International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# Y.2065

(03/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

## Service and capability requirements for e-health monitoring services

Recommendation ITU-T Y.2065

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS**

| | |
|---|---|
| GLOBAL INFORMATION INFRASTRUCTURE | |
| General | Y.100–Y.199 |
| Services, applications and middleware | Y.200–Y.299 |
| Network aspects | Y.300–Y.399 |
| Interfaces and protocols | Y.400–Y.499 |
| Numbering, addressing and naming | Y.500–Y.599 |
| Operation, administration and maintenance | Y.600–Y.699 |
| Security | Y.700–Y.799 |
| Performances | Y.800–Y.899 |
| INTERNET PROTOCOL ASPECTS | |
| General | Y.1000–Y.1099 |
| Services and applications | Y.1100–Y.1199 |
| Architecture, access, network capabilities and resource management | Y.1200–Y.1299 |
| Transport | Y.1300–Y.1399 |
| Interworking | Y.1400–Y.1499 |
| Quality of service and network performance | Y.1500–Y.1599 |
| Signalling | Y.1600–Y.1699 |
| Operation, administration and maintenance | Y.1700–Y.1799 |
| Charging | Y.1800–Y.1899 |
| IPTV over NGN | Y.1900–Y.1999 |
| NEXT GENERATION NETWORKS | |
| **Frameworks and functional architecture models** | **Y.2000–Y.2099** |
| Quality of Service and performance | Y.2100–Y.2199 |
| Service aspects: Service capabilities and service architecture | Y.2200–Y.2249 |
| Service aspects: Interoperability of services and networks in NGN | Y.2250–Y.2299 |
| Enhancements to NGN | Y.2300–Y.2399 |
| Network management | Y.2400–Y.2499 |
| Network control architectures and protocols | Y.2500–Y.2599 |
| Packet-based Networks | Y.2600–Y.2699 |
| Security | Y.2700–Y.2799 |
| Generalized mobility | Y.2800–Y.2899 |
| Carrier grade open environment | Y.2900–Y.2999 |
| FUTURE NETWORKS | Y.3000–Y.3499 |
| CLOUD COMPUTING | Y.3500–Y.3999 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T Y.2065

## Service and capability requirements for e-health monitoring services


### Summary

Recommendation ITU-T Y.2065 provides service and capability requirements for e-health monitoring services.

Three classes of e-health monitoring services, including their general and specific characteristics, are described. Service requirements for the support of e-health monitoring services are also described, and based on the identified service requirements, the capability requirements are specified.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T Y.2065 | 2014-03-22 | 13 | 11.1002/1000/12072 |

### Keywords

Capability requirements, e-health monitoring services, service requirements.


* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

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

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T Y.2065

## Service and capability requirements for e-health monitoring services

### 1 Scope

This Recommendation describes the service requirements for the support of e-health monitoring services, and it specifies the corresponding capability requirements.

The scope of this Recommendation includes:

– classification of e-health monitoring services;

– description of characteristics of e-health monitoring services;

– service requirements for supporting e-health monitoring services;

– capability requirements for supporting e-health monitoring services.

Relevant service scenarios of e-health monitoring services are provided in Appendix I.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 device** [ITU-T Y.2060]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

**3.1.2 Internet of things (IoT)** [ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 e-health monitoring (EHM) service**: A service which consists of observing and recording information based on a customer's physiological data, environmental data and other data, with the aim of monitoring the customer's state of health through the use of information and communication technologies.

**3.2.2 e-health monitoring healthcare (EHMH) service**: A class of EHM services providing the customer with health monitoring services for a 'healthy' state.

**3.2.3 e-health monitoring rehabilitation (EHMR) service**: A class of EHM services providing the customer with health monitoring services for a 'not fully healthy' or 'in recovery' state of health.

**3.2.4 e-health monitoring treatment (EHMT) service**: A class of EHM services providing the customer with health monitoring services for an 'illness' state of health.

**3.2.5 EHM system**: A set of hardware and software components which constitute as a whole the technical chain of e-health monitoring (EHM) service provisioning.

NOTE – EHM systems include EHM devices, gateways, networks, service support platforms and EHM applications.

**3.2.6 EHM device**: A device, as defined in [ITU-T Y.2060], which has sufficient qualification for e-health monitoring (EHM) service provisioning.

NOTE – Examples include EHM devices for EHMH (i.e., EHM devices which have sufficient qualification for EHMH), EHM devices for EHMT and EHM devices for EHMR.

**3.2.7 EHM terminal**: An e-health monitoring (EHM) device directly connected to the communication network.

**3.2.8 EHM end point**: An e-health monitoring (EHM) device connected to the communication network through gateway(s).

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| CT | Computed Tomography |
| ECG | Electrocardiogram |
| EHM | e-health Monitoring |
| EHMH | e-health Monitoring Healthcare |
| EHMR | e-health Monitoring Rehabilitation |
| EHMT | e-health Monitoring Treatment |
| EMR | Electronic Medical Record |
| EMSS | Emergency Medical Service System |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile communications |
| ICT | Information and Communication Technology |
| IP | Internet Protocol |
| IoT | Internet of Things |

| | |
|---|---|
| MRI | Magnetic Resonance Imaging |
| PDA | Personal Digital Assistant |
| PEMS | Pre-hospital Emergency Medical Service |
| QoS | Quality of Service |
| RFID | Radio Frequency Identification |
| SSAS | Service Support and Application Support |
| UMTS | Universal Mobile Telecommunications System |
| WAN | Wide Area Network |
| WSN | Wireless Sensor Network |

## 5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

## 6 Classification of e-health monitoring services

This clause introduces a classification of e-health monitoring (EHM) services. The main purpose of this classification is to simplify the analysis of service network requirements and capability requirements for the support of EHM services.

For this classification of EHM services, two factors are considered: completeness and independency. Completeness means that the identified classes of EHM services cover all possible EHM services. Independency means that the identified classes of EHM services do not overlap with each other; in other words, each class has unique features specific to the EHM services of that class.

In this classification, human health is seen in one of four possible states: healthy, in recovery, not fully healthy, and illness. Each state has some service requirements which are unique to that state. These four states can be mapped into three EHM service classes which meet the two factors of completeness and independency: EHM healthcare, EHM rehabilitation and EHM treatment. Figure 6-1 shows these four human states of health and the corresponding EHM service classes.

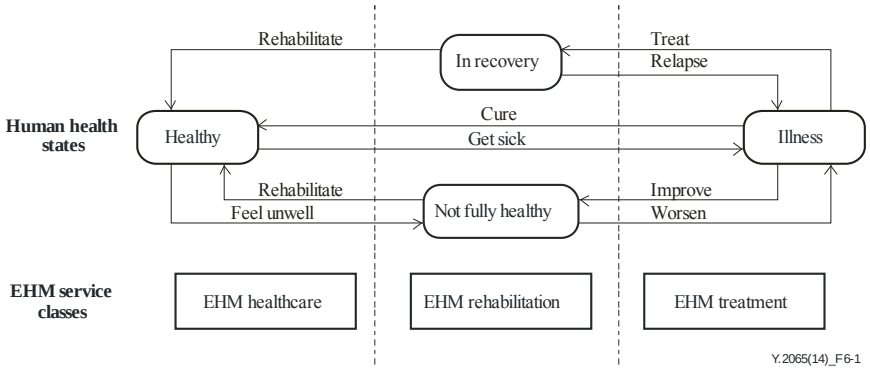


**Figure 6-1 – Human states of health and corresponding EHM service classes**

NOTE 1 – These EHM service classes have different characteristics, e.g., in terms of the number and type of target customers, target customers' mobility and the timing of service feedback to customers. Different service requirements are identified for each class.

