delivery Illustration 64
Figure 14 : Generalized View Of Microchip Technology 64

Tables

Table 1: Shortfall of Doctors, Hospital Beds & Nurses 2
Table 2: Communication Technologies 21
Table 3: Comparison of the Communication technologies 21
Table 4: ISO Standards 23

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	E-mail Address
A. K. Mittal	Sr. DDG	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Secretariat:

Name	Designation	Organisation	E-mail Address
Sushil Kumar	DDG	Telecommunication Engineering Centre (TEC)	ddgsd.tec@gov.in

C. Working Group (WG) Chairs:

	Name	Designation	Organisation	E-mail Address
Chairman	Alok Kumar Mittal	Group Manager	STMicroelectronics	alok.mittal@st.com
Rapporteur	Ananda Sen Gupta	Founder & CEO	Trackmybeat Healthcare (India) Pvt Ltd	ananda.sengupta@trackmybeat.com
Co-Rapporteur	Parmatma Rai	Director (CL)	Telecom Engineering Centre	prai64@rediffmail.com

D. Primary Authors:

Name	Organisation
Alok Kumar Mittal	STMicroelectronics
Ananda Sen Gupta	Trackmybeat Healthcare

E. Contributors:

S.No.	Name	Organisation
1.	Dinesh Chand Sharma	EU Standards
2.	Ms. Ishrath Humairah	Tech Mahindra
3.	Prof. K. Ganapathy	Apollo Tele Health Services
4.	Dr. Neena Pahuja	DeitY
5.	Rajendra Pratap Gupta	Chairman, Personal Connected Health Alliance India
6.	Santhosh Kumar Madathil	Wipro Technologies
7.	Sumit Dhingra	Reliance Industries Ltd.
8.	Rahul Kumar	TCIL
9.	T.P. Mallik	i-Diagnosis Telematics Private Limited
10.	Ashish Kumar Mishra	Clarity Medical Pvt. Ltd.
11.	Mani Rajakannu	TCS
12.	Rahul Kumar	TCIL
13.	Ms. Mevish P Vaishnav	India Innovation Working Asia

F. Joint Editorial Team:

S.No.	Name	Organization
1	A K Mittal	TEC
2	Sushil Kumar	TEC
3	Rajendra Pratap Gupta	Chairman, Personal Connected Health Alliance India
4	A.Bhattacharya	C-DOT
5	Anuj Ashokan	TTSL
6	Sriganesh Rao	TCS
7	Niranth	Huawei
8	Hem Thukral	India Smart Grid Forum (ISGF)
9	Alok Kumar Mittal	STMicroelectronics
10	Rohit Singh	Smart 24x7 Response Services
11	Sharad Arora	TTSL
12	Rajeev Kumar Tyagi	TEC
13	Raunaque Quaiser	STMicroelectronics

Executive Summary

Health of the citizens is a serious area of concern for countries around the world, as the reach of health care services remains limited, due to variety of constraints. Benefits of advancement in medical sciences and related technologies, as a result, are not available to all. Use of telecommunication network/services for e-health has improved the accessibility to health services only in a limited way so far.

Non-communicable diseases (NCD) such as hypertension, diabetes and cardiovascular diseases affect more than 100 million people in India today. NCD cause more than 40% of hospital stays and nearly 60% of the total number of deaths in the country, thus resulting in severe financial strains both for the individuals as well as the country's health system.

Most of these diseases cannot be addressed by any quick measures, but require regular monitoring and lifestyle management. Given the limited affordable medical infrastructure, and large share of the population of India living in rural areas with very limited access to medical personnel or facilities, it is imperative that technology be used appropriately to help in remote management of health of the masses.

This document contains technical report of Telecom Engineering Centre on health sector. It introduces the subject with brief illustration of M2M communication and its framework for health monitoring.

The M2M WG of Health, through detailed deliberations and discussions with key stakeholders such as health service providers and solution vendors, has created list of relevant use cases for health care for India, e.g. remote patient monitoring, rural health, wearable devices, clinical monitoring, remote robotic surgery etc. The WG has also analysed existing international standards, and the report has listed and briefly described the standards. Standardization will help in interoperability of devices and networks and thus lead to economies of scale.

In the end, way forward has been suggested wherein action points on various aspects like adoption of standards, development of devices, certification mechanism etc. have been brought out.

1. Introduction

The United Nations estimates that 841 million humans were 60 years old or more in 2013 (about 12% of the world's population), with 120 million of those being 80 or above (1.7% of the total). In 1950, just 8% of the world's population was 60 or older (205 million). The U.N. predicts the 60-and-above segment will reach 21% of the world's population in 2050 (over 2 billion humans) as shown in figure-1 [1], with 4.1% (about 392 million) being 80 or more that year.

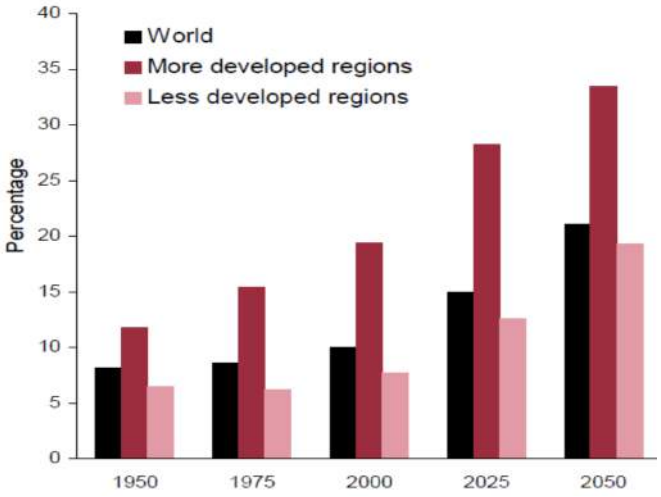

FIGURE 1: PROPORTION OF POPULATION AGED 60 OR ABOVE, WORLD AND DEVELOPED REGIONS, 1950-2050

The older population is growing faster than total population in almost all regions of the world. The growth rate of older population is estimated to be 1.9% which is higher than the growth rate of the total population [1]

The aging population increases the need for chronic disease management, and that means cost pressures will grow in healthcare in the years ahead.

Rural and urban divide in India:

- Rural population is spread over 6,40,000 villages.
- 11% of all episodes in rural areas and 10 % in urban areas do not receive healthcare.
- 12 % of people living in rural areas and 1% in urban areas have no access to a health facility.
- Urban India has 31.60 % population but has 74 % hospital (10,13,017) beds (CBHI, DGHS, MOHFW, GOI, 2012, p. 166).

Disease burden in India

As per the National Health Profile 2013 report, extensive screening was undertaken for hypertension and diabetes under NPCDCS (National programme for prevention and control of cancer, diabetes, CVD and Stroke), covering around 108 million people, and 5.99% of the people were suspected with diabetes and 4.93% were detected with hypertension. In the urban slums, of the people screened, 10.87% were suspected with diabetes, and 13.09% were detected with hypertension.

In 2004, 4.8 million (59.4 percent) of the estimated 8.1 million deaths in India were due to Non-Communicable Diseases (NCDs). (Mahal A, Karan A & Engelgau M, 2010). It is important to consider the fact that about 24 % of these deaths happened in the productive age group of 35-64 years

NCDs accounted for nearly 40 % of all hospital stays and 35 % of all out patient visits in 2004 (Mahal A, Karan A & Engelgau M, 2010 p. 40). If we assume that in 2004, all the care-givers and sick individuals above the age of 15 years were productive, then it yielded an annual income loss from

NCDs of one trillion rupees. The estimates further state that the GDP in 2004 would have been 4-10 percent higher if all the NCDs were eliminated (Mahal A, Karan A & Engelgau M, 2010).

TABLE 1: SHORTFALL OF DOCTORS, HOSPITAL BEDS & NURSES IN INDIA

Shortfall	Reference period	Source
1.75 million hospital beds	2025	E&Y
6 lac Doctors	2023	ICMR
2400000 Nurses	Needed by 2012	WHO

In 2050, the population of India would be 1.69 billion about 500 people per square kilometre and senior citizens would be over 250 million. This will present a challenging scenario for the policy makers.

At present, good hospitals are available only in metros and in big cities. It is very much required to transform the healthcare with IT. IT will work as an enabler so that the doctors may advise to more patients.

Various aspects of e-health, m-health and Telemedicine are required to provide the health services in the country to bridge the gaps. They will become essential in rural areas where there is a scarcity of doctors and the hospitals.

2. What is M2M Communication?

It refers to the technologies that allow wired / wireless system to communicate with the devices of same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, meter reading, temperature etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information. A conceptual picture is shown below:

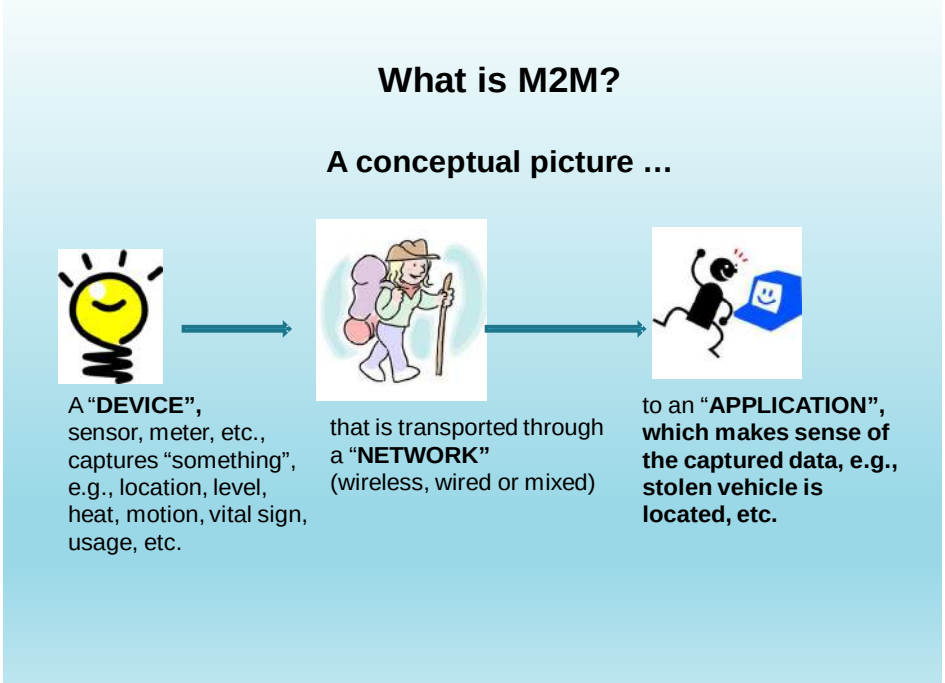

FIGURE 2: M2M CONCEPT

The enabling technologies for M2M are sensor networks, RFID, mobile Internet, wired & wireless communication network, IPv4 / IPv6, etc. In wireless communication Wi-Fi, ZigBee, 6LoWPAN, Bluetooth technology may be used for short range connectivity of devices to the gateway and GSM 2G/ 3G/ 4G or WiMAX for connecting M2M gateway to server.

IPv4 addresses are going to exhaust. Standardization and adoption of IPv6 in telecom and ICT organizations will provide an opportunity of having billions of devices which can be IP enabled and seamlessly addressable through mobile or wired broadband connections.

Internet of Things: - M2M is a subset of IoT. IoT is a more encompassing phenomenon because it also includes *Human-to-Machine communication* (H2M).

Various sectors such as Power, Automotive, Health, Safety & Surveillance and Agriculture etc. may be transformed to smart by using M2M / IoT. This will improve the quality of life.

3. Conceptual description of M2M communication in Health Monitoring

Personal Connected Health (PCH) allows service providers and patients to:

- Use technology to collect data conveniently and securely
- Communicate more frequently with little manual intervention
- Effectively monitoring and better understanding of personal health data

M2M framework for health monitoring is shown in figure-3. Wearable devices such as Pulse-Oximeter, Blood pressure meter, Glucometer, Heart rate monitoring, Smart bandage etc. may provide the vital parameters of the body and will motivate the person to remain fit. These parameters may be transmitted from device to the smart phone and further to the doctor automatically.

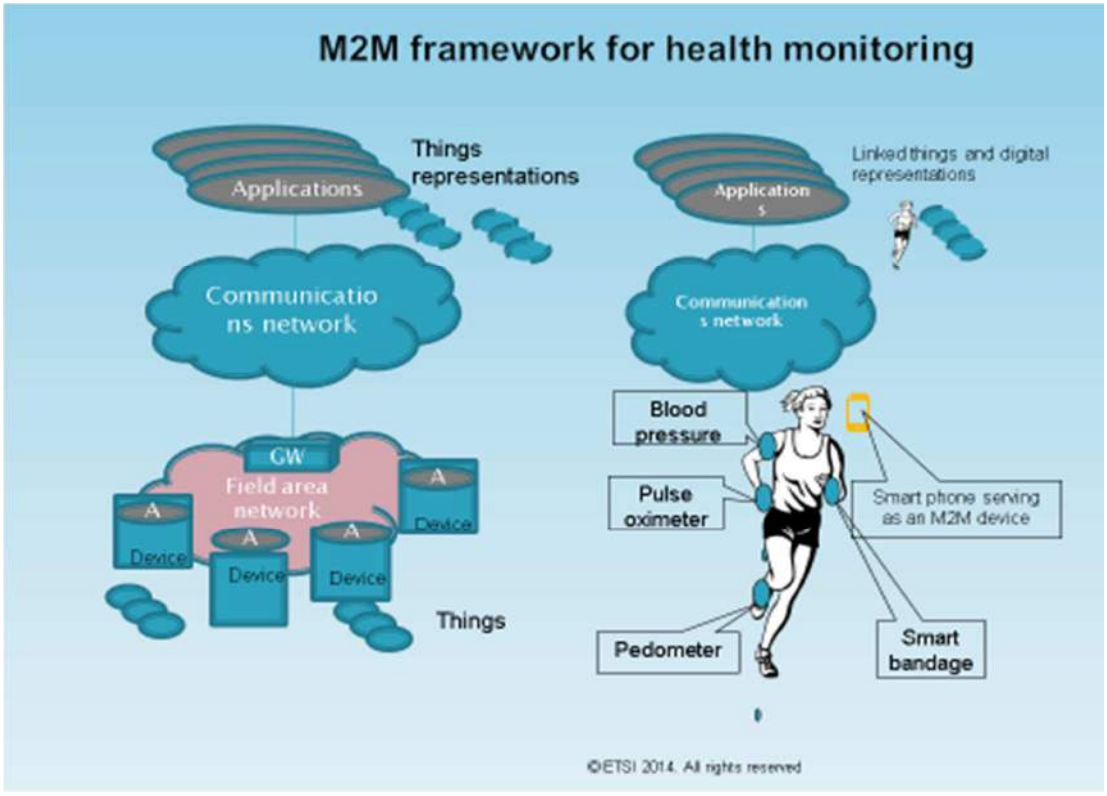

FIGURE 3: M2M FRAMEWORK FOR HEALTH MONITORING

4. Typical M2M application in Healthcare

- Remote monitoring of patients after surgery, while resting at home
- Transmission of vital parameters of a patient from ambulance to hospital
- Remote monitoring of old aged patients
- Remote consultation
- e-ICU

Using M2M communication along with ICT infrastructure, various vital parameters of patients like temperature, pulse-rate, respiration rate, heart conditions or patient location can be sent from remote locations for further analysis. This may be required for preventive healthcare, post-surgery conditions, patients from hospitals and old age people.

Machina Research forecasts that the worldwide installed base of M2M connected devices within the health sector will approach 847 million by 2023 world-wide. Out of which, North America will be the contributing 386 million connections, followed by Europe and developed countries in Asia Pacific; and the Healthcare industry will generate a total revenue of $90.9 billion from M2M technology.

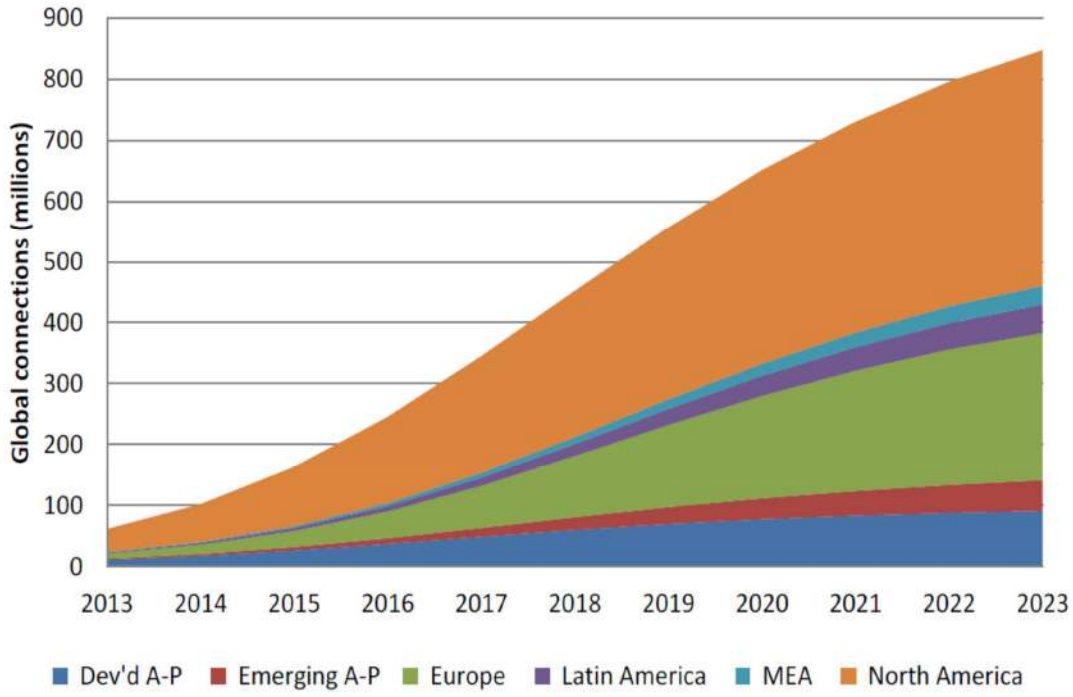

FIGURE 4: GLOBAL HEALTHCARE M2M CONNECTION BY REGION; 2013-2023 (MACHINA RESEARCH; 2014) [10]

5. M2M Healthcare Use Cases

Few typical applications that can leverage M2M platforms for healthcare are briefly described below

5.1. Remote Patient Monitoring (RPM)

Remote Patient Monitoring (RPM) is a Tele-health solution that enables monitoring of patients outside of conventional clinical settings (e.g. in the home). The patient has medical device on or close to his body which has sensors that capture the patient's healthcare/ physiological data. This data is then transferred across networks with the help of transmitters and is monitored for any abnormality with the help of software and/or by clinical experts.