NOTE 2 – EHM service classification does not sufficiently address health emergency situations. In such situations, there are a large number of requirements to be satisfied which are beyond the specific scope of e-health monitoring services.

## 6.1 EHM healthcare (EHMH) services

The target people of EHMH services are those in good health (healthy) but who pay close attention to their health status or those who still require some attention in that they are potentially at risk of getting diseases.

NOTE – EHMH services are usually provided by social and commercial organizations offering daily health-care services to people without on-site care.

## 6.2 EHM rehabilitation (EHMR) services

The target people of EHMR services include people with chronic diseases (not fully healthy state of health), and others who need on-site care (in recovery state of health).

NOTE – EHMR services may be provided by qualified organizations, such as rehabilitation centres, physical examination agencies, community medical stations and so on.

## 6.3 EHM treatment (EHMT) services

The target people of EHMT services include those who are hospitalized (illness state of health) and need medical services.

NOTE – EHMT services may be provided by qualified professional organizations, e.g., hospitals, medical emergency centres and so on.

# 7 Characteristics of e-health monitoring services

## 7.1 General characteristics

### 7.1.1 A class of services exploiting the capabilities of the IoT

EHM services exploit the identification, data capture, data processing and communication capabilities of the IoT [ITU-T Y.2060] to monitor customers' health, whilst maintaining the required privacy.

EHM services involve capabilities at all layers of the IoT reference model [ITU-T Y.2060], i.e., at the device layer, network layer, service support and application support layer and the application layer, whilst having some unique service requirements and capability requirements with respect to other classes of services which are exploiting the capabilities of the IoT.

### 7.1.2 Support of data sharing

The data generated by EHM services can be shared among different EHM services according to regulations, laws and other requirements.

### 7.1.3 Enhanced value via service support and application support layer capabilities

The service support and application support layer [ITU-T Y.2060] is key to the infrastructure of the IoT. Based on the capabilities of the service support and application support layer, the capabilities of the EHM services, e.g., data sharing and data communication, are enhanced in terms of efficiency, reliability and safety.

### 7.1.4 Enhanced value via network layer capabilities

In order to support customer access to EHM services remotely and locally, the network acts as a data transmission channel.

Based on the network layer capabilities, e.g., policy-based communication, network-based locating and network resource provisioning, the capabilities of EHM services are enhanced, e.g., in terms of network intelligence.

### 7.1.5 Combination of health-related technology and ICT

EHM services make use of both health monitoring-related technologies and information and communication technologies (ICTs); this implies that EHM services have to comply not only with ICT technical specifications but also with health-related specifications.

### 7.1.6 Multiple EHM devices serving one single user

Multiple EHM devices can serve one single user in a collaborative way.

Many EHM devices have a single function. For example, a blood pressure monitor measures blood pressure but it does not collect other physical health signals, such as ECG information, blood-oxygen levels, information on posture and so on. This implies that multiple EHM devices may be associated with one single user in a collaborative way to gather health information.

### 7.1.7 Users with different accessibility needs

Since EHM services address people with different accessibility needs, they have to be capable of meeting those needs accordingly.

### 7.1.8 Regulated services

Various EHM service aspects, including device, application and other aspects, are regulated by specific entities according to regulation and laws. Different types of EHM services may need to follow different regulation policies.

## 7.2 Specific characteristics of EHM services

### 7.2.1 Characteristics of EHM healthcare services

1) Service and network scalability

Compared to EHMT and EHMR services, the number of service providers and customers involved with EHMH services may be very large, as there are less professional and administrative constraints associated with these services. Consequently, service and network scalability is a key concern.

2) Wide service coverage

The EHMH users may access the services from a wide range of locations including home, school, office, train, vehicles and so on.

3) Data transmission with high reliability requirements and weak latency constraints

EHMH services need data transmission with high reliability but which also allows high latency.

– Data of EHMH services are transmitted without faults.

– EHMH services have weaker latency constraints than EHMT and EHMR services.

4) Unguaranteed support of clinical intervention

The EHMH services do not guarantee support of clinical intervention for customers.

### 7.2.2 Characteristics of EHM rehabilitation services

1) Access to data produced by EHMT and EHMH services

EHMR services may benefit from accessing data which have been produced by EHMH and EHMT services.

2) Restricted service coverage

EHMR services may be provided to users in qualified locations.

NOTE 1 – Inside qualified service buildings, users can usually obtain EHMR services with full capabilities. In other locations, users may access EHMR services with partial capabilities.

3) Support of clinical intervention

EHMR services provide support for clinical intervention to users.

4) Data transmission with high reliability requirements and medium latency constraints

EHMR services need data transmission with high reliability and which allows medium latency.

– Data of EHMR services are transmitted without faults.

– EHMR services have a stricter latency requirement than EHMH services, but a looser latency requirement than EHMT services.

### 7.2.3 Characteristics of EHM treatment services

1) Centralized management

EHMT services have usually centralized management inside organizations providing these services.

2) Medical imaging

Medical imaging devices used in EHMT services, such as CT, MRI, ultrasonic devices and so on, usually generate big data streams.

– Big data streams are generated among departments inside a hospital or among hospitals, as well as between hospital and emergency cars, and between disaster sites and hospital or emergency cars.

3) Data transmission with high reliability and low latency requirements

EHMT services need data transmission with high reliability and low latency requirements.

– EHMT services have the highest requirements of latency compared to EHMH and EHMR services.

## 8 Service requirements for support of e-health monitoring services

### 8.1 EHM roles

The roles participating in EHM services include EHM customer, EHM device provider, network provider, platform provider and EHM application provider.

These EHM roles can be mapped to the IoT business roles introduced in Appendix I of [ITU-T Y.2060], as shown in Figure 8-1.

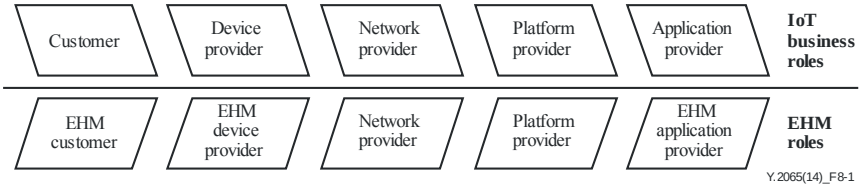


**Figure 8-1 – Mapping between EHM roles and IoT business roles**

The EHM customer is the end user of EHM services.

NOTE – For the purposes of this Recommendation, a healthy person, an in recovery or not fully healthy person, and a hospitalized person are the three actors which are considered as playing the role of an EHM customer.

The EHM device provider manages the EHM devices.

The network provider provides network access and connectivity for EHM devices, and provides network connections for the service support platform and for EHM applications.

The platform provider provides general service capabilities and EHM-dedicated service capabilities.

The EHM application provider provides EHM applications.

## 8.2 Service requirements of EHM customers

The following EHM customer requirements are essential for the support of EHM services.

### 8.2.1 Service requirements of a healthy person

A healthy person who is willing to use EHMH services to monitor his/her health condition is the target user of EHMH services.

1) A healthy person needs support to connect to the EHMH applications of EHM devices for EHMH in a convenient way; this includes meeting any accessibility needs. For usability, EHM services should be understandable in layman's terms.

2) A healthy person needs support for EHMH service access regardless of his/her location.

   NOTE 1 – Healthy people can use EHMH services continuously whether they work in a local city or travel or settle down in another city or country.

3) A healthy person needs support for information sharing.

   NOTE 2 – For example, the data generated by EHMR and EHMT services can be accessed by EHMH services as reference data.

4) A healthy person needs support in receiving one single bill regardless of the number of devices used.

5) A healthy person needs support for his/her location to be tracked.

   NOTE 3 – Based on the location information, EHMH services can send out messages for help if needed.

6) A healthy person needs support for fault recovery of used devices as soon as possible.

7) A healthy person needs support for personal information protection.

### 8.2.2 Service requirements of an in recovery or not fully healthy person

An in recovery or not fully healthy person is the target user of EHMR services.

1) An in recovery or not fully healthy person needs support to connect to the EHMR applications of EHM devices for EHMR in a convenient way; this includes meeting any accessibility needs. An in recovery or not fully healthy person needs support for EHMR connectivity.

2) An in recovery or not fully healthy person needs support for EHMR service access regardless of his/her location.

NOTE 1 – An in recovery or not fully healthy person can use EHMR services continuously whether he/she works in a local city or travels or settles down in another city or country. He/she wishes to have the same service experience throughout their use of the services.

3) An in recovery or not fully healthy person needs support for information sharing.

NOTE 2 – For example, the data generated by EHMH and EHMT services can be accessed by EHMR services as reference data.

4) An in recovery or not fully healthy person needs support in receiving one single bill regardless of the number of devices used.

5) An in recovery or not fully healthy person needs support for his/her location to be tracked.

NOTE 3 – Based on the location information, an in recovery or not fully healthy person can receive first aid in an emergency situation.

6) An in recovery or not fully healthy person needs support for fault recovery of used devices as soon as possible.

7) An in recovery or not fully healthy person needs support for personal information protection.

### 8.2.3 Service requirements of a hospitalized person

A hospitalized person who is under treatment in medical facilities such as hospitals, medical emergency centres or ambulances, is the target user of EHMT services.

1) A hospitalized person needs support to connect to the EHMT applications of EHM devices for EHMT in a convenient way; this includes meeting any accessibility needs.

2) A hospitalized person needs support for obtaining reliable EHMT services.

3) A hospitalized person needs support for information sharing.

NOTE 1 – For example, the data generated by EHMH and EHMR services can be accessed by EHMT services as reference data.

4) When a hospitalized person uses multiple EHM devices for EHMT at the same time, time synchronization among EHM devices is needed.

NOTE 2 – Parameters gathered by multiple EHM devices for EHMT need to be synchronized to reflect the value of the different physiological parameters at the same time.

5) A hospitalized person needs support for his/her location to be tracked so that, e.g., he/she can get first aid in an emergency situation.

6) A hospitalized person needs support for fault recovery of used devices as soon as possible.

7) A hospitalized person needs support for personal information protection.

8) A hospitalized person needs support for the availability of EHM devices.

## 8.3 Service requirements of an EHM device provider

The following EHM device provider requirements are essential for the support of EHM services.

1) In order to reduce EHM device costs and to provide support for interoperability with service support platforms, EHM applications and other EHM devices, the EHM device provider needs support for EHM devices which reuse common purpose capabilities as much as possible.

2) When EHM device updates of software or firmware take place, the EHM device provider needs support for notifying the EHM application provider and EHM customer.

3) The EHM device provider needs support for EHM device reliability and security according to technical standards requirements.

4) The EHM device provider needs support for open interfaces to EHM device capabilities in order to enable EHM device capabilities' access by EHM applications, service support platforms, networks and other devices.

5) The EHM device provider needs support for the collection of fault information from devices, networks, service support platforms and application to give verdict on whether the root of an accident comes from the devices.

6) The EHM device provider needs support for acquiring the information related to device initialization and registration from the application provider, platform provider and network provider.

7) The EHM device provider needs support for the time calibration of EHM devices.

## 8.4 Service requirements of a network provider

### 8.4.1 Network provider essential requirements

The following network provider requirements are essential for the support of EHM services.

1) The network provider needs support for distinguishing which EHM service is in use (i.e., EHMH, EHMR and EHMT). This is for example, to guarantee the EHM service's QoS and EHM customer's QoE.

### 8.4.2 Network provider's essential but not EHM specific requirements

The following network provider requirements are essential for the support of EHM services but not specific to EHM services.

1) The network provider needs support for providing access to EHM applications as fast as possible upon service request.

2) The network provider needs support for obtaining the customer's EHM service-related information in order to allocate or configure for the EHM customer the appropriate network resources, such as IP address, network bandwidth, QoS policy, and so on.

3) The network provider needs support for flexible accounting for an EHM application provider and EHM customer.

4) The network provider needs support for the collection of fault information from devices, networks, service support platforms and applications to give verdict on whether the root of an accident comes from the network.

5) The network provider needs support for the remote update of an EHM customer's network subscription information residing in the EHM customer's device.

## 8.5 Service requirements of a platform provider

The following platform provider requirements are essential for the support of EHM services.

1) In addition to IoT common service capabilities, the platform provider needs to provide EHM dedicated service capabilities for EHM services.

2) The platform provider needs support for EHM service information sharing.

3) The platform provider needs support for data storage of EHM service information, e.g., to ensure EHM service information is not lost or inconsistent.

4) The platform provider needs support for the collection of fault information from devices, networks, service support platforms and applications to give verdict on whether the root of an accident comes from the service support platform.

5) The platform provider needs support for time synchronization for EHM devices, service support platforms and application servers.

### 8.6 Service requirements of an EHM application provider

#### 8.6.1 EHM application provider's essential requirements

The following EHM application provider requirements are essential for the support of EHM services.

1) The EHM application provider needs support for EHM service information sharing.
2) The EHM application provider needs support for the collection of fault information from devices, networks, service support platforms and applications to give verdict on whether the root of an accident comes from the application.
3) The EHM application provider needs support for protecting the EHM customer's personal information.
4) The EHM application provider needs support for registration management of an EHM customer's devices.
5) The EHM application provider needs support for distinguishing the accuracy of the EHM data collected by the EHM devices.
6) The EHM application provider needs support for time synchronization of the EHM data provided to EHM applications by EHM devices.

#### 8.6.2 EHM application provider's essential but not EHM specific requirements

The following EHM application provider requirements are essential for the support of EHM services but are not specific to EHM services.