By using RPM, patients after surgery can be shifted to their homes and monitored remotely. It will help in cost reduction and availability of the beds for other patients.

Increasing number of people with chronic medical conditions and senior citizens, coupled with shortage of skilled medical personnel is driving the demand for remote Tele-health services all over the world. Remote Patient Monitoring helps increase access to care and decrease healthcare delivery costs. It addresses the key concern points of the stakeholders of the healthcare system by enabling the exchange and flow of information from the patient's medical device (outside of hospital) to the clinical staff such as doctors, nurses and paramedics.

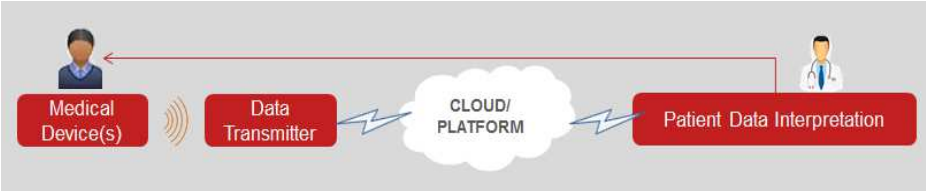

FIGURE 5: REMOTE PATIENT MONITORING CONCEPT

Components of RPM Solution:

- Sensors on a device that is enabled by wired or wireless communications to measure physiological parameters.
- Local data storage at patients' site that interfaces between sensors and other centralized data repository and/or healthcare providers.
- Data transmission and connectivity.
- Centralized repository to store data
- Diagnostic application software that develops treatment recommendations and intervention alerts based on the analysis of collected data. This may be augmented by medical experts such as doctors, nurses, etc.
- Depending on the disease and the parameters that are monitored, different combinations of sensors, storage, and applications may be deployed.

Communication channel used

- Wired communication like serial port, USB, audio port etc.

- Wireless Data Transmission Channels such as Bluetooth, Wi-Fi, GPRS, Telecom Connectivity.

Data bandwidth requirements

Data bandwidth requirements are dependent on the vital parameters used, nature of patient's data being monitored and the frequency of data transfer. Based on the range of devices available/ put to use, the data bandwidth requirements differ.

At times, the remote device or gateway device may store the data in case network connectivity is unavailable, and all data is forwarded in bulk once network connectivity is available.

The use case is discussed in detail in annexure.

5.2. Rural Health

Number of hospitals and doctors in the rural areas are not adequate at present. For providing the health services in these areas: e-health, m-health and telemedicine solutions are required to be implemented.

In a rural health, there are two typical scenarios:

- A large number of users will be catered at a health centre
  Challenges faced in Rural Health scenario are shortage of Physicians, Consultants at the PHC (Primary Health Centres), Distance to travel to nearest PHC, Health record generation and upkeep for future visits. M2M Health provides a way to manage all these and reduce paper work and at the same time give visibility and traceability of the data at all levels.

  PHCs are equipped with Medical Devices integrated to a computer or a Health Kiosk with communication channel to transfer data as well as live audio, video for a Physician to consult remotely. Patient records are stored locally as well as synched with a backend server on a regular basis with unique patient ID.

- An ASHA(Accredited Social Health Activists) or Anganwadi worker will visit individual user's home to help monitor health

  In either case, the monitoring will be done using multi-user personal health devices.

  The solution comprises of a mobile device (phone or a tablet) connected to the Medical Device with wired or wireless interface and enabled with Biometric ID, Camera and GPS with a mobile network connectivity to the backend Server where data can be submitted individually or in a consolidated manner. Patient ID can be validated through Aadhaar.

  In addition, Current process involves collecting the readings manually on paper and also on the Health card provided to patients with details of the patient, (name, gender, age etc) and Health readings along with the address. The same data needs to be transferred by the Health worker to a register and consolidated at Office.

  M2M allows complete automation of this workflow with accurate data recordings with GIS mapping, time stamp and automatic transfer to central server where individual and consolidated

reports, demography wise is available. This avoids paper work, less error prone and live update of data with visibility to the Health inspector at all times.

Brief information about this use case is as follows:

Type of Device: Class 1/2/3

- The typical devices used will be type 1 and type 2. In special cases, there may be type 3 devices at a health centre.

Communication channel used

Here the full connectivity scenario applies, as described in the Continua Health connectivity diagram.

If the device communicates through a gateway device such as a tablet/phone/PC, then the connectivity between the device and the gateway device will be Bluetooth/ZigBee/NFC/USB. The gateway device will connect using WAN connectivity mechanisms to the central server on the cloud.

Data bandwidth requirements

The data bandwidth requirement for the basic health data transfer is low. However, if a database has to be downloaded locally, a one-time registration process will be required for the gateway device which may have to hold a local database with some minimum information describes previously to identify the user uniquely. For that one time registration process, medium quantity of bandwidth may be necessary, but it can also be done over a slower link since it is a one-time interaction.

Compliance to standard

Suitable ISO and BIS standards

Deviations from standard

The user identification process will be unique for Indian rural scenario, which may not apply in other situations (and in other countries).

Challenges

The key challenge here is user identification. There must be a way of uniquely identifying the user of the device, so that the data can be stored accurately against the correct user in a centrally located server.

There are two options here:

- Have the user identification to be in-built in the device - where the device itself exchanges data with a central server and has a process to identify the user. For example, the device has a finger scanner which then connects to central server, which responds with the matching user identification.

In this case, the device will directly connect to the network (hence will have a SIM card) and will have an IP address.

- Have the user identification be done through a gateway device - tablet or phone with SIM (with IP address). In this case, the tablet may have either a finger scanner for greater accuracy, or for cheap practical use, have a database of users, which the health personnel can select user identification from. The minimum requirement in case of a database will be to display user's name, father's name and/or address, so that the user can be chosen uniquely. In case, Aadhaar has been implemented, that could become an identifier through local database. Technically, a personal computer can also be used as the gateway device to communicate with the device and central server.

Creating an accurate user database is a substantial effort in a rural scenario. Hence firstly, user data collection is necessary, either from census data or data from other local authorities such as Panchayat and others. Once that is done, this data has to be uploaded to a central location, which the local gateway or device has to access and match with.

Alternative is to use Biometric ID (finger print) with validation to Aadhaar database. The workaround that has been described is to have some basic user information available, but even there the data has to be collected in advance. Adding new users will also not necessarily be an easy process.

Criticality of QoS

For type 1 and type 2 device usage scenario, the QoS requirement will be low as the data collected is for longer term monitoring scenarios, and the volume of data is also small.

Ownership of data

The ownership of data will of course lie with the user. However, since the rural user is not a technologically advanced user, the Ministry of Health, Government of India, will have to be involved in the processes and database management.

Patient Safety Requirements

The devices will have to follow standard quality and safety standards as per BIS or other applicable international standards.

Initiatives by Government of India

The key challenge here is user identification. Every user of the device must be uniquely identified, so that the data can be stored accurately against the correct user in a centrally located server. For this biometric identification with Aadhaar application may be used to identify the user of devices. Similar practice may be adopted to identify the ASHA / Anganwadi workers / compounders handling the devices.

For M2M communication, we need a reliable communication network. As per TRAI report of March 2015, urban India has reached a tele-density of 146.5%, whereas rural India stands only at 46%. There are approx. 175 million subscribers accessing internet through wireless phones. Out of this

approximately 10 % to 15% subscribers may be from rural areas. As per census 2011, India was having population of approx. 1.21 billion, which at present it may be approx. 1.23 billion. It is worth mentioning that 62% of the Indian population is living in rural areas (0.65 million villages) whereas only 32% in urban areas. It shows a big Urban – Rural digital divide. This gap is required to be filled for extending urban services in the rural areas through ICT (Information and communication technology) network.

ICT network is required to be improved in the rural areas. Government of India has already approved a project called NOFN (National optical fiber network) with plan outlay of Rupees 20 Thousand Crores (US $3.3 Billion) to create a backbone for telecom and IT services in the rural areas. In this project, 2.5 lakh Village Panchayats will be connected on optical fiber cable and each Village Panchayat will be provided 100 Mbps data link. Project is likely to be completed by 2017.

Out of 100 Mbps on this bandwidth, various services such as Tele-medicine, Tele-education, e-health, High speed internet, e-Governance, e-Panchayat, and Aadhaar applications may be provided. Telecom service providers may hire the bandwidth for connecting mobile BTS and expand their network in the rural areas.

The rates of smart phones are reducing continuously and many smart phones are now available in less than Rs. 5000/-, it is expected that rates will further reduce and thereby increasing the affordability of smart phones. Cheaper smart phones with long battery life will increase the tele-density and the internet usage in the rural areas.

These activities may revolutionize the telecom services in the rural areas. Rural masses may be benefitted by use of various mobile apps and also the M2M services.

5.3. Patient Identification

The Patient Identification is needed for correct logging of the data in the Electronic Health Record systems. This is important for the Rural health scenario and also otherwise for logging correct data for patients.

The Patient identification and parameters for data logging can be done by the following:

- Aadhaar number: In India, a unique number is provided by UIADI (Unique Identification Authority of India) to each citizen.

  Electronic Health Record Standards for India recommends:
  UID as a unique (primary or secondary) patient identifier. The UID should be used to identify a particular patient across all organizations (and their EMR systems); Aadhaar number is recommended for use in EMR as either the primary or secondary, where the primary is an internal unique health identifier used by the healthcare provider organization. [15]

- RFID: Near Field communication tag unique to the user can be issued. It will contain a unique ID for the user and when this tag is put on the authentication device, a unique number is used to get the Patient identity etc. This can be good for Primary healthcare system

- Iris Type: The eye scan can be used as unique identity. However, the technology still needs to be deployed on mass-scale

- Mobile Phone number: Users phone number can be used as unique ID. Though the Mobile phone penetration in the population is high the challenge is that all people do not have the mobile. Also, people do change the mobile phone numbers. In this case, the portability of the records to the new number needs to be done

- Smart cards: Smart cards can be used for the unique ID. These can be ISO7816 compatible. The health-system must have the smart card reader input.

Each user must have a unique Health card which will help in identification.

5.4. Assisted Living

Elderly and other vulnerable people requiring close medical supervision can lead an independent life through Assisted Living technologies powered by remote connectivity.

Following Scenarios exist specific to elderly care

- Fall condition: This is to detect if the user has fallen down and unable to get up due to some injury. The message needs to be sent to nearby Family members/Care Giver/ Hospital.
- Vital Signs monitoring: There is a need to monitor the health parameters on a regular basis and alert the health-care services in case of any health related alarms.
- Routine check-up: There may be a need to send routine check-up reminders and appointment settings from time to time as applicable.
- Scheduler for Medicine reminder: Regular medicines need to be taken for chronic diseases and reminders need to be sent from the server to the user.
- The reminders can be managed locally also by a Smart-phone App or other mechanism. However, usage of medicines needs to be recorded. There are Pill boxes and Pill strips under design and development in developed countries, which can log the time when a pill is taken.
- Activity monitoring: In case of general prescription for physical activity of the user, there may be a need to monitor of minimum steps taken and calories burnt per day.
- Home Dialysis: Home Dialysis is an upcoming requirement since many Elderly people need to go regularly for the Dialysis. The dialysis can be done at home and reports can be generated for remote monitoring and consultancy.
- Geo Fencing: This may be required to monitor the movement of specific elderly users having specific problems like dementia. The geo fencing applications are required to either manage the users' movement in and around home or to track their movement when outside home.

Type of Device: Class 1/2/3

- Device Type 1 & 2
- Only Post Surgical : Type 3

Communication channel used

- BT/ BTLE/ ZigBee / Low Power RF in ISM Bands: This is mostly to allow user mobility in the home
- USB: Wired connections only for specific parameter logging from specific Instruments
- 2G/3G/4G/ Wi-Fi/Broadband: for Server Connectivity through Gateway

Data bandwidth requirements

- Low data rate for Personal care devices

Security requirements

- Data shall be encrypted

Privacy

- Data access to be provided to user, hospital, doctor
- Based on user agreement: It can be provided to Family members, Care giver, Insurance Companies

Compliance to standard

- Kindly refer to Continue Block diagram for the devices like: “Independent Living Activity”, “Activity Monitor” and “Medication adherence”

Criticality of QoS

- Quality of Service is critical like in the earlier cases especially on any Fall detection, Vital recordings above set thresholds.

Ownership of data

- There needs to be a central health repository which patients can rely on to avoid dependency for the patient data on multiple Hospitals. Even though data ownership is normally with patients, in case of elderly care, it may be necessary to have the data accessible to caregivers or health service providers.

Challenges

- In current scenario the patients are fully dependent on Hospitals to provide any sort of medical care or long term monitoring services like this. The available solutions are also expensive. There is a need to have Care providers to set up and run these services economically with minimal and needed support / tie up with Hospitals.

5.5. Smart Wearable Devices

The purpose of the smart-wearable devices is to monitor health of the user while being worn by the user on the body. The recorded parameters can be stored on the memory embedded in the design or transferred to the Aggregation manager

These devices need to be battery operated since they need to be carried and hence low-power consuming.

The Smart wearable devices include the followings type. This list is not to be considered exhaustive.

- Pedometer
- Wearable ECG Device or Patch

- Pulse-Oximeter
- Heart-Rate monitor
- Glucose monitor
- Emergency alert device
- Smart Glasses, etc.

Type of Device: Class 1/2/3

- Device Class will be 1 & 2
- In some cases like ECG, it can be Class-3 Type

Communication channel used

Generally Low-Power connectivity channel has to be used for communications, to take power usage requirements as well as radiation concerns, into account. These would include the following technologies

- Bluetooth Low Energy
- ZigBee
- Low Power Radio
- High bandwidth products e.g. a 12 lead ECG with high sampling frequency and data streaming may need standard Bluetooth

Data bandwidth requirements

- Generally the devices shall consume low to medium bandwidth only (approximately few 100 Kbps).

Compliance to standard

- The specific approved profiles of BTLE, BT, NFC can be used for communication.

Challenges

- The data communication to be in small bursts of time to save the Battery consumption.
- Some companies have already launched their Smart-Watches and Smart-Wearables. The protocols used in these devices are to be mentioned (Proprietary/ Specific standards).

Criticality of QoS

- Since these devices to be used in Personal Area Network, the QoS shall be good from Device to the Aggregation Manager.

Patient Safety Requirements

- The radio transmission shall not cause any harm on the humans. These are already taken care when using standard communication technology.

5.6. Ambulance Management System/Mobile Care

Following are the aspects of M2M in Ambulance or Mobile care

- Ambulance Fleet Management
    - This is to save time and reach the patient within “Golden hour”.

    - Provide necessary traffic management for fast movement of the Ambulance.
- Vital parameter transfers
    - Providing the patient information and vitals to the hospital and care givers. This saves time when the patient reaches the hospital.
    - Patient's vital data covering temperature, blood pressure, pulse rate, glucose level can be sent to hospital while the patient is being moved to save precious time. This can be achieved by equipping the ambulance with tele-treatment facilities.
    - Patient allergies needs to be recorded and informed to the hospital.
    - Video conferencing from moving ambulance is an additional benefit. It provides clear view of the physical condition of the patient to the doctors who can prepare for the patient. This is especially useful for the patients who met an accident.
    - ECG data from moving ambulance can be transmitted to hospitals using 12 Lead ECG equipment by using cellular communication.
    - Two-way communication is needed using UHF/VHF/ Cellular communication. This is needed to provide information to hospital about the patient condition and physical information.
- Providing necessary care to patient being carried in ambulance
    - Provide necessary information or feedback by hospital/ doctors to the paramedic staff travelling with the patient. This is done while vital information of the patient is being monitored and analysed by the medical professionals.