1) The EHM application provider needs support for the upgrade of software/firmware hosted in EHM devices.
2) The EHM application provider needs support for flexible accounting from the network provider and/or platform provider.
3) The EHM application provider needs support for EHM service access which is independent of the EHM application's location, i.e., EHM applications need to be accessed by EHM customers continuously no matter where the EHM applications are located.
4) The EHM application provider needs support for network switching mechanisms in order to be able to change the network provider to which applications can subscribe.
5) The EHM application provider needs support for getting the location information of EHM customers.

## 9 Capability requirements for support of e-health monitoring services

### 9.1 Introduction to the EHM capabilities

The following subclauses describe the EHM capability requirements according to the IoT reference model [ITU-T Y.2060].

The EHM reference model, shown in Figure 9-1, exhibits two types of capabilities, EHM essential IoT capabilities derived from the EHM service requirements and EHM not essential IoT capabilities. They are located at the various layers of the IoT reference model [ITU-T Y.2060].

NOTE 1 – The EHM reference model excludes on purpose the IoT capabilities which are not related to the specific support of EHM services. Consequently, this clause does not cover other IoT common capabilities which are still necessary to support EHM services.

NOTE 2 – The distinction between EHM essential IoT capabilities and EHM not essential IoT capabilities concerning the capabilities described in each of the following subclauses is beyond the scope of this Recommendation.

In Figure 9-1, rounded rectangles represent layers (i.e., application layer, service support and application support (SSAS) layer, network layer, device layer) according to the IoT reference model; rectangles represent capabilities provided by the various layers of the IoT reference model, as well as security and management capabilities.

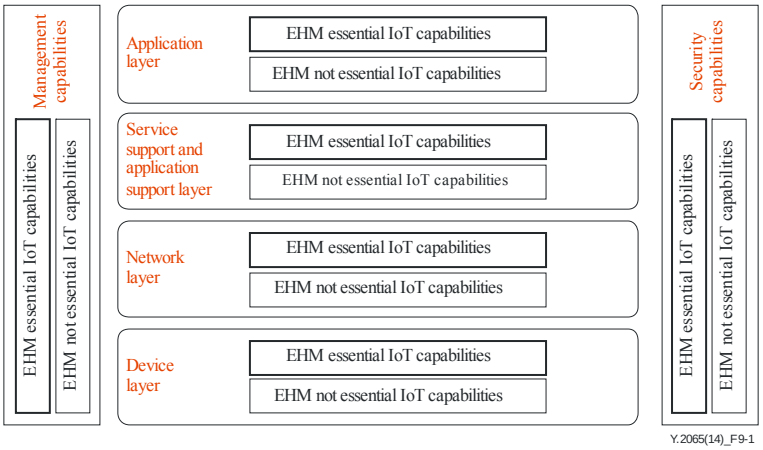


**Figure 9-1 – EHM reference model**

## 9.2 Capabilities of the application layer

### 9.2.1 Information sharing

Information sharing is one of the basic capability requirements for EHM. According to the service requirements 8.6.1(1), 8.2.1(3), 8.2.2(3), 8.2.3(3), the application layer is required to provide standard interfaces and policy-based mechanisms to enable the sharing of EHM information among different EHM services. Examples of policy rules for policy-based mechanisms include, but are not limited to, government rules, privacy rules, commercial agreements between application providers and so on.

### 9.2.2 Accounting related information provision

According to service requirements 8.6.2(2), 8.2.1(4), 8.2.2(4), the application layer is recommended to report accounting related information to the SSAS layer. The accounting related information includes, but is not limited to, application type (EHMH, EHMR and EHMT), the number of times that the application is used, the time during which the application is used, etc.

### 9.2.3 QoS information provision

According to service requirements 8.4.2(2), 8.4.1(1), 8.2.3(2), the QoS information for EHM services is required to be configured by the application layer and provided to the other layers, so that the other layers can ensure the QoS of EHM services according to the QoS information provided by the application layer.

The following QoS related parameters are recommended to be indicated in the provided QoS information:

1) Required response time

   As different types of EHM services need to be dealt with in different time periods, response time is an important criterion in reckoning the requirements of an EHM service.

2) Allowed dispose time

   Dispose time is the time period from the moment when data arrive at the server to the moment when doctors or application providers execute an appropriate reaction. Generally speaking, dispose time includes the time to analyse data, the time to store data in the storage area, the time to send an alarm to doctors when unusual results are deduced, and so

on. Dispose time as part of the response time is very important in reckoning the EHM application capabilities.

3) Instantaneity level

Instantaneity level indicates the level of priority of the EHM application when the EHM application related data are transmitted, processed and queued.

4) Minimum transmission rate

In some EHM scenarios (i.e., in an emergency car or disaster rescue), the voice, video or dynamic monitoring data need be transmitted to the remote server for diagnosis and treatment in real time. To ensure real-time data transmission, a minimum transmission rate is required to be indicated.

5) Maximum transmission time

Maximum transmission time as part of the response time is used to limit the transmission time. For some non-real time EHM applications (i.e., routine physical examination), although there is no minimum transmission rate requirement, there is an allowed maximum transmission time restriction.

## 9.3 Capabilities of the SSAS layer

### 9.3.1 Service accounting and charging

Service accounting is responsible for gathering data about the usage of EHM services and for charging the service usage to the user. Different policies may be considered for service accounting and charging, e.g., the number of times the service is used, the amount of time the service is used or the volume of service data used. According to service requirements 8.6.2(2), 8.2.1(4), 8.2.2(4), the service accounting and charging capability supported in the SSAS layer has the following requirements:

1) It is required to provide service accounting and charging to EHM service users.
2) It is recommended to provide service accounting and charging according to the quality of service of EHM services.
3) It is recommended to provide service accounting and charging also in support to roaming scenarios among networks owned by different network providers.
4) It is recommended to provide service accounting and charging according to the frequency of access to EHM services.
5) As a user may use several EHM devices at the same time, it is recommended to support unified service charging per user, not per end point.

### 9.3.2 Message conversion

According to service requirement 8.5(2), the SSAS layer is required to provide message conversion for EHM applications and EHM devices. Structured information sharing among EHM applications is realized via messages which are composed of predefined syntax and semantics. The messages transmitted between EHM applications and EHM devices are often not uniform. EHM applications and EHM devices may use messages with different syntax or semantics, which are possibly not compatible with each other. So the SSAS layer is required to provide message conversion for EHM applications and EHM devices.

### 9.3.3 Data storage

According to service requirement 8.5(3), the SSAS layer is required to provide data storage for EHM applications and EHM devices.

NOTE – The exponential growth in electronically stored EHM data and the simultaneous storage of huge amounts of data are putting pressure on this capability. Large data centres are of increased relevance for support of this capability.

The data storage capability requirements include the following:

1) Standard format

   The data stored in the SSAS layer are recommended to be stored in standard format so that the information can be easily exchanged among different EHM applications.

2) Object orientation

   The data storage in the SSAS layer is recommended to adopt the object-oriented access technique for layer separation and independence, so that the information of each EHM customer and each EHM device can be modelled as objects and mapped into the storage area.

3) Time stamping

   The EHM application data stored in the SSAS layer are required to be marked with collection time, since health conditions can vary over time. Using time stamping, the EHM applications can obtain useful information according to the health history.