Ambulance Fleet Management:

- To locate the nearest ambulance when any patient calls for it. For this purpose, basic fleet management features of Vehicle Tracking System may be sufficient.
- Secondly, the hospital gets an alert when the Ambulance reaches certain distance from the respective Hospital. This time can be utilized by the hospital to get ready to receive the patient. This will include the arrangements for stretcher, wheel chair and/or the para-medical staff at the hospital. . This can be done by utilizing geo-fencing feature which is part of the basic feature of Vehicle Tracking System
- Third and the most vital requirement is that treatment of patient should start immediately on his arrival at the hospital. If possible, treatment or possible preventive measures can commence in the ambulance itself.
  This information is covered in detail in the Intelligent Transport System report

There are following types of Ambulance services

- Advance transport ambulance: Contains special equipment
- Patient transport ambulance: Not much medical equipment are there

National Health Mission website provides the details of the National Ambulance Service (NAS). Few details are mentioned below

- 29 States or union territories have the facility where people can dial 108 or 102 telephone number for calling an ambulance.
- 108 is predominantly an emergency response system, primarily designed to attend to patients of critical care, trauma and accident victims etc.

- 102 services essentially consist of basic patient transport aimed to cater the needs of pregnant women and children though other categories are also taking benefit and are not excluded.
- JSSK (Janani Shishu Suraksha Karyakram) entitlements include free transfer from home to facility, inter facility transfer in case of referral and drop back for mother and children. These are the key focus of 102 service.
- 7344 ambulances (490 Advanced Life support and 6749 Basic Life Support ambulances) are being supported under 108 emergency transport systems including new.
- 7371 ambulances are operating as 102 patient transport including new ambulances.
- 6235 empanelled vehicles are also being used in some States to provide transport to pregnant women and children e.g. Janani express in MP, Odisha, Mamta Vahan in Jharkhand, Nishchay Yan Prakalpa in West Bengal and Khushiyo ki Sawari in Uttarakhand.

  Further details are available at http://nrhm.gov.in/nrhm-components/health-systems-strengthening/emri-patient-transport-service.html

Communication channel

Since this is from moving vehicle, telecom network is mandatory to be used. Hence 2G/3G/4G channels will be used from ambulance to the Server/Hospital

Inside the Ambulance: Since the patient is stationary, wired connectivity can be used like, USB for the vital parameters devices to the aggregation manager.

Data bandwidth requirements

- Vital Signs: Low bandwidth requirement
- ECG: High bandwidth requirement

Challenges

It can be noted that inside the Automotive Vehicle, the electrical noise can be high, hence the communication channel has to be robust

The use case is discussed in detail in annexure.

5.7. Video Conferencing

The video conferencing solution, would bridge the healthcare practitioners and the patients, across geographies, to make basic healthcare services available. It could assist in monitoring with recently discharged or recovering patients, preliminary consultation with patients in locations where in-person appointments with a specialist may not be easily available, among many other possible benefits.

It could be made available for personal, public or inter/intra hospital network access.

Basic Infrastructure requirements:

- A continuous power supply, possibly achieved using a UPS or inverter, the rating and capacity of which depends on the power requirements of the overall A/V conferencing and assistive technology system.
- A reliable network infrastructure. Reliability can be improved by using an automatic network switching technology, for example, used in mobile phones, for data and roaming.
- A supervisor or guide or nurse, at the patient side of the conference, a person with a certain amount of training in assisting patients and the medical personnel at the other end, including handling equipment(s) and basic technical knowledge.
- A sufficiently good camera and microphone array and a sufficiently capable hardware and software system.
- Suitable infrastructure will be necessary also on the patent's side – high quality camera, a tablet or a computer, high bandwidth network access for video transmission

To organize the conferencing solutions, we would need a central command centre, where scheduling, QOS, patient/doctor data and technical troubleshooting, will be handled.

Patient identification may be done by Barcodes/RFID/NFC or serial nos. on hardcopy patient files, to enable quick access to review past history and such records, as agreed to, in an user agreement.

Communication channel used

USB: For specific parameter logging from diagnostic instruments and wireless network connectivity via dongle.

2G/3G/4G/Wi-Fi/Broadband/LAN: for reliable QOS and Network Connectivity with the command centre and/or the end-user devices

Data bandwidth requirements

A/V Data needs to be compressed based on a trade-off between audio/video quality, cost of compression-decompression and the infrastructure capabilities. Current industry-standard compression technologies are: H.261,H.263,H.264/MPEG-4,H.265

Buffering, caching and such mechanisms may be implemented, on both ends, to improve bandwidth utilization, ensure synchronisation of video/audio and enhance live streaming experience.

Patient and doctor generated data and miscellaneous general data, should be compressed using zip or bzip2 or one of the suitable compression algorithms, to further add to reduction in bandwidth and capacity usage.

The use case is discussed in detail in annexure

5.8. Medical Assets tracking

Description:

Asset Tracking and Device Tracking is important aspect in the health sector where all the healthcare instruments need to be tracked in hospital.

Asset tracking is needed not only to identify the location of the asset but also to understand its usage, calibration, maintenance needs, and digital data being published by these assets to central storage for record keeping.

RFID/NFC technology can play an important role in the asset tracking inside the hospital. All the hospital equipment / instruments can have a NFC passive Tag embedded with unique id of the instrument.
All the entrance/exit should have NFC transceiver which would record the movement of the medical instrument/equipment and update in the database on the hospital management system.
Whenever there is need to search the instrument/equipment the user can refer to the Hospital Management system which will provide the last location of the asset

These tags can be mounted on the movable machines like X-Ray, Ultra-Sound and similar equipment.

Medical Devices especially large equipment will have a wired or wireless connectivity through Hospital network or otherwise to communicate to central repository as well as to asset tracking and maintenance services.

Type of Device:

- Class 1 type

Communication channel used

- Near Field Communication (ISO14443 / ISO15693)

Data bandwidth requirements

- Low data rate as NFC data rate 424 kbps

Security requirements

- No security requirements as we are just tracking the movement of the Hospital equipment /instruments. The communication between the passive tag and the NFC transceiver should be secure

Privacy

- No issue of privacy.

Compliance to standard

- ISO14443 / ISO 15693

Deviations from standard

- None

Challenges

- All the existing instruments need to be tagged with passive NFC tag.
- Active Transceiver gates need to be deployed as each entrance to track the movement of the Medical instrument/equipment
- The asset management system needs to be integrated in the Hospital management system

Criticality of QoS

- It is good to have but it will add value to the Hospital and proper tracking can be done for each instrument

Ownership of data

- The database will be owned by the hospital

Patient Safety Requirements

- No hazard or threat to the patient or Hospital

5.9. Clinical Monitoring

Clinical monitoring can either be used to have an application to monitor clinical trials i.e. observing the data and safety parameters. Or it can be used to observe the effectiveness of drugs prescribed for a disease/condition of a patient over time. This would help the clinical research organization (CROs), doctors and end consumers i.e. patients. The concepts of Remote Health Monitoring will apply to this use case.

5.10. Radiology data transfers

The data from X-Ray or other Imaging system is transferred to the remote location using high-bandwidth connectivity

Today, the top MRI manufacturers offer some variation in IoT-type services including remote monitoring, predictive maintenance, and remote diagnostics. GE offers its in-site service platform; Siemens provides Siemens Remote Services; and Philips has its Philips Remote Services.

According to recent analysis from ABI Research, the install base of the connected medical imaging equipment market consisting primarily of magnetic resonance imaging (MRI) machines, computed tomography (CT) scanners, and X-ray machines is set to grow at a 17% CAGR between 2014 and 2020. [8]

The use case is discussed in detail in annexure

5.11. Remote Drug Delivery

Remote drug delivery will increase the effectiveness of treatment. To increase the patient compliance with treatment regime, which require daily mediations for long periods of time, drug delivery from an implantable microchip wirelessly controlled by a doctor would help. This technology will help to improve treatment for humans.

The use case is discussed in detail in annexure.

5.12. Remote Robotic Surgery

Remote surgical robots (tele-surgical robots) would utilize remote sensing and robotics to help surgeons perform surgeries remotely by controlling remote surgical tools and observing real-time images sent from remote surgery room. This would increase the reach of good surgeons by multiple fold and remove the distance factor from reasons for unavailability of surgery at distant places. A remote surgical robot system is mainly composed of a master console and a slave robot. Master console consists of a tool simulator, a video display, and a PC. Slave robot includes a robotic arm

control system, image processing system and a PC. Also, audio devices at both the locations would make the communication easy and chances of errors minimal.

5.13. Laboratory Information System

Laboratory information system shall provide automatic data upload on the EHR based on the Patient identity

5.14. Summary of Use Cases

The table below summarises the summary of the use-cases and their matrix for the various parameters

Use case/ Requirements	Device Type Class I/ II/ III	Communication Channel	Bandwidth requirement	Security requirement	Privacy requirement	Data Ownership	QoS requirement
Personal healthcare device (Preventive)	II	USB, BT, ZigBee,NFC, Sub-Gig, GPRS (2G/3G/4G), Wi-Fi	Low	High	High	User	High
Elderly care/ assisted living	II & III	USB, BT, ZigBee, NFC, Sub-Gig, GPRS (2G/3G/4G), Wi-Fi	High	High	High	User, Care-Giver, Hospital	High
Remote Patent Monitoring (Continuous care)	II & III	USB, BT, ZigBee, NFC, Sub-Gig, GPRS(2G/3G/4G), Wi-Fi	High	High	High	User, Hospital	High
Rural scenario (Shared Resources)	II	USB, BT, ZigBee, NFC, Sub-Gig, GPRS (2G/3G/4G), Wi-Fi	Low	High	High	User, Hospital	High
Ambulance/ Mobile care	II & III	USB, BT, ZigBee, NFC, Sub-Gig, GPRS (2G/3G/4G)	High	High	High	User, Hospital	High
Clinical monitoring	I	USB, BT, ZigBee, NFC, Sub-Gig, GPRS (2G/3G/4G), Wi-Fi	High	High	High	User, Hospital	High
Smart Wearable Devices	I	USB, BT, ZigBee, NFC, Sub-Gig, GPRS	Low	High	High	User	Low

		(2G/3G/4G), Wi-Fi					
Radiology data transfers	II	USB, BT, GPRS (2G/3G/4G), Wi-Fi	High	High	High	User, Hospital	High
Remote Robotic surgery	III	Broadband Leased lines, Optical Fibre,	High	High	High	User, Hospital	High
Tele-call centre	I	GPRS (2G/3G/4G), Wi-Fi	High	High	High	User, Hospital	High
Asset Tracking and Device tracking inside hospital	I	RFID/NFC, Wi-Fi	Low	High	High	Hospital	Low
Patient Identification	I	NFC, Biometric, Smart-card, UID (Aadhaar)	Low	High	High	User, Hospital	High
Remote Drug Delivery	III	USB, BT, ZigBee, NFC, Sub-Gig, GPRS (2G/3G/4G), Wi-Fi	High	High	High	User, Hospital	High
Video conferencing	I	GPRS(3G/4G), Wi-Fi	High	High	High	User, Hospital	High

Legends:

H: High: >1 Mbps

L: Low: ~100 bps

M: Medium: ~100 Kbps

6. Communication Technologies

Various communication technologies used for local data connectivity are depicted here as under in the table.

TABLE 1: COMMUNICATION TECHNOLOGIES

Technology	Profiles adopted World-Wide	References
USB	Universal Serial Bus Device Class Definition for Personal Healthcare Devices	http://www.usb.org/developers/devclass_docs
Bluetooth Bluetooth Low Energy	Bluetooth SIG, Health Device Profile, version 1.1.	https://www.bluetooth.org/Technical/Specifications/adopted.htm
NFC (ISO14443/ISO15693)	NFC Forum (2013), Personal Health Device Communication 1.0.	http://www.nfc-forum.org/specs/spec_license
ZigBee	ZigBee Alliance, Healthcare Profile Specification, version 1.0, revision 15.	

Other emerging technologies may be used are ANT, 6LoWPAN etc.

TABLE 2 : COMPARISON OF THE COMMUNICATION TECHNOLOGIES

Technology/ Protocol	Frequency band	Advantages	Limitations	Suitable for
Wireless				
Bluetooth Low Energy	2.4 GHz	• Mature technology • Easy to implement • Low Power • Powered by coin cell • Longer battery life	• New Technology • Will take its own time to proliferate • Small data packets	• Healthcare devices • Fitness devices
NFC	13.56 MHz	• Consumes less power • Almost instantaneous connectivity between devices • No power is required in-case of passive Tags	• Extremely short range • Expensive • Low information security • Low market penetration	• Healthcare devices • Fitness devices
Wi-Fi	2.4 GHz	• Mature technology • High home/office penetration • High data rates achievable • Easy to implement	• Limited range • Poor building penetration • High interference from other sources • Power consumption	• Base station in Health Clinics

			higher than those technologies that operate in the sub-GHz band	
ZigBee	2.4 GHz, 920 MHz, 915 MHz, 868 MHz, 780 MHz	• Full support of IEEE 11073 device specialization profile • Longer battery life from low cost coin cells for wearable devices (source: ZigBee alliance) • Wireless range up to 70 meters indoor and 400 meters outdoor (source: ZigBee alliance)	• Not widely adopted • BLE is the direct competition for ZigBee providing different modes/profiles of operation. BLE is getting adopted faster than ZigBee within short span of time	• Health Monitoring and Safety • Client Activity Monitoring • Health and Wellness monitoring
ANT	2.4GHz	• Low power mode supporting longer battery life • Adopted by major mobile manufacturer • Supports mesh capability which is an edge over BTLE	• BLE is giving direct competition to ANT as it is already supported by all the mobile manufacturer • Not all mobile Manufacturer is supporting ANT hardware • Low penetration in market is less due to present eco-system of other Wireless Technologies	• Fitness device • Healthcare device
Cellular	For India, 900 MHz, 1800 MHz, 2100 MHz and 2300 MHz is allocated.	• Mature technology • Rapid deployment • Communication modules are low cost and standardised.	• Coverage not 100% • Reliability not the best • Short technology life-cycle (2G, EDGE, 3G, LTE etc.)	• Tele-Health • Remote Health Monitoring
Wireline				
DSL	0-2.208 MHz	• Inexpensive (installation and use) • High SLA • Less installation time • Bonded DSL provides inherent redundancy	• Low data security • Lower throughput • Higher latency	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health
Ethernet	16,100,250 ,500, 600 MHz 1 GHz, 1.6-2.0 GHz	• Inexpensive (installation and use) • Excellent throughput • Low installation time • Easily scalable	• Lowest data security • Lowest SLA • Highest latency • Bursts of additional bandwidth not	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health

			possible	

7. International Organizations working on Health standards

Globally, many organizations are working towards development of standard for M2M communication in health sector. Prominent among them are listed below.

7.1. ISO Standards

TABLE 4 ISO STANDARDS

ISO Standards	Subject
ISO EN 13606	Electronic Health Communication (EHRCOM)
ISO 13485:2003	Medical devices - Quality management systems - Requirements for regulatory purposes
ISO/TR 14969	Medical devices - Quality management systems - Guidance on the application of ISO 13485:2003

7.2. HL7 (http://www.hl7.org/implement/standards/)

Health Level Seven is a standard for exchanging information between medical applications. These data standards allow healthcare organizations to easily share clinical information.

HL7 and its members provide a framework (and related standards) for the exchange, integration, sharing, and retrieval of electronic health information. These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems. HL7 standards support clinical practice and the management, delivery, and evaluation of health services, and are recognized as the most commonly used in the world.

7.3. DICOM (http://medical.nema.org/Dicom/about-DICOM.html)

The Digital Imaging and Communications in Medicine (DICOM) standard is used for the exchange of images and related information. (ISO 12052)

It defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use. DICOM is implemented in almost every radiology, cardiology imaging, and radiotherapy device (X-ray, CT, MRI, ultrasound, etc.), and increasingly in devices in other medical domains such as ophthalmology and dentistry. With tens of thousands of imaging devices in use, DICOM is one of the most widely deployed healthcare messaging standards in the world. There are billions of DICOM images currently in use for clinical care.

Since its first publication in 1993, DICOM has revolutionized the practice of radiology, allowing the replacement of X-ray film with a fully digital workflow. Much as the Internet has become the platform for new consumer information applications, DICOM has enabled advanced medical imaging applications that have “changed the face of clinical medicine”. From the emergency department, to

cardiac stress testing, to breast cancer detection, DICOM is the standard that makes medical imaging work — for doctors and for patients.

7.4. Personal Connected Health Alliance (PCHA)

PCHA is a first-of-its-kind collaboration between Continua, m-Health Summit and HIMSS, focused on engaging consumers with their health via personalized health solutions designed for user-friendly connectivity (interoperability) that meet their lifestyle needs thus binding together the unique strengths, global reach and resources of its founding partners. PCHA brings together the critical elements needed to ensure that deployed technologies are user-friendly, secure and can easily collect, display and relay personal health data.

7.5. Continua Health Alliance

Continua is a non-profit, open industry organization of healthcare & technology companies joining together in collaboration to improve the quality of personal healthcare. Continua Health Alliance is having more than 200 member companies around the world, it is dedicated to establishing a system of interoperable personal connected health solutions with the knowledge that extending those solutions into the home fosters independence, empowers individuals and provides the opportunity for truly personalized health and wellness management.[6] Continua health alliance is member, ITU.

Continua Design Guidelines employs near field communications (NFC) for its touch area network, Bluetooth Classic and Bluetooth Low Energy for its personal area network, and ZigBee for its local area network. The industry standard IEEE Exchange Protocol has been adopted because it provides transport agnostic essential data structures necessary to ensure accurate and comprehensive understanding of the measured data upstream. Furthermore, it simplifies FDA approval of devices maintaining the IEEE protocols. [5]

Continua design guidelines are approved by ITU-T study group 16, in the meeting held in Japan in July 2014 and are available at “Introduction to the ITU-T H.810 Continua Design Guidelines”.

Detailed pictorial diagram is shown in Figure below

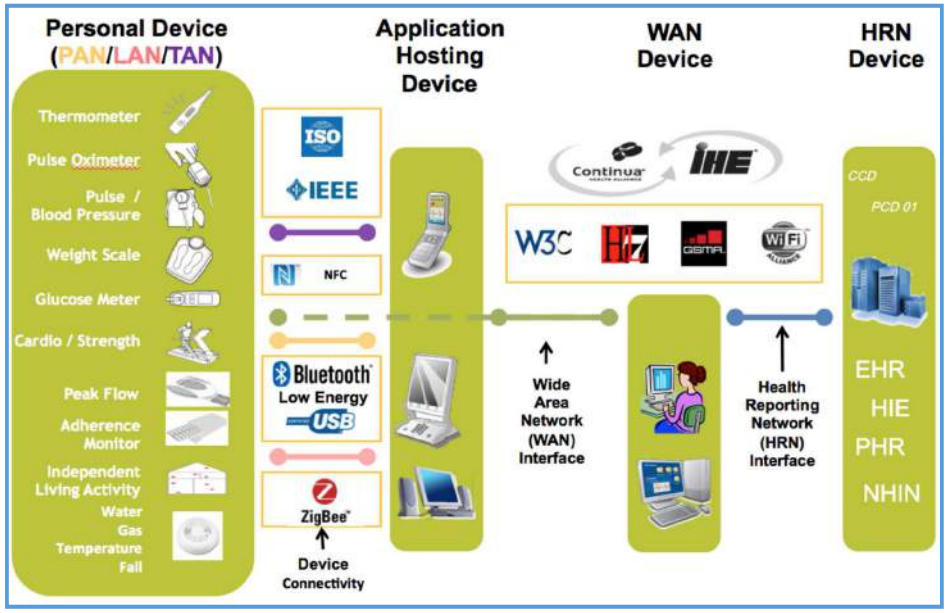

FIGURE 6: REMOTE HEALTH MONITORING ARCHITECTURE BY CONTINUA HEALTH ALLIANCE (SOURCE: ITU-T TECHNICAL PAPER HSTP-H810, JULY 2014)

7.6. ITU- International Telecommunication Union

ITU has established a focus group on "M2M service layer" in 2012. FG M2M is mandated to identify a minimum set of common requirements of vertical markets, focusing initially on the health-care market, application programming interfaces (APIs) and protocols supporting e-health applications and services, and to draft technical reports in these areas.

The Focus Group has decided, not to duplicate efforts and take benefit from existing work and expertise. Therefore, FG M2M is including vertical market stakeholders that are not among the traditional ITU-T membership, such as Continua Health Alliance and the World Health Organization (WHO) for health-care, and will collaborate with M2M communities worldwide (including research and academia), SDOs, forums and consortia. FG M2M initial focus is on e-health.

Within the Focus group, a number of working groups have also been created to carry out the different activities viz. WG1: Use cases and service models, WG2: Requirements and architectural framework of the M2M Service Layer, WG3: API and protocols. The parent group is ITU-T Study Group 11. FG M2M will work in close collaboration with all ITU-T Study Groups, especially SG 11, SG 13 and SG 16.

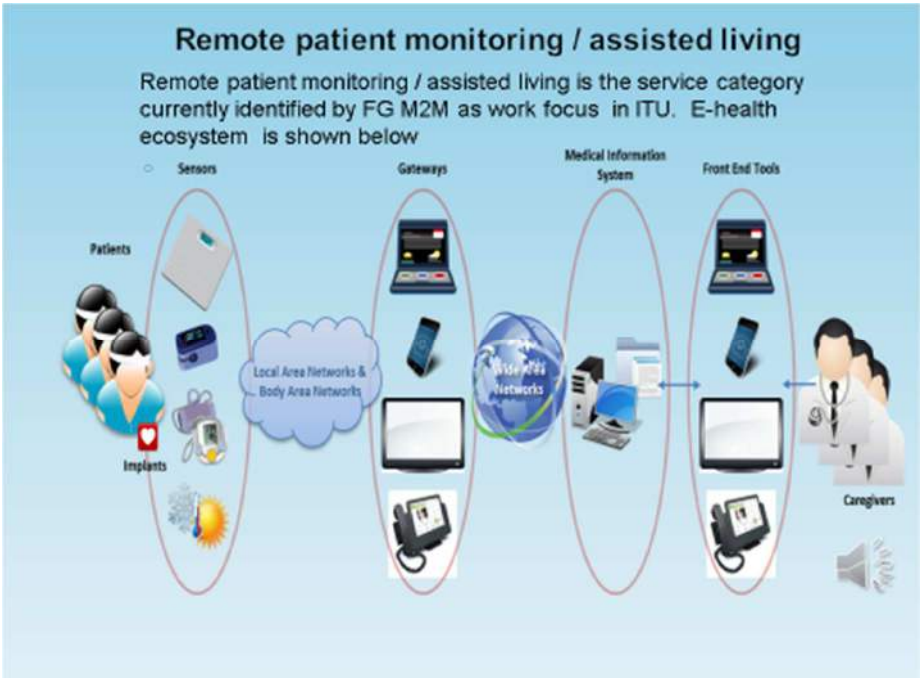

FIGURE 7: REMOTE PATIENT MONITORING [SOURCE: ITU-T FOCUS GROUP ON M2M SERVICE LAYER DOCUMENT [3]

7.7. Electronic Health Record Standards for India

Government of India intends to introduce a uniform system for maintenance of Electronic Medical Records / Electronic Health Records (EMR / EHR) by the Hospitals and healthcare providers in the country. An Expert committee was set up to develop EMR / EHR Standards for adoption / implementation in the country. Draft EMR / EHR Standards were hosted on the website of the Ministry soliciting comments from the stakeholders and general public. The 'Electronic Health Record Standards for India' have been finalised and approved by the Ministry of Health and Family Welfare, Government of India. [14]

http://www.nhp.gov.in/sites/default/files/pdf/emr_ehr_standards_of_india_august_2013.pdf

7.8. BIS Standards for Health

S.No	BIS Standards	Subject	Reference
1.	MHD 17 HEALTH INFORMATICS SECTIONAL COMMITTEE	SCOPE Standardization in the field of information for health, and Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between Independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications) and to reduce duplication of effort and redundancies. To co-ordinate with the work of ISO/TC 215 Health informatics & its sub	

		committee	
2.		IS/ISO 17115:2007 Health Informatics-Vocabulary for terminological systems March 2011	
3.		IS/ISO 20301:2006 Health Informatics-Health Cards-General characteristics March 2013	
FINALISED DRAFTS UNDER PRINT			
1.	DOC.MHD 17(140)	Health Informatics-Digital Imaging and Communication in / ISO 12052:2006 Medicine(DICOM)including workflow and data management	
2.	DOC MHD 17 (0237)	Health Informatics-Electronic health record communication— /ISO 13606-1:2008 Part 1: Reference model	
3.	DOC MHD 17 (0238)	Health Informatics-Electronic health record communication— /ISO 13606-2:2008 Part 2 Archetype interchange specification	
4.	DOC MHD 17 (0239)	Health Informatics-Electronic health record communication— /ISO 13606-3:2009 Part 3: Reference archetypes and term lists	
5.	DOC MHD 17 (0240)	Health Informatics—Interoperability of telehealth systems and networks- /ISO 16056-1:2004 Part 1: Introduction and definitions	
6.	DOC MHD 17 (0241)	Health Informatics—Interoperability of telehealth systems and networks- /ISO 16056-1:2004 Part 2 : Real-time systems	
7.	DOC MHD 17 (0242)	Health informatics-Requirements for an electronic health record architecture /ISO/TS 18308:2004	
8.	DOC MHD 17 (0243)	Health informatics-Electronic health record-Definition, scope and context /ISO/TR 20514:2005	
9.	DOC MHD17 (313)	Health informatics- personal health devices communication Part 10404 /ISO/IEEE 11073-10404 Device specialization-Pulse oximeter	
DRAFT APPROVED FOR CIRCULATION			
1.	DOC MHD 17 (0301)	Health informatics- good principles and practices for a clinical data warehouse ISO/TR 22221:2006	

8. Key Challenges

1. Specification: There are no established independent specifications or certification process for medical devices, including the connected medical devices.
2. Adoption of EMR: Electronic medical records are still in early stage of adoption in the Health sector in India, thus usage of a digital mechanism of remote health care may take time to be implemented.
3. Gap in Skills and Knowledge: Extensive manpower training will be required for skill development regarding remote health management.
4. Budget for Deployment: Well defined healthcare budgets will be required at the State level, for widespread deployment and adoption of remote health monitoring solutions.
5. Acceptance by Doctors: Government policies may be required to ensure doctors use the solution appropriately.
6. Affordability: The medical devices need to be affordable for deployment in the population.
7. Public acceptance: Public will need to be educated about the benefits of preventive healthcare and the use of technology.

9. Way forward

1. Biometric authentication of users using Aadhaar (UID) database and UID Number may be adopted as the authentication process electronic health record system. A design and implementation plan for this work item needs to be created.
2. ITU-T H.810 - Continua Health Alliance's Design Guidelines providing "Interoperability design guidelines for personal health systems" may be further studied for India's needs. A consultation process with device manufacturers and other stakeholders may be initiated for their opinion on the ITU-T H.810 guidelines.
3. The government will need to take the initiative for creating connected medical device certification standards as well as testing labs for guiding compliance. The ministry of commerce has announced the decision to fund the setting up of three medical device testing laboratories in Noida (UP), Haryana and Gujarat, which already have device manufacturing clusters.
4. The health devices are mostly used in PAN and TAN networks and can follow the technology specific profiles, for example BLE profile for wearable devices.
5. A repository for electronic health record data may be set up in India, following the standards defined by the Ministry of Health and Family Welfare.
6. Multiple work items have to be created to (a) map the use cases with M2M architecture proposed for India; (b) map the Indian use-cases with the use-cases covered by Continua, and ETSI; and (c) identify the gaps and non-applicability of the use-cases with respect to the overall M2M architectural requirements

10. References

[1] World Population Ageing 1950-2050, Population Division, Department of Economic and Social Affairs, United Nations

[2] World Population Prospects, The 2012 Revision, Volume 1, Department of Economic and Social Affairs, United Nations

[3] ITU-T Focus Group on M2M Service layer, M2M enabled ecosystems: e-health, D0.2 – Version 1.0, (04/2014)

[4] M2M standardization in ITU-T and its perspective, HyoungJun Kim, ETRI (khj@etri.re.kr), Chair of WP3 in ITU-T SG13, Vice-chair of FG on M2M in ITU-T SG11

[5] HSTP-H810 Introduction to the ITU-T H.810 Continua Design Guidelines

[6] http://www.continuaalliance.org

[7] http://www.pchalliance.org

[8] http://m2mworldnews.com/2015/03/20/48515-driven-by-increased-demands-on-healthcare-suppliers-connected-medical-imaging-equipment-to-grow-at-a-17-cagr/

[9] WHO http://apps.who.int/gho/data/node.country.country-IND?lang=en

[10] Machina Research news:

https://machinaresearch.com/static/media/uploads/machina_research_press_release_-_healthcare_report_-_2014_05_07.pdf

[11] Draft Policy on Internet of Things:

http://www.deity.gov.in/sites/upload_files/dit/files/Revised-Draft-IoT-Policy.pdf

[12] National Health Profile (NHP) of India – 2012 by Central Bureau of Health Intelligence: http://www.cbhidghs.nic.in/index2.asp?slid=1256&sublinkid=1163

[13] National Health Profile (NHP) of India – 2013 by Central Bureau of Health Intelligence:

http://www.cbhidghs.nic.in/index2.asp?slid=1284&sublinkid=1166

[14] National Health Portal: Electronic Health Record Standards

http://www.nhp.gov.in/electronic-health-record-standards

[15] Electronic Health Record Standards For India, August 2013

http://www.nhp.gov.in/sites/default/files/pdf/emr_ehr_standards_of_india_august_2013.pdf

[16] Doing Business in India Ernst & Young

http://www.indianembassyrome.in/doingbusiness.pdf

11. Annexure 1

Use Case Analysis of M2M in Healthcare

This chapter explains:

1.0 Use Case Analysis

11.1. Use case Remote Patient Health Monitoring

Title : UC_Health_RemotePatientMonitoring

Source (as applicable)

Continua Health Alliance
Ishrath Humairah, Tech Mahindra
Santhosh Madathil, Wipro
Ananda Sen Gupta, Trackmybeat Healthcare (India) Pvt Ltd
Mani Rajakannu, EIS-MDD, TCS
Rahul Kumar, TCIL
Alok Mittal, STMicroelectronics

Objective

This use case describes the building blocks for remote patient monitoring (RPM) - that would enable key health data from the patient/user to be uploaded to the Electronic Health Record (EHR) system monitored by the care-provider (hospital).

This will, in turn, allow the health-care service provider to have access to current health data of the patient and be able to plan care services for the patient remotely. Thus, the doctor would be able to review the health condition of the patient without the patient having to travel to meet the doctor.

Background

Current Practice

The existing infrastructure for Telemedicine / Remote Patient Monitoring is not at all adequate to address the growing healthcare needs. There are a few instances where technology is used for example, Tele-consultation between city-based Tertiary hospital and a satellite healthcare centre in a smaller town.
The Apollo Hospitals group has been a pioneer in Telemedicine in India, leveraging VSAT technology, and has provided access to secondary / tertiary consulting services to remote rural healthcare centres through VSAT. Most of the tele-consultations were mainly reviews of medical cases.
This facility is however not extensively available in the country, and is quite expensive to maintain. A full-fledged Remote Patient Monitoring initiative has not been taken up even in the metros and urban areas.

Need for Use Case

India poses a unique set of challenges when it comes to “accessibility of quality healthcare”. The key factors that impact healthcare are:

- One of the most populous countries, with more than 70% of its population in rural areas (more than 25% BPL)
- Skewed Healthcare infrastructure with more than 70% of the infrastructure concentrated in urban areas.

- Poor Health Report Card: Maternal Mortality Ratio (MMR) and Infant Mortality Rate (IMR) are high, it has the highest burden of communicable diseases and lifestyle changes have led to a spurt in NCDs (Diabetes and Hypertension)

- The number of beds and number of doctors per 1000 people is rather low. As a result, the doctors are able to give very little time diagnosing and treating patients, and this leads to long waiting times as well as inadequate and expensive medical treatment.

A well planned RPM framework built on-top of a robust infrastructure would ease the burden on the present Healthcare System and at the same time provide access to quality healthcare that is affordable.

Indian Ecosystem Specifics

Some of the key challenges seen in Remote Patient Monitoring System in India are as follows:

- Lack of supportive infrastructure to roll out remote patient monitoring services
- Lack of established and approved standards for medical device safety and usage
- High cost of subscribing for individual remote patient monitoring devices and subscription services as it is primarily borne by the patient
- Availability of affordable Medical Devices. It is expensive to import devices.
- The biased perception towards medical devices – as patients would prefer to see the doctor than rely on medical device.
- Lack of patient education in this area.
- Lack of comfort within medical fraternity in moving from traditional medical practices to adopting a new technology
- Availability of Medical staff trained in using a new technology

Description

Remote Patient Monitoring (RPM) is a mobile or Tele-health solution that enables monitoring of patients outside of conventional clinical settings (e.g. in the home). The patient has medical devices on or close to his body which has sensors that capture the patient's healthcare/ physiological data. This data is then transferred across telecommunications networks with the help of data transmission products, and is monitored for any abnormality with the help of software and/or clinical and healthcare experts.

Increasing number of people with chronic medical conditions and growing senior citizen population, coupled with shortage of skilled medical personnel have been driving the demand for remote health services all over the world. By increasing reach and efficiency of doctors, RPM helps increase access to care and decrease healthcare delivery costs.

It addresses a key pain point of the stakeholders of the healthcare system by enabling the exchange and flow of information from the patient's medical device (outside of hospital) to the clinical staff such as doctors, nurses and paramedics.

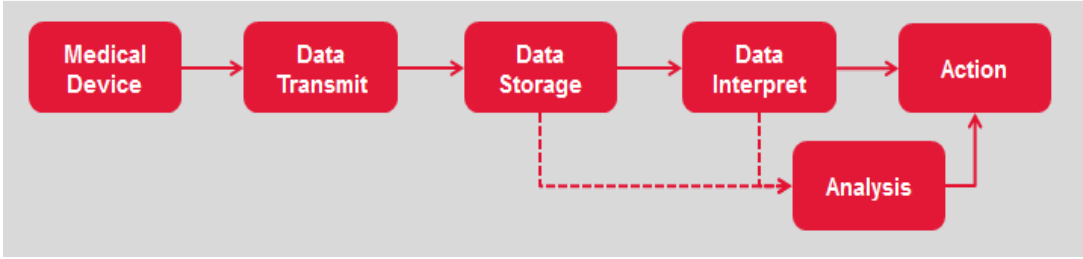

FIGURE 8 : INFORMATION FLOW IN REMOTE PATIENT MONITORING

RPM not only helps in monitoring the patients' medical conditions, avoid medical emergencies and hospital re-admissions, but also helps those in geographically isolated settings to access specialized and preventive medicine and care.