### 9.3.4 Time synchronization

According to service requirement 8.2.3(4), the time synchronization capability is required to be supported in the SSAS layer, which includes:

1) Time retrieval

   The SSAS layer is required to retrieve time parameters from authoritative time servers or via other ways according to the application requirements.

2) Time announcement

   The SSAS layer is required to publish the time parameters according to the application requests of EHM applications and devices. It is recommended that the SSAS layer publishes time parameters periodically for the time calibration of EHM devices and applications.

### 9.3.5 Location provisioning

According to service requirements 8.2.1(5), 8.2.2(5), 8.2.3(5), 8.6.2(5), the location provisioning capability is required to be supported in the SSAS layer to provide to EHM applications the position of EHM customers, according to regulations and laws.

The location provision capability supported in the SSAS layer includes:

1) Location information collection

   The SSAS layer is required to collect the location information from the network layer or device layer according to the collection strategy such as event triggered collection or periodic collection.

2) Location information tracking

   The SSAS layer is recommended to track the position of EHM customers via frequent collection of the location information of EHM customers.

3) Location information reporting

   The SSAS layer is required to report the location information required by the application layer in standard format.

## 9.4 Capabilities of the network layer

### 9.4.1 Policy-based communication

According to service requirement 8.4.1(1), the network layer is required to provide policy-based communication for EHM applications and EHM devices. Policy is a set of rules whose variables include, but are not limited to, time, bandwidth, data throughput, network type, traffic priority, and so on. By means of policy-based communication, EHM applications and EHM devices can obtain the desired QoS.

The policy-based communication capability provided by the network layer is required to set the network policy to support the QoS of EHM services according to their QoS requirements.

### 9.4.2 Network-based locating

According to service requirements 8.2.1(5), 8.2.2(5), 8.2.3(5), the network layer is recommended to provide the location related information from the network layer (e.g., IP address, access point location, and so on) for locating the position of EHM devices.

Event triggered location information notification is recommended to be supported. For example, when the EHM customer has moved out of the preconfigured network area, a network location information notification may be triggered by the event.

### 9.4.3 Network resource provision

According to service requirements 8.4.2(1), 8.4.2(2), 8.2.1(1), 8.2.2(1), 8.2.3(1), the network layer is required to provide the network resource provision capability for EHM applications and EHM devices. Example of network resources include, but are not limited to, a network address for an EHM device, network bandwidth for an EHM application, and so on.

Depending on the specific deployment of EHM applications and EHM devices, EHM applications and EHM devices may automatically use these provided network resources and configure themselves to connect to the network directly. In this way, EHM customers can use the EHM services directly, without the need to configure the EHM devices.

## 9.5 Capabilities of the device layer

### 9.5.1 Device identification

According to service requirement 8.4.1(1), the device layer is required to support device profiles to identify the intended use of EHM devices, such as the supporting of EHMH and/or EHMR and/or EHMT services.

NOTE – The EHM devices are different from ordinary customer electronic devices. In EHM services, the EHM devices collect physical signals directly and/or indirectly from the human body. The EHM devices have high demands for security, safety and reliability.

### 9.5.2 Gateway

According to service requirement 8.3(1), the device layer is required to provide gateway capabilities for EHM devices and EHM applications. A gateway can serve multiple EHM end points and it provides gateway capabilities by acting on behalf of the EHM end points (e.g., the gateway can provide data processing when the connected EHM end points cannot process the raw data by themselves).

### 9.5.3 Data sensing and processing

According to service requirement 8.6.1(5), the device layer is required to support the data sensing and processing capability for obtaining EHM data.

The data sensing and processing capability required to be supported in the device layer includes:

1) Data sensing

   Data sensing is used to obtain the raw EHM data and is required to respect corresponding regulations and laws. It is recommended to support the sensing of multiple EHM parameters in a single EHM device.

2) Data processing

   Data processing is used to process raw EHM data, such as filtering, aggregating, computing, etc., in order to obtain the desired EHM data.

NOTE – EHM devices can utilize this capability to derive the desired EHM data according to different policies, including at fixed time intervals, upon application request and so on.

### 9.5.4 Data collection time provision

According to service requirements 8.2.3(4), 8.3(7), the data collection time provision capability is recommended to be supported in the device layer, so that the collected EHM data can be marked with the collection time.

The collection time of EHM data is recommended to be known with precision by the EHM application server. It is required to mark the EHM data with the collection time in EHM devices or gateways instead of the EHM application server, since the network transmission time and dispose time affect the precision of the collection time.

The data collection time provision capability recommended to be supported in the device layer includes:

1) Time calibration

   The time calibration capability is used to obtain the time parameters from the SSAS layer and calibrate the built-in time clock of EHM devices.

2) Time provision

   The time provision capability is used to provide the calibrated collection time along with the collected EHM data for time stamping.

### 9.5.5 Device based locating

According to service requirements 8.2.1(5), 8.2.2(5), 8.2.3(5), 8.6.2(5), the locating capability is recommended to be supported in the device layer to get the position of EHM devices.

The EHM devices or gateways can utilize different techniques (e.g., GPS, gyroscope and motion state sensor) to implement the locating capability.

Different levels of location accuracy are allowed according to the application requirements. It is recommended to indicate the location accuracy when the location information is sent from the device layer to other layers.

### 9.5.6 Device redundancy

According to service requirements 8.2.3(8), the device redundancy capability is recommended to be supported in the device layer to guarantee increased reliability and availability for EHMT services.

## 9.6 Management capabilities

### 9.6.1 General

According to service requirements 8.3(5), 8.4.2(4), 8.5(4), 8.6.1(2), , 8.2.1(6), 8.2.2(6), 8.2.3(6), 8.2.3(1), 8.6.2(1), 8.6.1(4), the EHM system, composed of entities in the application layer, SSAS layer, network layer and device layer, is required to support the following management capabilities:

– fault management capability;

– configuration management capability;
– initialization and registration management capability.

### 9.6.2 Fault management

According to service requirements 8.3(5), 8.4.2(4), 8.5(4), 8.6.1(2), 8.2.1(6), 8.2.2(6), 8.2.3(6), the EHM system is required to recognize, isolate, correct and log faults that occur in the EHM system.

– It is required to enable service logging reports to the various parties involved in an EHM service.
– It is required to enable the collection and storage of fault management data.

### 9.6.3 Configuration management

According to service requirements 8.2.3(1), 8.6.2(1), the EHM system is required to provide the configuration management capability for EHM applications and EHM devices. Examples of provisioning actions include hardware and programming (configurations) changes, including the addition of new devices and programs, modification of the existing EHM system and removal of obsolete EHM systems and programs.

The different layers of the EHM system are required to support different configuration capability requirements.

1) The application layer and the SSAS layer are required to support the following capabilities:

• connection configuration management;
• software and firmware configuration management;
• EHM application configuration management, such as lifecycle management;
• service configuration management, e.g., service configuration, service profile setting and so on.

2) The device layer is required to support the following capabilities:

• fault management and connection management;
• software and firmware configuration management;
• proxy management, which includes but is not limited to the following capabilities:
  ◦ acting as a management client to perform the management functionalities for the EHM gateway itself;
  ◦ acting as a management proxy for EHM devices:
    – accepting and processing management requests, targeted at one or multiple EHM devices, from the application and SSAS layers;
    – accepting and processing management requests from one or multiple EHM devices and/or further interacting with the application and SSAS layers on behalf of the EHM devices (e.g., in the case of fault detection and reporting);
    – triggering the application and SSAS layers to start performing device management tasks (e.g., firmware/software update, fault diagnostics) with one or multiple devices;
    – scheduling of remote management tasks for sleeping devices.