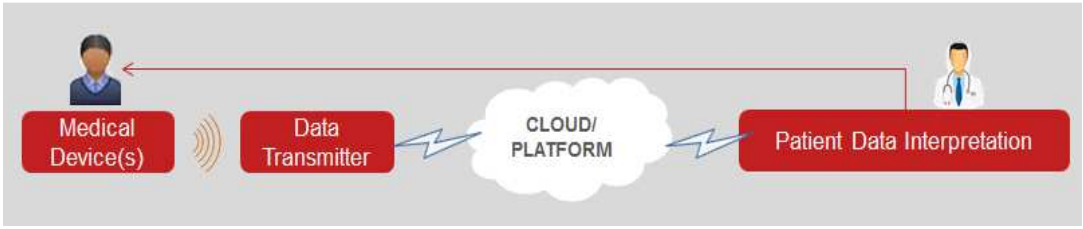

FIGURE 9 : REMOTE PATIENT MONITORING CONCEPT

Components of RPM Solution:

- Sensors on a device that is enabled by wired or wireless communications to measure physiological parameters.
- Local data storage at patients' site that interfaces between sensors and other centralized data repository and/or healthcare providers.
- Data transmission and connectivity.
- Centralized repository to store data
- Diagnostic application software that develops treatment recommendations and intervention alerts based on the analysis of collected data. This may be augmented by medical experts such as doctors, nurses, etc.
- Depending on the disease and the parameters that are monitored, different combinations of sensors, storage, and applications may be deployed.

Post-conditions

- The data is stored in the EHR System with time stamp.
- The data can be further analysed at the cloud services database.
- The detailed analysis can lead to a variety of actions, for example, long term recommendations for an individual or disease analysis for a population, which may lead to further intervention planning both at individual patient level or a policy level.

Use Case process Flow diagram

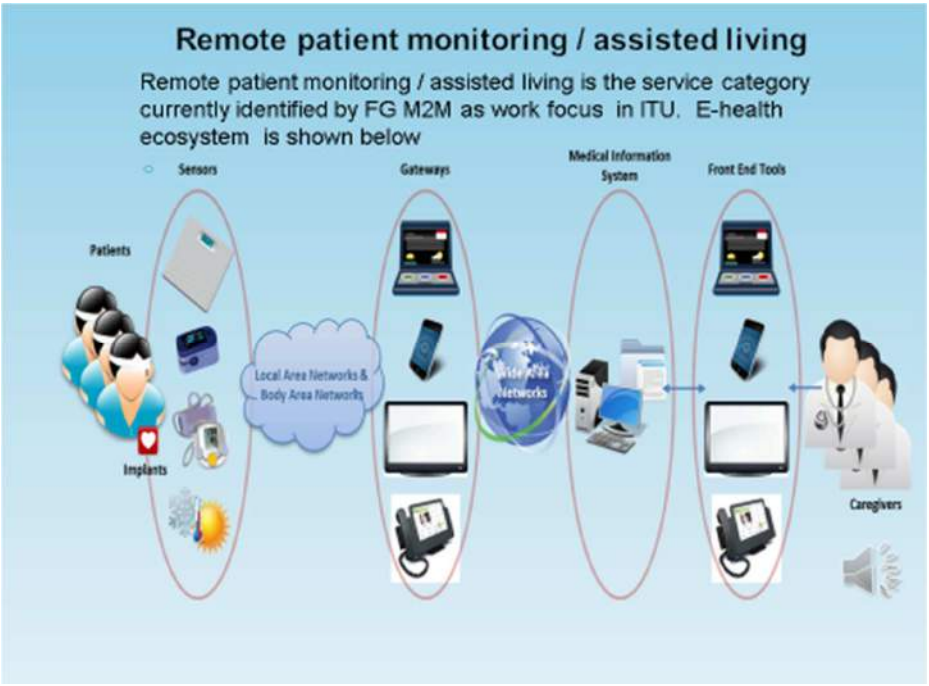

FIGURE 11 : REMOTE PATIENT MONITORING [SOURCE: ITU-T FOCUS GROUP ON M2M SERVICE LAYER DOCUMENT [3]

Information Exchange

Data bandwidth requirements

- Data bandwidth requirements are dependent on the personal device of patient being monitored and the frequency of data transfer.
- Based on the range of devices available/ put to use, the data bandwidth requirements differ.
- Sometimes, the remote device or gateway device may store the data and all data is forwarded in bulk when network connectivity is available

Architectural considerations (Non-functional Requirements)

Depending on the criticality of the data (and the regulations around it) being gathered, the personal devices can be categorised into a few classes.

Actors (as applicable)

Actor Name	Actor Type (person, organization, device, system)	Role Description
Patient	*Person*	*The person whose parameters are to be monitored. The monitoring could be in a clinical or non-clinical setting.*
Personal Device (Sensor)	*Device*	*Interfaces on one side with the physical world, measures patient's vitals (NiBP, Blood Sugar, ECG, Weight etc).* *Interfaces with a Medical Gateway at the other side. This interface could be either wired (Serial, USB) or wireless (BT, ZigBee) and these devices may either be single or multi parameter monitors.* *These devices may use proprietary protocol to communicate with the Gateway or use a standard protocol like ISO/IEEE 11073.*
Medical Gateway	*Device*	*The Device that interfaces with the personal devices at the patient's location, aggregates the information and communicates with the back end system (EHR / PHR / CIS). This Gateway could be a dedicated hardware-based device, or software on a PC or mobile device.*
Communication Infrastructure (backbone)	*System*	*This infrastructure forms the back bone of the RPM set-up. It could be a combination of Land-line / mobile telecom infrastructure.*
Medical Records	*System*	*The Database at the back-end (Could be an hospital based EMR, a Public PHR or any type of Clinical Information System*
RPM Application Platform	*System*	*This could be an Application Framework that leverages the Medical Records information and provides the Care-Provider a customized interface depending on the end-application (Chronic Disease Management, Clinical Trials etc).*
Tele healthcare Provider	*Organisation / Person*	*It Includes doctors, nurses and other Telehealth staff (can be paramedics) who are involved in monitoring the vitals, evaluate the information*
Clinician / doctor		*It Includes doctors / clinicians who can intervene based on data and feedback from Telehealth care provider, to take appropriate action for the patient*

- Sensors on a device that is enabled by wired or wireless communications to measure physiological parameters.

- Local data storage at patients' site that interfaces between sensors and other centralized data repository and/or healthcare providers.
- Data transmission and connectivity.
- Centralized repository to store data
- Diagnostic application software that develops treatment recommendations and intervention alerts based on the analysis of collected data. This may be augmented by medical experts such as doctors, nurses, etc.
- Depending on the disease and the parameters that are monitored, different combinations of sensors, storage, and applications may be deployed

Pre-requisites (Assumptions):

It is assumed that:

- The patients or their caregivers are capable of using the personal devices.
- The doctors are willing and capable in interpreting the medical data and use the electronic health records as a part of the diagnostic and treatment process.

Pre-conditions (if any)

It is assumed that:

- The personal health monitoring device is being worn/ used by the user appropriately to make accurate data measurement
- The communication between personal device and aggregator (medical gateway) is working and user is able to identify the communication channel availability
- The WAN connectivity is available from aggregator to the EHR system
- The user has agreed by contract to subscribe to the health parameter monitoring and records update
- When a "personal" device is being used, the user identity is managed by the unique-ID of the personal device which is either updated in the Cloud application or by assigning device ID to the specific user. In case a shared device is used, there needs to be another mechanism to identify the user of the device uniquely.

Triggers (if any)

- When a personal device is being used, this will trigger the use-case for collecting the data and sending it to the servers.
- An action from the doctor will be triggered in case the data received from the patient is abnormal / deranged.

Scenario description

Normal Scenario

- The personal health monitoring device is worn/ used by the User to make appropriate data measurement
- The device or an external mechanism is able to identify the user - whose data is being captured - in a unique manner
- The initial pairing of the personal device and the medical gateway / aggregator device can be done during the system installation and configuration, or on the fly, in case of a mobile patient
- Once the measurement is made on the personal device, this data is transferred to the gateway device over a local communication protocol such as Bluetooth, NFC, and ZigBee etc.
- The data is then transferred from the medical gateway to a central server holding the patient's EHR over a fixed or wireless network in a private and secure fashion, using WAN protocols
- Once the EHR has been updated, medical protocols / guidelines may be applied either by the system or Tele-health support personnel or nurses or clinicians, on the data.

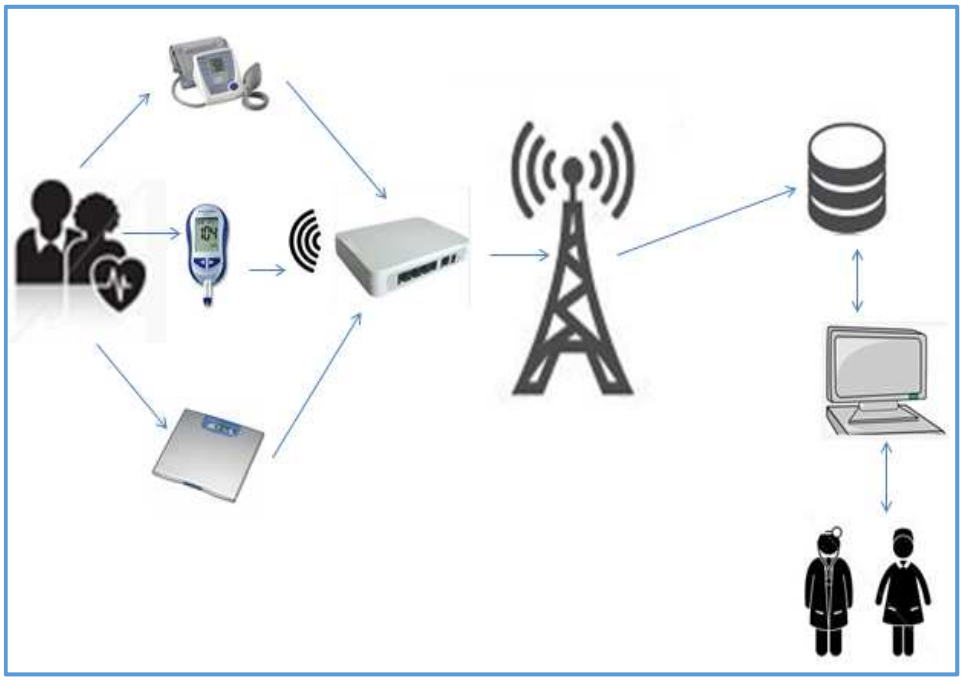

FIGURE 10: REMOTE PATIENT MONITORING CONCEPT

- This may throw up health alerts, in case the data is found to be deranged.
- Doctors or clinicians may take appropriate actions as per care pathways based on the data and/or health alerts. The action may be anything between emergency care actions to a general health advice.

Type of Device: Class 1/2/3

- Class 1 – Mostly wellness/ generic healthcare devices for temperature, and BP etc.
- Class 2 – Patient medical data coming from glucometers, and E.C.G patches etc.
- Class 3 – Data from implants, pacemakers and other critical devices.

Communication channel used

- Wired communication like serial port, USB, and audio port etc.
- Wireless Data Transmission Channels such as Bluetooth, Wi-Fi, and Telecom Connectivity.

APIs to be exposed to the Application from platform

Refer to specific standards for the device type. For example 11073-10404 Device specialization-Pulse Oximeter.

User Interface

- Physical device: User-Interface: ON-OFF Button, Indication of device working status, Low-Battery Indication, Device-Aggregator connection.
- Aggregator: Communication channel (BT, BLE, Wi-Fi etc.) interfaces. Connection to the WAN technologies (GPRS, Wi-Fi) shall be available, App shall be downloaded (when Mobile phone is used as Aggregator).
- EHR system interface: App for providing user interface for the data readings, Graphic format for the changes in parameters. Web access to EHR system via user authentication.
- Doctors/Care Giver Interface: Providing specific data points with the parameters which are within the Range or out of range.
- Government bodies: Web Interface for checking the trends of the patients subscribing to the service.

Communication Infrastructure

Communication Network	Technologies
Personal Area Network	USB, BT, BLE, NFC, Wi-Fi, ZigBee, ANT
Wide Area Network	GPRS, Wi-Fi, 2G, 3G, Fixed line broadband

Geographical consideration (for geographical spread and concentration of the constituent devices)

The healthcare devices are personal devices, it shall not affect any limitations or challenges for the geographical spread. Actually, each single user can have several healthcare devices.

The WAN connectivity is assumed to be available and enough to carry the data from all users in case of concentration of the devices.

In addition, the data packets in health devices are small and transmissions are sporadic in nature. No specific challenge for the geographical consideration is expected.

Incase of rural healthcare, the same consideration apply

Security

- Security: The requirements are standard for all the health devices. The device communication in the PAN and WAN shall be secure. The data exchange will be encrypted. The security keys between the communication channels will be defined by the service provider
- Criticality: The data is critical for the user and care-giver. This will define the course of action by the medical professionals.
- Security Threat: The hackers may like to interfere with the device communication in PAN and WAN technologies. The PAN network shall be built with authentication keys known to the user by way of pairing. Physical pairing can also be done using the NFC technologies

For WAN, the security requirements are already available.

Startup Shutdown process

The devices are generally battery powered and no-power cycling is expected. The battery charging or replacement shall be the responsibility of the user.

Data Backup and Archiving

The device may maintain the history of the data. Upon transfer of the information to the EHR System, the data may still be available on the local device memory. The oldest data may be overwritten if the device memory is exhausted

There can be local provision to retrieve the data (like USB connectivity) in case of the wireless communication failure. Similarly, a removable memory card can be used for data storage and it can be retrieved for data transfer.

Remote Device Management

Memory Management

The device memory management may be done locally. The user or service provider can decide to delete the historical data once the data upload has been done on the EHR System. This can be done using specific applications running on the computer which may manage the memory in secure manner.

In some systems, the service provider may manage the memory of the device.

Device Registration and configuration (Master slave, dual master –slave, peer to peer)

Each personal health device may have a unique serial number managed by the manufacturer. The device installation or usage needs to be commissioned by way of registering the device for the user and linking it to the EHR system. This is a manual process.

The combination of the manufacturer and serial number shall provide unique ID to the device. For example, in USB communication systems, the device shall have a Vendor ID and a Product ID and a

unique serial number. This is ensured by the manufacturer. The USB consortium (www.usb.org) assigns the Vendor ID.

The aggregator device shall ensure the unique number in WAN connectivity. This can be mobile phone number when the mobile phone is used as aggregator or the device IP address when using the Ethernet/Wi-Fi connectivity.

Device Remote Health monitoring and troubleshooting

For most of the personal care systems, the battery charging shall be managed by the user. The device may provide the indication for "low battery" and prompt the user to charge the device or replace the batteries.

The device battery life can be monitored remotely for certain devices. This is mandatory for the systems where user cannot charge the device. The data exchange from the device to the server will include the battery status. This enables the service provider to initiate the actions for the device replacement.

System Availability

Criticality of QoS (Quality of Services)

Remote Patient Monitoring deals with patient data that helps in critical decision making and saving patients' lives. Therefore it is extremely important to have guaranteed response times, have high end connectivity and backup services to enable seamless healthcare data transmission.

Based on patient data monitoring, analysis & interpretation, medical emergencies and hospital re-admissions can be avoided by monitoring patient's healthcare data. Similarly, long term care of patient's chronic conditions can be well planned with the same.

Criticality of quality of services is of high importance in Remote Patient Monitoring and focus should be on providing high quality of remote patient monitoring services by deploying the best in class medical devices, software, data transmission networks, and high quality clinical staff to provide the clinical interpretation services.

Time Synchronization

The device may maintain its time locally. The device time can be synchronised with the server by the built-in function. This is a preferred requirement. The local storage of data will be time-stamped using the local time of the device.

If the data is being updated on the server in real time, the EHR system will record the time as per the server time

Potential market growth

The Personal Emergency Response System (PERS) marketplace, which is often associated with providing the elderly and chronically ill population with a remote mechanism for communicating medical emergencies while in the home, is undergoing a facelift. Leading the way is a convergence in how traditional two-way PERS systems are intersecting with the use of real-time, Connected Health clinical measurements which monitor and track an individual's specific medical condition in the home, well outside of the four walls of an institutional care setting. The by-product of this convergence is a newly evolving, rapidly growing market for Remote Patient Monitoring (RPM) & Population Surveillance.

Ironically, healthcare reform has concurrently put the industry at a crossroads for effectively managing large populations in a well-coordinated, prospective, real-time manner, in contrast to an afterthought or retrospective manner. Healthcare reform is but one of a myriad of market forces driving these changes. Several reform and related elements behind this growth are

- High Risk / High Cost Individuals: Adults age 65 and older engage in the highest level of healthcare spending among all age groups. Additionally, almost half of all healthcare spending was used to treat just 5% of the population. Better management of these high risk / high cost individuals outside a hospital setting and in a preventive care manner is imperative to lowering healthcare costs, especially as the age structure of the overall population is projected to change greatly over the next four decades.

- Managing the Growing Incidence of Chronic Conditions: Unquestionably, individuals with multiple chronic diseases place the heaviest burden on the healthcare system. Approximately 80% of Medicare beneficiaries have one or more chronic conditions. Four out of five major chronic conditions that account for hospitalization impact those over 65. Better management of the elderly and their chronic conditions is not a nice-to-have but a must-have requirement. Services for older adults need to be person-centred, coordinated across the continuum of care and focused on health and wellness. Particularly as it applies to 24×7 prevention of acute illness episodes and disease-related disabilities, and where sophisticated, clinically-driven monitoring by population, device (PERS and "smart" Connected Health devices) and healthcare constituent (e.g. payer, provider, home care agency).

- Individual Coverage Expansion (Exchanges) / Medicaid Expansion: About 16 million new enrolees are expected to join Medicaid by 2017. Additionally, the onslaught of expanded coverage across higher-risk demographics and the potential for adverse selection on public exchanges will require risk-bearing entities (payers or providers) to look for alternative methods like RPM and surveillance to lower healthcare costs and manage high-risk populations at the point of coverage versus simply at the point of encounter.

- Homecare is not only preferred, but essential: Overall reducing the dependency on institutional care settings has many benefits, including cost savings. Homecare has the ability to play a tremendous role in reducing care spending by treating more people in a cost-effective manner at a fraction of the cost of other institutional settings – in some cases more than 75% lower. Incentives are aligned to promote homecare but also provide the peace-of-mind and safety while living independently.

- Readmission Reduction Programs: Hospital readmissions for older patients cost American taxpayers more than $15 billion per year – and many are avoidable. Medicare readmission penalties established by CMS will force both payers and providers to take a fundamentally new approach to coordinating care, particularly post-discharge. This will further incite the demand for RPM and Surveillance capabilities to identify risks well before readmission occurrences.

- Consumer/Patient Engagement: With patients, caregivers and their family members taking a more proactive role in managing their health, RPM & Surveillance is becoming increasingly prevalent in the healthcare industry. In addition to monitoring patients with chronic conditions and senior patients, RPM & Surveillance enables patients and their family members to track vital information like blood pressure, weight change, glucose levels and other vital signs while eliminating 90% of the "unnecessary data noise" that is not

warranting a clinical intervention. In effect, this means a more prospective surveillance monitoring of a patient's health management.

New, smart mobile devices, which provide 24×7 connectivity and extend a broader healthcare value proposition, are filling gaps in care for high risk/high cost patients including the chronically ill. In our view, healthcare's challenges are on a much-needed collision course with Connected Health innovations, including the convergence of personal emergency response system (PERS) and mobility – which is why many industry watchers are optimistic about the potential cost savings.

As this plays out, marketplace spending on these solutions will likely rise – and various market sources are noting that home monitoring systems with integrated communication capabilities are expected to reach 9.4 million connections worldwide, equating to a ~27% CAGR between now and 2017. In addition, the number of devices with integrated cellular connectivity is projected to grow at a ~47% CAGR during the same period. Finally, Juniper Research suggests that over the next five years, RPM will result in cost savings of up to $36 billion globally and that North America will account for little over three quarters of the savings.

The game is on. Scale and innovation are converging, and the notion of Population Health Surveillance is no longer aspirational – it is real and is emerging at the centre of true care coordination initiatives for payers, risk-bearing providers and the cadre of players across the community-based care continuum.

Contracts and Regulations

Ownership of data

The Patient's Medical Condition Data and its derivatives are currently owned by the Hospitals, Healthcare Service providers, and medical device companies - who are offering the services in various pockets of the country. Privacy and Security of the data is of concern here.

Many parties owning the data means patient cannot benefit from past health records. There should be a central repository at patient's disposal for his / her data.

The patient should have ownership of the data and should be able to authorise other parties involved in his healthcare decision making such as the doctor, nurse, provider, insurance company, etc.

Patient Safety Requirements

High quality medical devices that have been approved by various medical, technical and legal boards. Data transmission that does not pose a threat to patient's health condition (such as high radiation and frequencies), this is more important for continuous monitoring devices.

Compliance to standard

- HIPAA (the defacto standard to comply with so that it becomes easier to pass the compliance test in other regions).

- Suitable ISO and BIS standards - but these are not well defined for Medical Device based Remote Patient Monitoring Scenarios in India. It is best to follow international standards to be future ready.
- Continua Health Alliance: International non-profit industry organization enabling end-to-end, plug-and-play connectivity of personal health devices, systems and services in Personal Connected Health.
- IEEE 11073 Standards.

Deviations: from standard

None for the Personal Healthcare devices

11.2. Use Case Ambulance Patient Monitoring System

Title ID: UC_Health_Ambulance Patient Monitoring

Objective

This use case talks about Patient Monitoring System during journey period of the Ambulance from patient location to the hospital. This use-case is similar to Remote Patient monitoring system with addition to the requirements of the mobile system

Source (as applicable)

T.P.Mallik, iDiagnosis Telematics
Alok Mittal, STMicroelectronics

Background

Current Practice

The Ambulance is required to carry Patients to the hospital on urgent basis. This can be due to urgent medical attention required by the Patient due to a sudden occurrence of an ailment, or involvement in an accident causing the physical injury to the patient.

The medical treatment of the patient starts after reaching the hospital and after initial procedures of registration are completed. At present the travel time of the ambulance is lost, without any treatment of the patient. Delay in reaching the hospital in case of critical patient may result even in death of the patient.

Need for Use Case

The patient needs the Ambulance service due to requirement of urgent medical attention due to a problem like heart attack or due to accident.

The need for this use case is that the moment the critical patient gets into the ambulance, relevant data related to registration of the patient covering the disease history, allergy (if any) and patient's vital parameters like heart beat and pulse rate, temperature are communicated to the hospital. The para-medical staff or any accompanying doctor may even take ECG or blood sugar like diagnostic information and convey the same to the hospital so that the moment patient reaches the hospital the treatment can begin thus saving the initial critical time which is vital for recovery of the patient. To save life of the patient in case the specialist doctor is in the hospital, on receipt of the vital data may prescribe medication which can be given to the patient during traveling time of the ambulance.

The challenge is that all ambulances may not have the doctor travelling with the patient. In such a condition, the para-medical staff can take specific steps based on the advice of doctors remotely.

The Ambulances are associated with specific hospitals and they carry the patients to the pre-assigned hospitals. This system can be optimized to save time of medical attention which can be provided to the patient based on his condition. The ambulance can carry the patient to the nearest hospital thus saving the travel time. The ambulance location needs to be tracked on the map so as to check the nearest hospitals and calculate the expected time of arrival of the patient.

The ambulance generally blow the siren for inviting attention of other users to provide the road path for fast movement of the patient. Similarly this siren invites the attention of traffic-police which can

help clear the traffic from the road-crossings. This system can be automatized to make fast movement of the ambulance.

Indian Ecosystem Specifics

Same as above
In addition to above, in specific cases of utmost urgency, the movement of the Ambulance has been facilitated by the traffic police to make a "Green Corridor" to provide very fast travel time. This has been done to carry human organs for transplant from airport or specific hospital to the hospital which has patient requiring the organ transplant.

National Health Mission website provides the details of the National Ambulance Service (NAS). Few details are mentioned below

- 29 States or union territories have the facility where people can dial 108 or 102 telephone number for calling an ambulance.
- 108 is predominantly an emergency response system, primarily designed to attend to patients of critical care, trauma and accident victims etc.
- 102 services essentially consist of basic patient transport aimed to cater the needs of pregnant women and children though other categories are also taking benefit and are not excluded.
- JSSK(Janani Shishu Suraksha Karyakram) entitlements include free transfer from home to facility, inter facility transfer in case of referral and drop back for mother and children. These are the key focus of 102 service.
- 7344 ambulances (490 Advanced Life support and 6749 Basic Life Support ambulances) are being supported under 108 emergency transport systems including new.
- 7371 ambulances are operating as 102 patient transport including new ambulances.
- 6235 empanelled vehicles are also being used in some States to provide transport to pregnant women and children e.g. Janani express in MP, Odisha, Mamta Vahan in Jharkhand, Nishchay Yan Prakalpa in West Bengal and Khushiyo ki Sawari in Uttarakhand.

  Further details are available at http://nrhm.gov.in/nrhm-components/health-systems-strengthening/emri-patient-transport-service.html

GVK EMRI has, through Tech Mahindra as its technological partner, been able to develop a comprehensive Emergency Management System. The organization in providing the below

- Ensuring 24*7 availability of Network and Systems.
- Managing the Golden Hour efficiently.
- Ensuring a promptly assessed and hassle free helpline.
- Harnessing strong linkages/ partnerships/ alliances with hospitals, doctors, police, fire stations etc.
- Allows tracking of call based on location of caller.
- Enables Dispatch Officer to access the GIS Vector data (maps) provided by Government agencies and identify the incident location.
- Identifying the exact location of ambulance on real time basis.
  Reference: http://www.emri.in/technology/

  Some of the technology components used are as below

Automation of the processes involves the following major components of technology:

- Telecom Switch with automatic call distribution features & IVR facility
- Computer Telephony Integration
- Voice Loggers
- GIS/GPRS Software
- AVLT – Automatic Vehicle Location and Tracking
- Mobile Application

Description

- There are following types of Ambulance services
    - Advance transport ambulance: Contains special equipment
    - Basic Life Support Ambulance
- Patient Transport Ambulance: Not much medical equipment are there
- Two-way communication is needed using UHF/VHF/ Cellular phones
- This is needed to provide information to hospital about the Patient condition and physical information.
- Telemedicine set up in the ambulance facilitates recording, measurement and transmission of vital patient information like patient allergies, ECG, blood sugar to the hospital.
- Video conferencing is also required for transferring medical information of the patient. This helps the doctors to ascertain the physical condition of the patient remotely.
- Online 12 Lead ECG information can be transmitted from moving Ambulance. ECG needs to be DICOM compliant.

Integration of Ambulance Movement

The ambulance movement can also be linked to the road-traffic management system. The GPS tracking of ambulance movement can provide the advance information on management of traffic and provide warning to other road-users to be alert and provide the required pass-way to the ambulance. Even the traffic lights can be switched to green for providing the fast passage to the patient without disturbing other road users.

Actors (as applicable)

Actor Name	Actor Type (person, organization, device, system)	Role Description
Patient	Person	The person who needs urgent medical attention and is carried in the Ambulance to the hospital. The vital parameters of this 'actor' needs monitoring
Paramedical Staff	Person	Person in the Ambulance who is semi or fully trained to handle the medical conditions. He/she puts the monitoring devices on the patient for measurement of

Actor Name	Actor Type (person, organization, device, system)	Role Description
		the vitals
Patient monitoring Device	Device	Devices responsible for monitoring the patient Interfaces on one side with the physical world, measures patient's vitals (NiBP, Blood Sugar, ECG, Blood Group, Pulse-Rate and SpO2 values etc). Interfaces with a Medical Gateway at the Ambulance which is connected to the Hospital The interface between the device and Gateway can be mostly wired (Serial, USB) or wireless (for example BT, BTLE, ZigBee). These devices may use a standard protocol like ISO/IEEE 11073
Medical Gateway	Device	The Device that interfaces with the Vital Monitors at the patient end, aggregates the information and communicates with the hospital providing the information of the patient.
Communication Infrastructure (backbone)	System	This infrastructure forms the back bone of the Remote Patient monitoring system. It can be mobile telecom infrastructure or devices communicating over UHF/VHF radio frequency range for reliable and dedicated one-to-one communication between Ambulance and Hospital
Medical Records	System	The Database at the back-end (Could be an hospital based EMR, a Public PHR or any type of Clinical Information System recording the parameters of the patient
Ambulance Management System	Organisation	An organisation or centralised emergency system which is able to dispatch the ambulance to the required location and identify the nearest hospital which can provide the required medical help to the patient
Care Provider / Clinician	Organisation or Person	Including Doctors, Nurses and other clinical staff who are involved in monitoring the vitals and responsible for the following: 1. Suggesting the para-medical staff in the Ambulance to take specific action

Actor Name	Actor Type (person, organization, device, system)	Role Description
		2. Prepare for emergency reception of the patient

Pre-requisites (Assumptions):

It is assumed that:

- Once the patient is carried in the ambulance, the para-medical staff is connecting the devices to the patient correctly, for measurement of the vital parameters.
- The Device to aggregator communication is working and the patient monitoring system is showing the vitals recorded.
- The initial pairing of the device from the monitoring-device to the aggregator device is already available during the system installation and configuration.
- The WAN connectivity is available from aggregator to the hospital system and it is being monitored by the healthcare professionals or central Ambulance management system.
- The ambulance is equipped with the telemedicine software, which will ensure that a unique ID is assigned to the ambulance and the patient is registered online.

Triggers (if any)

- The phone call from the patient or their family members or any caller informing the need of the ambulance service.
- Acknowledgement of the phone call by the emergency services by dispatching the ambulance from the nearest hospital.
- Ambulance "on the Service" kind of trigger which can activate the tracking of the movement of the Ambulance, facilitating the traffic management.
- "Patient on board" kind of trigger which can activate the logging of the vital parameters data of the patient and monitoring of it.

Scenario description

Normal Scenario (as applicable)

- The phone call from the patient or their family members or any caller informing the need of the ambulance service.
- Or, the remote patient monitoring system triggers an alarm due to abnormal condition at the Patient monitoring central system for the need of the Ambulance.
- Acknowledgement of the phone call by the emergency services by dispatching the ambulance from the nearest hospital.
- Ambulance "on the Service" kind of trigger which can activate the tracking of the movement of the Ambulance by central system, facilitating the traffic management for Ambulance reaching the Patient's address.
- "Patient on board" kind of trigger which can activate the logging of the vital parameters data of the patient and monitoring of it.
- (Optional) The nearest hospital is located on the map with the facilities required to handle the emergency situation if the ailment or problem is known.

- The data from the personal health device is being uploaded in the EHR System with time stamping, these vitals are being monitored.
- The Ambulance travels to the hospital (nearest in case of central management services or the designated hospital) and traffic management is again activated.
- The vital parameters of the patient and approximate time of arrival being monitored by the hospital and central system.
- Ambulance reaches the hospital and patient is transferred to emergency and the treatment is started without any loss of time.

Post-conditions (if any)

- The patient data is being logged time wise and uploaded in the EHR System or emergency-response system.
- Vitals parameters data is being analysed at the cloud services database.
- Any medical procedure being conducted in Ambulance on the patient is recorded.
- Usage of Ambulance services is logged (getting busy and getting available).
- Availability of Ambulance is again uploaded in the system after the patient is delivered to the hospital.
- Time of the emergency response system and services availability recorded.
- The information of the patient is transferred to the central EHR system once the identity of the patient is being established.
- The Hospital address is being sent to the mobile numbers of family members pre-configured in the system.

Information Exchange

- Data bandwidth requirements are dependent on the vital parameters of patient being monitored and the frequency of data transfer.
- Based on the range of devices available/ put to use, the data bandwidth requirements differ.
- At times, the remote device or gateway device may store the data and all data is forwarded in bulk when network connectivity is available.

Data bandwidth requirements for Vital Signs: Low

ECG: High

Video Streaming: Very High

Architectural considerations (Non-functional Requirements)

Type of Device: Class 1/2/3

- Class 1 – Mostly wellness/ generic healthcare devices for temperature, BP, blood group etc.
- Class 2 – Patient medical data coming from glucometers, E.C.G, etc.
- Class 3 – Data from implants, pacemakers and other critical devices.

Communication channel used

- Wired communication like serial port, USB, and Ethernet etc.
- Wireless Data Transmission Channels such as Bluetooth, Wi-Fi.
- WAN connectivity: Wi-Fi (City Wi-Fi if available), Telecom Connectivity (2G/ 2G/4G GPRS, CDMA connectivity), WiMAX.

Interface Requirements (as applicable)

- Inter-device communication technologies between the monitoring devices to the Aggregator. These are already discussed.
- Examples of communication devices include a mobile gateway device with interface to WAN technologies, mounted inside the Ambulance.

APIs to be exposed to the Application from platform

For Patient monitoring device: Refer to specific standards for the device type. For example 11073-10404 Device specialization-Pulse-Oximeter.

User Interface

- Physical device User (Ambulance Staff) Interface: ON-OFF Button, Indication of device being working, Low-Battery Indication, Device-Aggregator connection, Display monitor showing the GPS coordinates, Maps in the city and location of the patient and hospital. Map services can provide the shortest path (distance and time) available with expected time of travel.
- Aggregator: Indications for the connection with the Patient monitoring device, Connection to the WAN technologies (GPRS, City-Wi-Fi/ WiMAX, UHF-VHF communication channels) shall be available.
- Emergency Response System/ Central Ambulance management system: Web access to Map services to show the Ambulance locations and traffic condition in the city. The system shall provide access to the Hospital locations on the map and their emergency handling capability and availability of the medical staff. This system may have interface to the central telephone system able to locate the location of the calling phone number registering the emergency call.
- Doctors/Care Giver Interface: User-Interface shall provide the parameters recorded of the patient in parametric and graphical way. These shall high-light any specific data points which are out of range. It may be required to have a video streaming of the patient from ambulance. This is particularly useful for cases of accidents. This helps the doctors to make fair assessment of the patient condition and be prepared for it. This interface is needed for the doctors to do Pan-Zoom-Tilt of the camera to focus on any specific body part of the patient.
- Government bodies: Web Interface for checking the KRA (Key result areas) like the emergency response time, number of ambulances available and active in the city, Any specific locations where mass-requirement of the ambulance were needed (in case of accident of public transport system, fire in building, and terrorist attack etc.)