### 9.6.4 Initialization and registration management

According to service requirements 8.2.3(1), 8.6.1(4), the initialization and registration management capability is required to be supported in the EHM system. When EHM devices access the EHM system for the first time, the initialization and registration management capability can help the

EHM devices to complete the device initialization set-up, and write the device and user information into the related database.

The initialization and registration management capability needs the following support at the different layers:

1) Application layer and SSAS layer

   The application layer and the SSAS layer are required to be able to write the device or user information into the related application layer or SSAS layer database and to provide to the EHM devices the required configuration information for the initialization set-up of the EHM devices.

2) Network layer

   The network layer is required to provide the network resources for EHM devices to access the network, e.g., network address allocation.

3) Device layer

   The device layer is required to support the capability of initialization set-up. The EHM device can complete the initialization set-up by itself or with the help of the EHM gateway according to the provided configuration information from the application layer or the SSAS layer.

### 9.7 Security capabilities

According to service requirements 8.2.1(7), 8.2.2(7), 8.2.3(7), 8.3(3), 8.6.1(3), the EHM system is required to support the following security capabilities:

1) Authentication and authorization

   The EHM system is required to support authentication and authorization mechanisms.

2) Secure communications

   According to service requirements 8.2.1(2), 8.2.2(2), the information carried by the EHM services may be delivered across different administrative domains (e.g., countries, operators). The EHM system supports secure communications between different domains. The information exchanged between different domains must be protected from random errors, as well as snooping or hacking attacks.

3) Confidentiality

   Whenever information is exchanged, stored or processed, the confidentiality of the data must be enforced and safeguarded by the EHM system. All exchanges of data between e-health partners, for example EHM device provider, EHM application provider, network provider and platform provider, must be performed in a way that prohibits any unwanted disclosure of data, e.g., to third parties.

4) Integrity

   The integrity of the transmitted information must be guaranteed: transmitted data from the sender should be received without any alteration. It must be identified that the transmitted data have not been damaged, reduced or altered. Any loss of integrity of the transmitted data must be recognizable by the recipient.

5) Access control

   It should be ensured that only authorized persons and EHM system entities (e.g., applications, devices) are able to access protected data.

6) Audit trail

   Any access or attempt to access medical data through EHM services must be fully transparent, traceable and reproducible.

7) Data storage security

It is recommended to support data storage security strategies including, but not limited to, data backup, anti-hacker data protection, uninterruptible power of data storage, data integrity validation and data recovery. In addition, data access control is required to be supported for privacy.

# Appendix I

## e-health monitoring service scenarios

(This appendix does not form an integral part of this Recommendation.)

### I.1 Individual/family (indoor and outdoor)

The EHM services described in this appendix are examples of EHMH services.

In the individual/family scenarios, by means of communication and diagnostic tools, EHM customers can sample their own physiological parameters at anytime and anywhere, and send them to health-care institutions in a timely and accurate way. The staff of health-care institutions can provide guidance to EHM customers based on both the past and current data received regarding their conditions.

The individual/family scenarios include both indoor and outdoor ones. In indoor scenarios, the sampled physiological parameters can be transmitted in both wired and wireless ways, while in the outdoor scenarios sampled physiological parameters are generally transmitted in a wireless way.

In individual/family scenarios, e-health monitoring devices should have the basic medical monitoring capability, as well as the features of miniaturization, portability, easy operation and the capability of short-distance communication.

An example of an indoor EHM service scenario is shown below in Figure I.1:

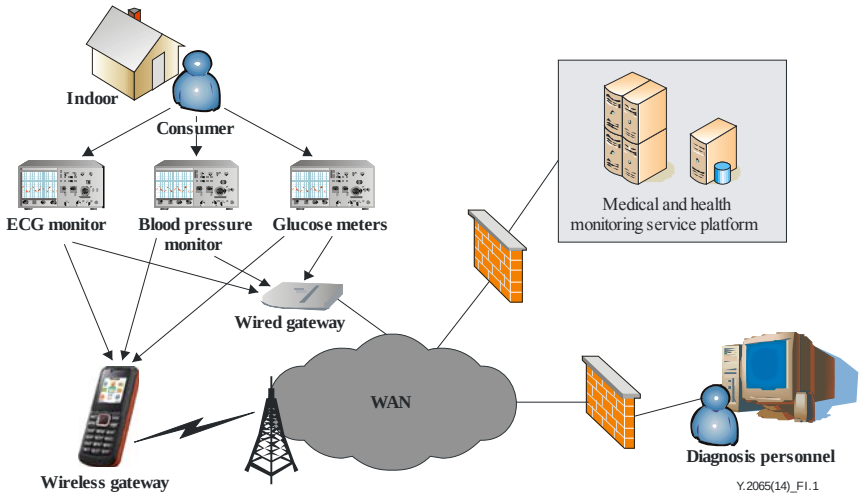


**Figure I.1 – Indoor scenario**

An example of an outdoor service scenario is shown below in Figure I.2:

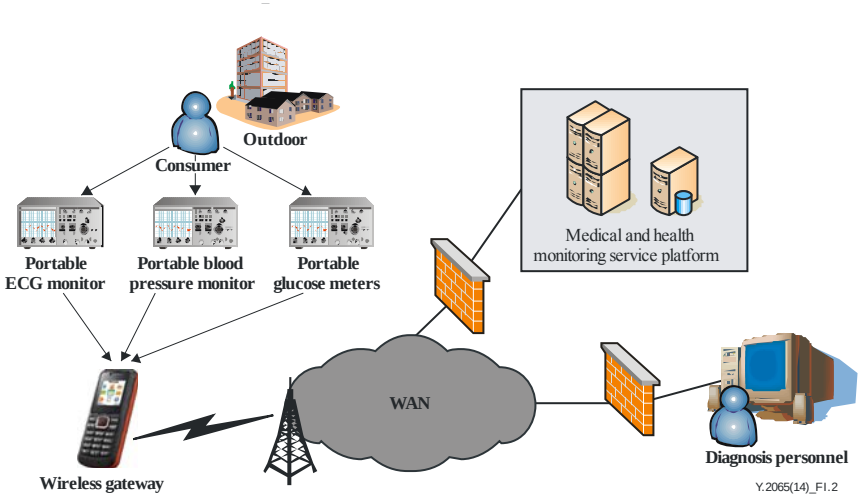


**Figure I.2 – Outdoor scenario**

Customers can detect their sampled data through portable ECG monitors, portable blood pressure monitors, portable glucose meters and other portable equipment, then they can preprocess the monitored data and forward the data to the medical and health monitoring service platform via a wired gateway or a wireless gateway (as wired network connectivity is not convenient outdoors, one must use a wireless gateway, e.g., a smart phone).

The diagnosis personnel can access in real time the monitored data through the service platform, determine the customer's conditions according to their basic information and past medical history, and give health guidance to them.

## I.2 Physical examination

A user is assumed to have physical examinations or disease check-ups regularly or to have had them in the past. The physical examination includes routine checks such as height, weight, blood pressure, eyesight, chest X-ray, etc., and where required, specific disease check-ups. The user chooses to send the monitored data via a wired or wireless gateway to the ubiquitous e-health monitoring server in health-care institutions or have the data written into the user's e-health records (including a user's basic information and past health records, which are stored in the system). Then the medical staff analyse and determine the user's health conditions according to both current and past data, and gives health guidance to the user.

In the physical examination scenario, the e-health monitoring devices should have the basic medical monitoring capability, as well as the communication capability to transmit the monitored data and receive data from the e-health application servers.

An example of a physical examination scenario is shown below in Figure I.3.

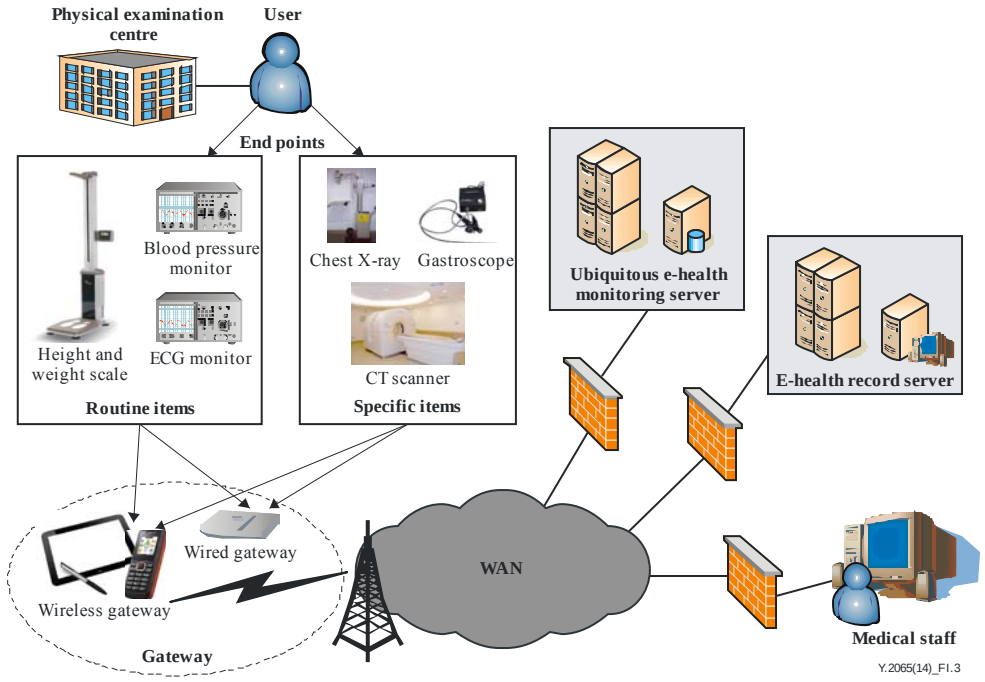


**Figure I.3 – Physical examination scenario**

The features of a physical examination service include, but are not limited to, the following concerning:

– Existing resources:
  - various kinds of advanced medical devices embedded with sensors, such as height and weight scales, ECG monitors, blood pressure monitors, etc.
  - advanced communication and information processing technologies, including the technologies of IoT, wireless sensor networks, context awareness, etc.
  - e-health monitoring service platform and e-health record applications.

– Required capabilities:
  - Device: The devices used in a physical examination service for physiological parameter collection should have high accuracy and stability to ensure reliable measurements.
  - Gateway: The gateway is necessary: a) in special areas of the physical examination centre (gateway collecting different data and transmitting them); b) for possible service extension to home environments (this scenario is not described here). The gateway should convert the information received from each device into the data (and associated formats) transmitted over the WAN. A high signalling processing capability is required with a larger number of subordinate end points.
  - Network: A private network may be applied to ensure secure and reliable connectivity between the gateway and the e-health monitoring and e-health record servers. For the possible service extension to home environments, a public network is used. However, special attention should be paid to data and network security in this case.

– Security requirements:
  - Authentication and authorization: the e-health monitoring server and the e-health record server provide authentication and authorization for gateways and devices. The authentication and authorization of each end point can be done by the gateway it is subordinated to, or by the e-health monitoring server and the e-health record server.

- Data storage: devices should be able to store the acquired data for a certain period of time (for example, 24 hours, 7 days, etc.). The gateway should at least be able to store the routing and topology related information of the subordinate end points, and the physiological parameters. When a gateway is the authentication point of end points, the gateway should be also able to store the authentication and authorization information of the subordinate end points.
- Electrical safety: The devices should be able to resist electromagnetic interference and meet the limitation requirements of electromagnetic interference. Radiation levels should meet certain standards.

## I.3 Disaster rescue

In disaster rescue scenarios, by means of advanced communication and diagnostic tools, the sampled physiological parameters of injured people can be obtained at anytime, anywhere and in a timely and accurate way by the medical staff located both inside and outside of the disaster area. Then the medical staff can determine the conditions of those injured according to sampled physiological parameters, and they can give first-aid guidance to them. The location information of those injured is acquired and recorded by means of the wireless sensor network, so that those who are injured can be easily found by the medical staff.

The disaster rescue scenarios include those inside the disaster area and those outside of the disaster area. For those inside the disaster area, the sampled physiological parameters are transmitted in a wireless way, while for those outside of the disaster area, the sampled physiological parameters can be transmitted in wired or wireless ways.

In disaster rescue scenarios, the e-health monitoring devices should have the basic medical monitoring capability, as well as the capabilities of short-distance and long-distance communication in order to acquire and transmit data to the wireless gateway and remote monitoring centre.

An example of a disaster rescue scenario is shown below in Figure I.4.

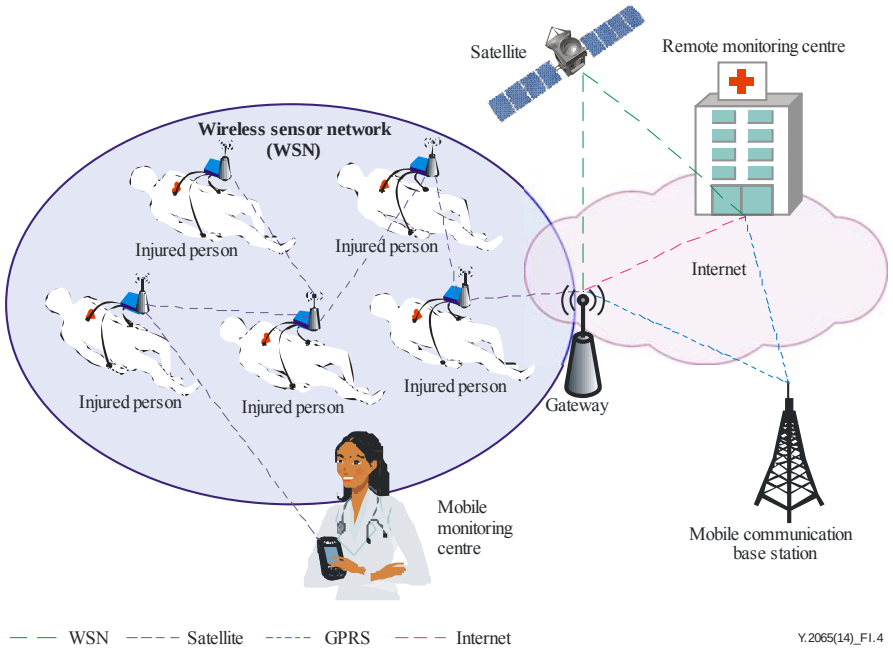


**Figure I.4 – Disaster rescue scenario**

The network of e-health monitoring services in disaster rescue scenarios can be divided into two parts: the wireless sensor network and the long-distance network.

Where there is a complicated geographical environment in the disaster area, wireless networks can be established more easily and flexibly than wired networks. So networks based on wireless technologies such as wireless sensor networks are usually established in the disaster area.

The long-distance network is built outside the disaster area: through it the sampled physiological parameters can be transmitted in both wired and wireless ways, e.g., via Internet, GPRS or satellite.

In the wireless sensor network, each injured person wears a wireless end point. The end point includes two parts: portable multi-parameter sensors and a wireless transceiver. The injured person's physiological parameters, such as ECG, blood pressure, heart rate and temperature, are measured in a timely and accurate way by portable multi-parameter sensors without medical staff on site. Then, the physiological parameters from all the injured people are transmitted to the mobile monitoring centre and wireless gateway by wireless transceivers and a wireless network. At the same time, the location information of those injured will be acquired and recorded by the wireless sensor network, so that they can be easily found by the medical staff.

The mobile monitoring centre can be a panel computer or personal digital assistant (PDA) carried by the medical staff in the disaster area. The physiological parameters collected from the injured people are shown on the computer/PDA so that the medical staff can supervise them in a timely way when moving within the disaster area.

The wireless gateway is the gateway of the wireless sensor network. It has three main functions: configuring the wireless sensor network, gathering physiological parameters of all the injured people from the wireless sensor network and communicating with the remote monitoring centre via the long-distance network (e.g., transmitting the physiological parameters to the remote monitoring centre and transmitting instructions from the remote monitoring centre to the wireless sensor network).

The remote monitoring centre can be a hospital with rich medical resources. The doctors can monitor in real time the critically injured people's conditions according to the received physiological parameters and they can comprehensively determine their illness. Then the doctors send first-aid guidance to the medical staff in the disaster area via the long-distance network and the wireless sensor network, so that those who are critically injured can get a timely and accurate diagnosis, as well as appropriate emergency treatment.

The features of a disaster rescue service include, but are not limited to, the following concerning:

– Providers of a disaster rescue service

In a disaster area, medical staff include doctors and nurses; the nurses take care of those who are slightly injured, while both nurses and doctors take care of the seriously injured people. Both nurses and doctors are required to have basic medical treatment training before undertaking the disaster rescue tasks.

Outside of the disaster area, some medical staff are located in the remote monitoring centre. They monitor the seriously injured people and are required to have a high level of professional medical treatment experience before undertaking these tasks.

– Users of disaster rescue service

The identification of the injured person is realized via a wristlet which has an RFID (radio frequency identification) module embedded in it and which is worn by each injured person. The wristlet is the one and only way of identifying an injured person during treatment. The physiological parameters of the injured people are bound with their own ID number, and all this information is sent to the medical staff, including those inside and those outside of the disaster area.

The activation of useful related information concerning the injured person: the medical staff record the injured person's information, such as name, age, gender, family relationship, etc. in the equipment constituting the mobile monitoring centre. With this information, the medical staff can activate the useful related information (such as drug history, family history of disease) concerning the injured person. The physiological parameters collected from the injured person are also shown on the mobile monitoring centre computer so that the medical staff can supervise the injured person in a timely way when moving within the disaster area.

– Unique features of service

The wireless end points: the wireless end points are portable medical multi-parameter devices. The sensors of medical parameters, such as ECG, blood pressure, heart rate and temperature, are integrated into the wireless end points to reduce the number of required devices and simplify the complexity of the wireless sensor network. At the same time, the wireless end points replace the medical staff's manual way of collecting the injured person's physiological parameters.

The network inside the disaster area: considering the complicated geographical environment of the disaster area, a wireless sensor network is built inside the disaster area. In the wireless sensor network, each injured person wears a wireless end point. The injured people's physiological parameters are collected by the wireless end point and transmitted via the wireless sensor network to the mobile monitoring centre and then to the remote monitoring centre.

The location of the injured people: in the disaster area, the location of those injured varies. In some disaster cases, such as earthquakes or floods, the global system for mobile communications/ universal mobile telecommunications system (GSM/UMTS) network is not available; in these cases, the injured person can be located by the wireless sensor network, so that he/she can be found by the medical staff. On the other hand, if the GSM/UMTS network and the injured person's mobile phone are available, the injured person can use the mobile phone to report his/her location.

Data storage: end points should be able to store the physiological parameters of the injured people. The gateway should be able to store the locations, routings and topologies of the end points in the wireless sensor network, and store the data when needed. The remote monitoring centre should store the acquired data if needed and also for future treatment.

– Common features of service

The gateway: the gateway has the three capabilities of configuring the wireless sensor network, gathering the physiological parameters from the wireless end points and communicating with the remote monitoring centre via the long-distance network. A high signalling processing capability of the gateway is required to ensure both wireless sensor network and long-distance network reliability.

The network outside the disaster area: the long-distance network built outside the disaster area and through which data can be transmitted in both wired and wireless ways, such as Internet, GPRS and satellite, ensures data are received by the remote monitoring centre.

– Security requirements

Electrical safety: the wireless end points should be able to resist electromagnetic interference and meet the limitation requirements of electromagnetic interference. Radiation levels should meet the related standards.

## I.4 Pre-hospital emergency medical service

### I.4.1 Overview of pre-hospital emergency medical service

The pre-hospital emergency medical service (PEMS) which is usually offered outside of the hospitals, can be defined as an emergency medical treatment for patients injured by accidents or life-threatening diseases, and who are treated during transportation from an on-site location

to the hospital; it can also reduce the time and costs of patient transportation significantly. The PEMS system is an important component of the emergency medical service system (EMSS), which is a precondition for successful rescue, and plays a significant role in modern life.

The summary of PEMS operational steps (as shown in Figure I.5) is as follows:

Step 1: An emergency call is made from the patient's side to the receptionist at the PEMS platform.

Step 2: Information on patient location computed by GPS navigation system is sent to the hospital tele-management, which is responsible for the initial evaluation of the patient, triage decisions and pre-transfer arrangements.

Step 3: Urgency is initially evaluated according to the information provided by the patient's call. Based on the evaluation result, a triage decision is being made and then ambulance assignment is allocated by the hospital tele-management.

Step 4: On-site rescue where supervision and consultation for primary care treatments is not available i.e. there is no physician on site.

Step 5: History, physical examination findings and available test data exchange takes place between the ambulance and hospital. Based on this information, which hospital the patient will be taken to and what medical resources (e.g., physician, surgical instruments) should be prepared by the hospital for the patient are arranged by the pre-transfer management.

Step 6: The patient is taken to the hospital by ambulance.