Communication Infrastructure

Communication Network	Technologies
Personal Area Network	USB, BT, BLE, NFC, Wi-Fi, ZigBee, ANT
Wide Area Network	GPRS, Wi-Fi

Deployment Considerations

In the Ambulance, the deployment of the devices which can sustain the shocks and vibration of the vehicle needs to be done. Since the patient is stationary, wired connectivity can be used like USB for the vital parameters devices to the Aggregation manager.

It can be noted that inside the Automotive Vehicle, the electrical noise can be high, hence the communication channel has to be robust.

Geographical consideration (for geographical spread and concentration of the constituent devices)

The Emergency-response Ambulances shall be distributed evenly in the city based on the population density. The hospital-attached ambulances can be concentrated near their hospitals.

The availability of the ambulance can be monitored and controlled via central emergency services system.

Security

- Proper measures need to be taken so that the device cannot be hacked and controlled from any device other than the designated one.
- The requirements are standard for all the health devices. The device communication in the PAN and WAN shall be secure. The data exchange will be encrypted. The security keys between the communication channels will be defined by the service provider. The communication can be made secure with Encryption technologies like AES or more.
- Criticality: The data is critical for the user and care-giver. This will define the course of action by the medical professionals.
- Security Threat: The hackers may like to interfere with the device communication in PAN and WAN technologies. The PAN network shall be built with authentication keys known to the user (here the ambulance staff).
- The wired technologies can be used inside the ambulance to avoid any wireless communication. If physical interface like USB communication technology used the PAN area security issues can be avoided.
- For WAN, the security requirements are already available.

Startup Shutdown process

The devices are generally battery powered and will be Switched-On when the Ambulance services are required for usage. The Battery power system for the Ambulance infrastructure shall have backup mechanism. In case, the main batteries fail, the power system shall be transferred to the other battery-bank.

This indication shall be available if the battery conditions in the ambulance need maintenance or replacements. This is the responsibility of the ambulance service provider.

The usage of medical devices shall be shut-down when the ambulance usage is over and will be controlled by the ambulance staff.

Data Backup and Archiving

The devices used in ambulance may maintain the history of the data recorded by them. Upon transfer of the information to the EHR System, the data may still be available on the local device memory. The new set of readings needs to be started once the “Patient on board” trigger is activated

There can be local provision to retrieve the data (like USB connectivity) in case of the wireless communication failure. Similarly, a removable memory card can be used for data storage and it can be retrieved for data transfer.

The data being sent to EHR system can be managed by central servers for backup and archiving.

The patient-ID may not be immediately available in case of emergency and hence the data recorded during the emergency may be recorded in the temporary system which can later be transferred to EHR system upon "unique" patient identification being available.

The Ambulance may maintain its own data for the GPS locations with time stamping. This may be logged in central servers with "Ambulance-ID" which shall be unique.

Remote Device Management

Remote device memory space management: Each PHC device memory management may be done locally. The service provider can decide to delete the historical data once the data upload has been done on the EHR System. This can be done using specific applications running on the central console of the Ambulance which may managed remotely in secure manner. In some systems, the service provider may manage the memory of the device. There may be a need for a policy to maintain the minimum days of history of the data for the patients within the Ambulance.

Device Registration and configuration (Master slave, dual master –slave, peer to peer)

Each Ambulance shall have a unique id. There may be a need for a policy on it. A system needs to be in place to assign this unique-id.

Once a new ambulance is commissioned, the registration of the ambulance needs to be done in the central system (hospital and central emergency system) using this unique ID. This is a manual process. This unique ID can be linked to the GPS mounted on the ambulance.

System Availability

Criticality of QoS (Quality of Services)

Remote Patient Monitoring deals with patient data that helps in critical decision making and saving patients' lives. Therefore it is extremely important to have guaranteed response times, have high end connectivity and backup services to enable seamless healthcare data transmission.

Based on patient data monitoring, analysis & interpretation, medical emergencies and hospital readmissions can be avoided by monitoring patient's healthcare data. Similarly, long term care of patient's chronic conditions can be well planned with the same.

Criticality of quality of services is of high importance in Remote Patient Monitoring and focus should be on providing high quality of remote patient monitoring services by deploying the best in class medical devices, softwares, data transmission networks, and high quality clinical staff to provide the clinical interpretation services.

Time Synchronization

The time synchronisation for ambulance can be done using GPS information. The devices may maintain its time locally. The device time can be synchronised with the server by the built-in

function. This is a preferred requirement. The local storage of data will be time-stamped using the local time of the device.

If the data is being updated on the server in real time, the EHR system will record the time as per the server time.

Contracts and Regulations

Ownership of data

The Patient's Medical Condition Data and its derivatives are currently owned by the Hospitals, Healthcare Service providers, and medical device companies who are offering the services in various pockets of the country. Privacy and Security of the data is of concern here.
Many parties owning the data means patient cannot benefit from past health records. There should be a central repository at patient's disposal for his / her data.

The patient should have ownership of the data and should be able to authorise other parties involved in his healthcare decision making such as the doctor, nurse, provider, insurance company, etc.

Patient Safety Requirements

High quality medical devices that have been approved by various medical, technical and legal boards. Data transmission should not pose a threat to patient's health condition (such as high radiation and frequencies). This is more important for continuous monitoring devices.

Constraints

The devices used in ambulance shall be able to work in mobile (Automotive) environment and able to sustain the mechanical vibrations of the moving vehicle.

Challenges

Some of the Challenges anticipated are:

- The central emergency services for Ambulance management not yet established.
- Different healthcare services (Hospitals, Highway Authority, Government services etc.), have their own ambulances and it may lack an integrated control.
- Ambulance numbering system shall be established.

Available Global Standards

Compliance to standard: Name

- HIPAA (the defacto standard to comply with so that it becomes easier to pass the compliance test in other regions).
- Suitable ISO and BIS standards - but these are not well defined for Medical Device based Remote Patient Monitoring Scenarios in India. It is best to follow international standards to be future ready.

- Continua Health Alliance: International non-profit industry organization enabling end-to-end, plug-and-play connectivity of personal health devices, systems and services in Personal Connected Health.
- IEEE 11073 Standards.

11.3. Use Case: Video Conferencing System

Title ID: **UC_Health_VideoConferencing**

Objective

This use case discusses about a remote Tele-health solution, which would assist in bridging patients and healthcare practitioners, across geographies.

Source (as applicable)

Ashish Kumar Mishra, Clarity Medical Pvt. Ltd
HIPAA Parts 160, 162, 164
ITU H.320, H.264, V.80
Recommended Guidelines & Standards for Practice of Telemedicine in India, May, 2003 - Technical working group for Telemedicine Standardization, Department of Information Technology (DIT), Ministry of Communications and Information Technology (MCIT)
Global Observatory for eHealth series, Volume 1 - 6, July - August 2013, World Health Organization

Background

Current Practice

The healthcare facilities are non-uniformly distributed and generally concentrated in large cities. The patients who are immobile or located in remote locations and need a preliminary consultation or basic healthcare services, such as in chronic disease management, will have to travel to a facility which often is located at significant distance. This may cause discomfort to patients and incurs additional money, time and personnel costs.

And even in areas where physicians are accessible, specialised care might be a challenge. Especially, when, a team of multi-disciplinary physicians located at different geographical locations, need to collaborate.

A few organizations have begun implementing this video conferencing technology, but the healthcare demand is far greater than available.

Need for Use Case

A personal, public or inter/intra hospital video conferencing solution would address one or all of the problems mentioned in the “current practice” section, above and more.

Consultation would be easily accessible and if augmented with relevant medical and diagnostic equipment could enable a telemedicine ecosystem. This would also improve universal access of healthcare services and its distribution.

Collaboration among multiple physicians would occur in an efficient manner, in real time and with reduced costs of setup, travel and time. This would help availing specialized care, faster and cost-effective.

Besides, recent advances in technology and infrastructure have made the availability of healthcare services in remote locations, possible.

The guidelines outlined here would help address interoperability, basic operational mechanisms and such subjects, facilitating universal core implementations and encourage the acceptance and growth of the technology, ultimately, to benefit the masses.

Indian Ecosystem Specifics

Following are the few challenges that are India specific:

- Lack of, or limited growth in reliable, extensive and established power and network infrastructure to deploy this technology on a large scale.
- High cost of equipment and subscription services.
- Emphasis on physical presence by both the patient and the health professionals involved.
- Linguistic and socio-cultural differences between the participants, would risk inadequate or inappropriate communication.
- Slow adoption or aversion towards the technology within medical fraternity.
- Availability of trained personnel and staff.
- Lack of definitive and comprehensive policies, guidelines and standards.

Description

The video conferencing solution is a part of a tele-health solution, which would bridge the healthcare practitioners and the patients, across geographies, to make basic healthcare services available. Patients would login to a video conferencing system, where on the other end a doctor would be available for consultation. Trained personnel would assist the patient with connecting to relevant medical and diagnostic equipments that capture the patient's healthcare / physiological data. This data would then be sent over network to the doctor, to assist in the diagnosis of the patient. The doctor can also send reports and prescriptions over network to the patient.

Typically a video conferencing solution, subscribed by patients or doctors, contains:

- Reliable, wired or wireless, network infrastructure, with failover protection.
- Trained personnel, at the user side of the conference, for assisting the user and handling technical components of the system.
- A sufficient setup consisting of a camera and microphone array, a display unit, speakers and a capable hardware and software system.
- A central command centre, where scheduling, QOS, patient/doctor data, technical troubleshooting and such administrative and technical support will be handled.

Actors (as applicable)

Actor Name	Actor Type (person, organization, device, system)	Role Description
Patient	Person	The person seeking preliminary consultation and related healthcare services
Doctor / Physician	Person	The person providing the healthcare

		consulting
Team	People/Organization	A group of related people providing or receiving healthcare service
VCS – Video Conferencing System(a physical entity made of – mic and camera arrays, display units, hardware and software systems and other augmented technologies)	System	System responsible for hosting video conferences and performing additional tasks.
Communication Infrastructure (backbone)	System	This infrastructure forms the back bone of the VCS set-up. It could be a combination of wired and/or wireless telecom infrastructure
Medical Records	System	The Database at the back-end (Could be an hospital based EMR, a Public PHR or any type of Clinical Information System
Command centre	Organization/System	A central organization or system which handles security, scheduling, QOS, user data, troubleshooting and such assistive and administrative tasks.
Augmented equipments	Devices	Medical and diagnostic equipment that will integrate with the VCS to acquire patient data. Also includes printers and other such consumables.
Care Provider / Trained personnel	Organisation/Person	Including Technicians, Care givers, Doctors, Nurses and such who would assist the doctor or patient and handle technical situations

Contextual Illustration – (as applicable)

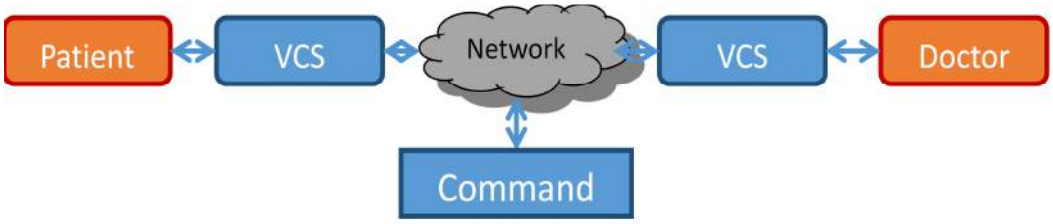

FIGURE 12: VIDEO CONFERENCING ILLUSTRATION

Pre-requisites (Assumptions):

It is assumed that:

- Reliable network connectivity and sufficient bandwidth, among VCS to gateway and the users has been established
- The user has agreed and subscribes to the services provided by a central Command centre or related organization
- The patient and doctor must give consent of every participant and access level, including any 3rd party that might want to join before, during or after conversation
- Adequate medical safety protocols are observed when using the VCS
- Patient and doctor have active unique ID assigned to them for login and authentication purposes

Pre-conditions (if any)

- The VCS must be switched on and validated to be in fully functional state and ready.
- The network connections must be validated for adequate bandwidth and connection quality.
- The medical and diagnostics devices have been cleaned and verified to be fully functional and ready.
- The patients and physicians have been briefed about the communication and are ready.
- Any pending tasks, due to previous video conference sessions have been completed.

Triggers (if any)

When a patient/doctor will request a video conferencing solution access and avails its services.

Scenario description

Normal Scenario (as applicable)

The following illustrates a high level example:

- The patient/doctor , if new users, would request the command centre for a valid and active unique ID for authentication
- The command centre verifies the request and issues a unique ID(UID)
- The patient uses the UID to request the command centre for access to a doctor.
- The command centre verifies the request and schedules a video conference between the doctor and patient
- The patient/doctor is assisted by a trained personnel in preparing for the video conference
- The patient and doctor log into a VCS using the UID
    - The UID and such information will be encrypted and sent to the command centre for authentication decision
- The command centre authenticates them and initiates a connection between both the parties.
- The patient and doctor discuss and exchange data and records
    - All information exchange happens via the command centre.
    - The command centre maintains the privacy and security of the data
    - The command centre logs the data for record purposes
- The discussion ends and they both, log out of the VCS
- The command centre closes the connection

Post-conditions (if any)

- The data of the video conference will be available in a secure, encrypted storage, for future review and record purposes
- The patient and doctor would have arrived at a decision and retain their UIDs
- In case of critical need, Ambulance service should be dispatched

Information Exchange

VCS at patient side:

UID: Unique ID assigned to the patient by the command centre.

Diagnostic: Data acquired by various medical equipments integrated with the VCS.

Miscellaneous user data: Notes and relevant data.

Connection: Data about various connection and device parameters, etc.

VCS at doctor side:

UID: Unique ID assigned to the doctor by the command centre.

Diagnostic: Data uploaded from patient side.

Miscellaneous user data: Notes, Prescriptions, Interpretations and analysis.

Connection: Data about various connection and device parameters, etc.

Command centre:

Connection data: Various parameters and states for QOS, scheduling, etc.

User data: The data exchanged by VCSs.

A/V Data would be compressed based on a trade-off between audio/video quality, cost of compression-decompression and the infrastructure capabilities. May use industry-standard compression technologies like: H.261,H.263,H.264/MPEG-4,H.265 or proprietary.

Buffering, caching and such mechanisms, may be implemented, on both ends, to improve bandwidth utilization, ensure synchronisation of video/audio and enhance live streaming experience.

Patient and doctor generated data and miscellaneous general data, should be compressed using zip or bzip2 or one of the suitable compression algorithms, to further add to reduction in bandwidth and capacity usage.

Architectural considerations (Non-functional Requirements)

Type of Device: Class 1/2/3

- Class 1 – Mostly wellness/ generic healthcare devices.

Communication channel used

- Wired Data Transmission – ISDN, leased line.
- Wireless Data Transmission Channels - Bluetooth, Wi-Fi, VSAT, other high-bandwidth wireless telecom connectivity.

Interface Requirements (as applicable)

- Bluetooth and/or Near Field Communication or any communication technology which can provide secure communication.
- Examples of communication devices include mobile computing devices, such as personal computer, personal digital assistant (PDA), tablet computer, smart phone.
- Long distance communication protocols such as GSM, CDMA.

Communication Infrastructure

Communication Network	Technologies
Personal Area Network	USB, BT, BLE, NFC, Wi-Fi, ZigBee, LAN
Wide Area Network	GPRS/EDGE, Wi-Fi, 3G, 4G, Fixed Line, VSAT

Each VCS endpoint system should have a failover scheme enabled. This will ensure that when one ISP loses connectivity, another ISP can take over and provide the connectivity. If all failover or standby connections lose their connectivity, the relevant data records and such reference data must be stored on the VCS system until such a time, that the data can be uploaded to the Command Centre or the Physician. The ongoing communication must be aborted, if a continuous disconnection interval lasts more than 5 minutes and all parties involved must be notified of the same.

Geographical consideration (for geographical spread and concentration of the constituent devices)

Geographical spread and concentration should of the VCSs not affect its performance or reliability, as they are already taken into consideration when implementing this technology.

Security

Since, the data will be private and critical in nature and transmitted, in general, over internet and other unsecured communication media, most security and safety measures applicable to secure applications on internet, like internet banking, email services and such, would apply.

The machine-to-machine level communication needs to be secured by at least AES 128-bit, SSL, TLS or an equivalent protocol and digital certificates/signatures.

Additionally, the data may be encrypted using a sufficiently strong algorithm, to further protect data in transmission and local machine storage, at user-to-user level.

Adequate virus, malware and such internet security and protection measures must be observed, at all points of contact with internet.

On initiating the videoconference the patient/doctor must identify themselves to each other, for additional identity verification.

Data storage, redundancy, archival and access control techniques may be implemented to ensure data availability, security and such, as may be required, by the user agreement, local law and governing bodies.

Start-up/Shutdown process

The start-up and shutdown of the device should be handled based on the VCS implementation and should be minimal and within 5 minutes.

The occasional power cycling may be required.

VCSs should implement and use a system backup and recovery method, available in the industry. The Command centre will have a data storage and recovery plan.

The VCS may be powered with UPS or inverters, in power failure scenarios, the capacity and specifications of which should be compliant with that of the VCS requirements. The VCS might sense the power levels of such power storage units and may initiate a system shutdown after due notification to the user.

Data Management

Already mentioned in other sections.

Data Backup and Archiving

The device may maintain the history of the data on the local device memory. The oldest data may be overwritten if the device memory is exhausted.

Data storage, redundancy, archival and access control techniques may be implemented to ensure data availability, security and such, as may be required, by the user agreement, local law and governing bodies.

Time Synchronization

The device may maintain its time locally. The device time can be synchronised with the server by the built-in function. This is a preferred requirement. The local storage of data will be time-stamped using the local time of the device.

Contracts and Regulations

Ownership of data

The Patient's Medical Condition Data and its derivatives are currently owned by the Hospitals, Healthcare Service providers, and medical device companies - who are offering the services in various pockets of the country. Privacy and Security of the data is of concern here.

Many parties owning the data means patient cannot benefit from past health records. There should be a central repository at patient's disposal for his / her data.

The patient should have ownership of the data and should be able to authorise other parties involved in his healthcare decision making such as the doctor, nurse, provider, insurance company, etc. Information regarding a person's physical condition, psychological condition, healthcare and treatment shall not be released without the patient's consent.

11.4. Use Case Remote Drug Delivery System

Title ID : UC_Health_RemoteDrugDelivery

Objective

This use case talks about an easy way to provide drugs/medicines to Patients and monitor compliance for people far off from healthcare facilities.

Source (as applicable)

Sumit Dhingra, Reliance Industries Ltd
Alok Mittal, STMicroelectronics

Background

Current Practice

The patients who are on medication for long duration of time, sometimes tend to forget their medication schedule even though there are lot of medication reminders and pill reminders available in the market.

Some drug delivery require longer schedules in specialised environment. This requires longer wait for the patient and it restricts the patient movements.

Need for Use Case

A reservoir that could be remotely triggered to release a drug would enable the patient or physician to achieve on-demand, reproducible, repeated, and tunable dosing. Such a device would allow precise adjustment of dosage to desired effect, with a consequent minimization of toxicity, and could obviate repeated drug administrations or device implantations, enhancing patient compliance. It should exhibit low off-state leakage to minimize basal effects, and tunable on-state release profiles that could be adjusted from pulsatile to sustain in real time. Recently in 2014, a few remote drug delivery systems have been introduced which are still in testing and controlled environment. Few of them are:

- Irradiation based device by NCBI (National Center for Biotechnology Information),
- Microchip based device by MIT spin-off in Massachusetts, backed by the Gates Foundation,

The drug delivery for pain killers for patient suffering from chronic pains need to be administered for a longer duration. Additional techniques like Iontophoresis can help in non-invasive drug delivery and a wearable kit can be worn by the patient. This helps the user to do their routine work with the wearable drug delivery system can provide the pain reliever as per the dosage prescribed by medical practitioner.

Indian Ecosystem Specifics

The majority of drug delivery systems that achieve prolonged release of drugs do so in a passive manner; drug release occurs in a more-or-less sustained manner irrespective of changing circumstances. In particular, the pattern of drug release is beyond the control of the patient or health professionals.

Actor Name	Actor Type (person, organization, device, system)	Role Description
Patient	Person	The person whose vitals are to be monitored. The monitoring could be in a clinical or non-clinical setting
Device (– Implant, Wearable device, microchip or membrane based)	Device	Device responsible for initiating or controlling the drug delivery Implanted or worn by the Patient for the required drug-delivery system Interfaces with a Medical Gateway via wired (Serial, USB) or wireless (BT, BLE, ZigBee) and these devices may either be single or multi parameter monitors. These devices may use proprietary protocol to communicate with the Gateway or use a standard protocol like ISO/IEEE 11073
Medical Gateway	Device	The Device that interfaces with the Vital Monitors at the patient end, aggregates the information and communicates with the back end system (EHR / PHR / CIS). This Gateway could be a dedicated hardware-based device, or software on a PC or Mobile Platform.
Communication Infrastructure (backbone)	System	This infrastructure forms the back bone of the RPM set-up and drug-delivery. It could be a combination of Land-line / mobile telecom infrastructure
Medical Records	System	The Database at the back-end (Could be an hospital based EMR, a Public PHR or any type of Clinical Information System
Remote monitoring and control unit / microprocessor or biosensor	Device	Application Framework or Device which can receive the commands and configuration parameters from the healthcare professional and responsible to communicate with the drug delivery device and provide the required commands
Care Provider / Clinician	Organisation or Person	Including Doctors, Nurses and other clinical staff who are involved in monitoring the vitals and responsible for the following: 1. Trigger the initiation of the drug delivery 2. Program or control manually the drug

		delivery 3. To check and maintain history of drug delivery 4. Configure the System for drug type, delivery time / dosage, application time

However, there are many situations (e.g., endocrine disorders, pain) in which drug release would ideally be provided on demand, or situations in which the magnitude of drug release would best be readily controllable at a specific endpoint. Apart from allowing optimal matching of treatment to need, such control could reduce side effects by minimizing excessive dosing. Moreover, a device that is administered once (e.g., by surgery or injection) and then triggered remotely could increase patient compliance, particularly in cases in which conventional administration is painful or inconvenient, or for elderly or mentally disabled patients.

Recent advances in materials science have enabled systems that respond to external stimuli such as electromagnetic fields, voltage potential like in Iontophoresis or ultrasound. They have been realized as microchips, liposomes, micro particles, nanoparticles, and macro scale polymers that release loaded drugs when the stimulus is applied. In principle, these materials enable control over the dose and timing of drug release and therefore can be used to achieve complex drug release regimens not possible with conventional passive sustained-release systems. However, most triggered systems reported to date release drug only in a burst rather than in continuous fashion, or only function for a single release event, or exhibit a poor ratio between on- and off-state release kinetics, and lack reproducibility over multiple release cycles.

Description

Remote drug delivery device should support:

- Triggered release
- Low off stage leakage
- Range of drug release profiles
- Non-invasive trigger ability within the body
- Different therapeutic window for different types of patients
- No on board power source or logic
- Duration of drug release

Actors (as applicable)

Contextual Illustration

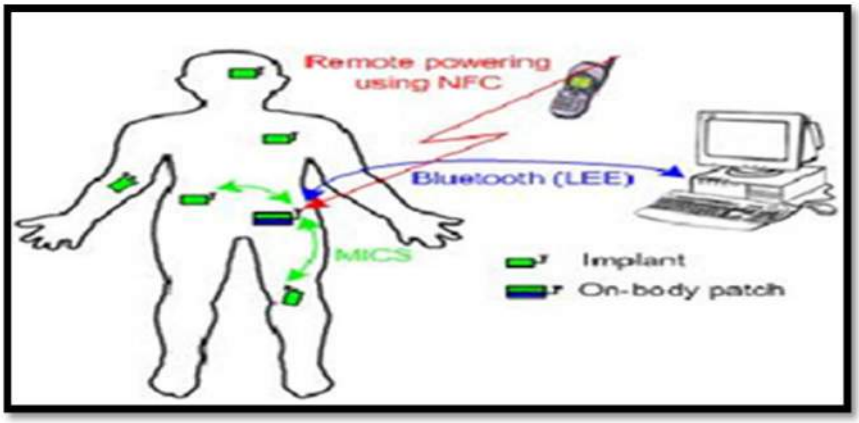

FIGURE 13: REMOTE DRUG DELIVERY ILLUSTRATION

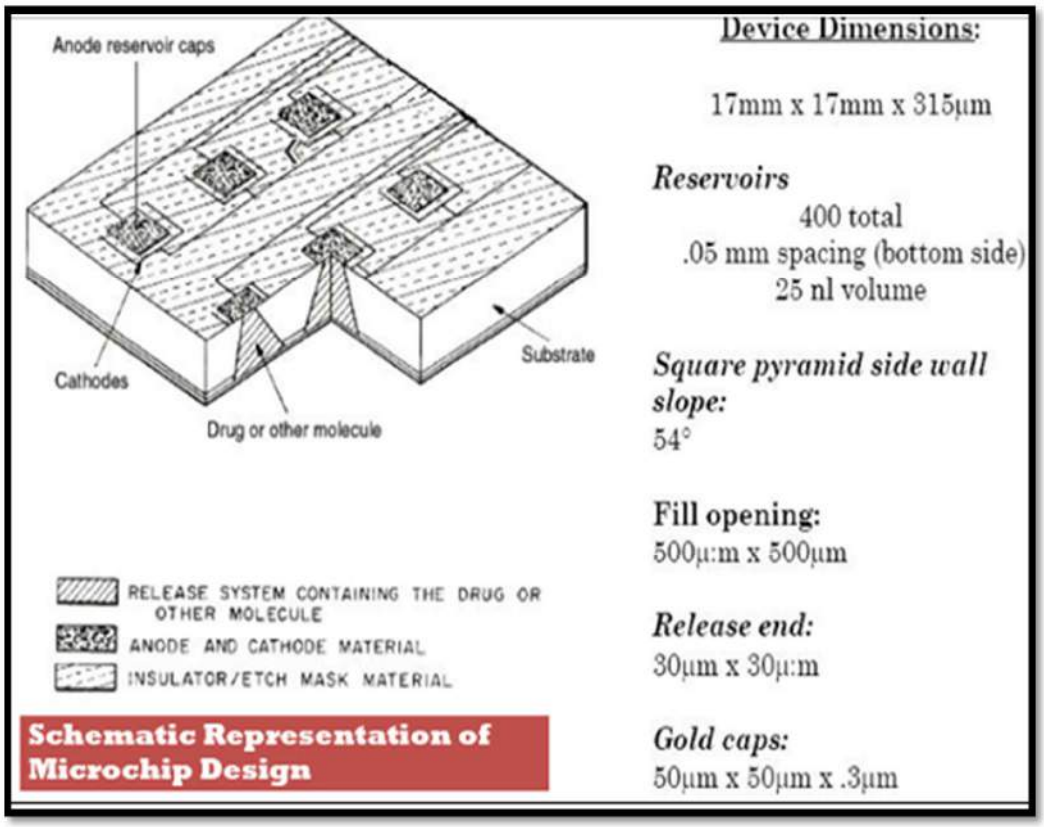

FIGURE 14 : GENERALIZED VIEW OF MICROCHIP TECHNOLOGY

Pre-requisites (Assumptions):

It is assumed that:

- The wearable or implanted device for drug delivery device is being worn/ used by the User appropriately.

- The Device to aggregator communication is working and user is able to identify the communication channel availability.
- The initial pairing of the device from the monitoring-device to the aggregator device is done during the system installation and configuration.
- The WAN connectivity is available from aggregator to the EHR system and to healthcare professionals
- The user has agreed by contract to subscribe to the health parameter monitoring, records updation and remote drug delivery
- When a "personal" device is being used, the user identity is managed by the unique ID of the personal device which is either updated in the Cloud-application by way of assigning the device ID to the specific user

Pre-conditions (if any)

Same as above

Triggers (if any)

When a personal device is being used (Switched-On) this will trigger the use-case for collecting the data and sending it to the servers

Post-conditions (if any)

- The data from the personal health device is being uploaded in the EHR System with time stamping
- The required amount of drug is delivered to the user via wearable device

Information Exchange

Drug delivery device/dispenser:

- Drug Identifier tag: Drug to be given.
- Drug Quantity: Drug quantity in units.
- Drug duration: Duration in which the specified quantity is to be dispatched.

Service Provider:

- Disease/Condition: Based on which the drug is chosen.
- Drug Data (includes all above).

Remote control:

- Drug initiation.

Architectural considerations (Non-functional Requirements)

Type of Device: Class 1/2/3

- Class 2 – Wearable devices delivering Pain relievers etc.
- Class 3 – Data from implants other critical devices.

Communication channel used

- Wired communication like USB etc.

- Wireless Data Transmission Channels such as Bluetooth Low Energy, Wi-Fi, NFC.

Interface Requirements (as applicable)

- Bluetooth and/or Near Field Communication or any communication technology which can provide secure communication.
- Examples of communication devices include mobile computing devices, such as personal computer, personal digital assistant (PDA), tablet computer, smart phone, integrated circuit card, and so on.
- Examples of wired communication links include cable connections such USB connection, RS 232 cable connection, and so on.
- Examples of wireless communication links include near field communication (NFC), Bluetooth, Infrared, ZigBee, and the like, and long distance communication protocols such as GSM, CDMA, and the like via Gateway.

User Interface

- Physical device User-Interface: ON-OFF Button, Indication of device being working, Low-Battery Indication, Device-Aggregator connection.
- Aggregator: Communication channel (BT, BLE, Wi-Fi etc) interfaces, Connection to the WAN technologies (GPRS, Wi-Fi) shall be available, App shall be downloaded (when Mobile phone is used as Aggregator).
- Doctors/Care Giver Interface: Providing specific data points with the parameters which are within the Range or out of range.

Communication Infrastructure

Communication Network	Technologies
Personal Area Network	USB, BT, BLE, NFC, Wi-Fi, ZigBee, ANT
Wide Area Network	GPRS, Wi-Fi

Geographical consideration (for geographical spread and concentration of the constituent devices)

This healthcare device is a personal device, it shall not affect any limitations or challenges for the geographical spread.

The WAN connectedly is assumed to be available and enough to carry the data from all users in case of concentration of the devices.

In addition, the data packets in health devices are small and transmissions are sporadic in nature. No specific challenge for the geographical consideration is expected.

Security

- Security: Proper measures need to be taken so that the device cannot be hacked and controlled from any device other than the designated one.The requirements are standard

for all the health devices. The device communication in the PAN and WAN shall be secure. The data exchange will be encrypted. The security keys between the communication channels will be defined by the service provider. The communication between the Remote device and the drug dispenser needs to be secure with Encryption like AES-128bit or more.

- Criticality: The data is critical for the user and care-giver. This will define the course of action by the medical professionals.
- Security Threat: The hackers may like to interfere with the device communication in PAN and WAN technologies. The PAN network shall be built with authentication keys known to the user by way of pairing.
- Physical pairing can also be done using the NFC technologies.
- For WAN, the security requirements are already available.

Start-up Shutdown process

The devices are generally battery powered and no-power cycling is expected. The Battery charging or replacement shall be the responsibility of the user.

The control circuitry consists of a computing unit, drug delivery dispenser or an input source and battery. The computing unit will control the desired reservoir to be activated so that a variety of drugs may be contained in each specific reservoir. The input source can either be a memory source, remote control device or a biosensor. A thin-film micro battery (thin-film micro, or any chargeable or rechargeable) can be used as a power source. All of these can be patterned directly onto the device.

Device Remote Health monitoring and troubleshooting

For most of the personal care systems, the battery charging shall be managed by the user. The device may provide the indication for “low battery” and prompt the user to charge the device or replace the batteries.

The device battery life can be monitored remotely for certain devices. This is mandatory for the systems where user cannot charge the device. The data exchange from the device to the server will include the battery status. This enables the service-provider to initiate the actions for the device replacement.

The system at care provider’s end connected to the microchip via wireless network will handle the monitoring and troubleshooting.

Contracts and Regulations

Contracts and Regulations	Impact on Use case
Guidance for Industry and FDA Staff: Class II Special Controls Guidance Document: Remote Medication Management System Document issued on: October 19, 2007	

Ownership of data

The Patient's Medical Condition Data and its derivatives are currently owned by the Hospitals, Healthcare Service providers, and medical device companies - who are offering the services in various pockets of the country. Privacy and Security of the data is of concern here.

Many parties owning the data means patient cannot benefit from past health records. There should be a central repository at patient's disposal for his / her data.

The patient should have ownership of the data and should be able to authorise other parties involved in his healthcare decision making such as the doctor, nurse, provider, insurance company, etc.

Patient Safety Requirements

High quality medical devices that have been approved by various medical, technical and legal boards. The drug shall be delivered as per the prescribed time, duration and quantity to avoid over-dose.

Challenges

Some of the Challenges anticipated are:

- No single commercialized product yet for remote drug delivery system in India
- Risk in controlling and troubleshooting the device

Available Global Standards

Compliance to standard: Name

- HIPAA (the defacto standard to comply with so that it becomes easier to pass the compliance test in other regions)
- Suitable ISO and BIS standards - but these are not well defined for Medical Device based Remote Patient Monitoring Scenarios in India. It is best to follow international standards to be future ready.
- Continua Health Alliance: International non-profit industry organization enabling end-to-end, plug-and-play connectivity of personal health devices, systems and services in Personal Connected Health.

  IEEE 11073 Standards

12. Abbreviations

Abbreviation	Full Name
AHD	Application Hosting Device
BT	Bluetooth
BTLE	Bluetooth Low Energy
ECG	Electrocardiography
EHR	Electronic Health Record
EMR	Electronic medical records
HIE	Health information exchange
HRN	Health Record Network
ISM	Industrial, Scientific and Medical Band of Spectrum Like 2.4GHz, 865-868MHz
ITU	International Telecommunications Union
LAN	Local Area Network
M2M	Machine-to-Machine
NFC	Near Field Communication
PAN	Personal Area Network
PCH	Personal Connected Health
PHI	Protected Health Information
QOS	Quality of Service
RMD	Remote Monitoring Device
Sub-Gig	Sub Giga Hz Radio Communication
TAN	Touch Area Network
USB	Universal Serial Bus
WAN	Wide Area Network

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA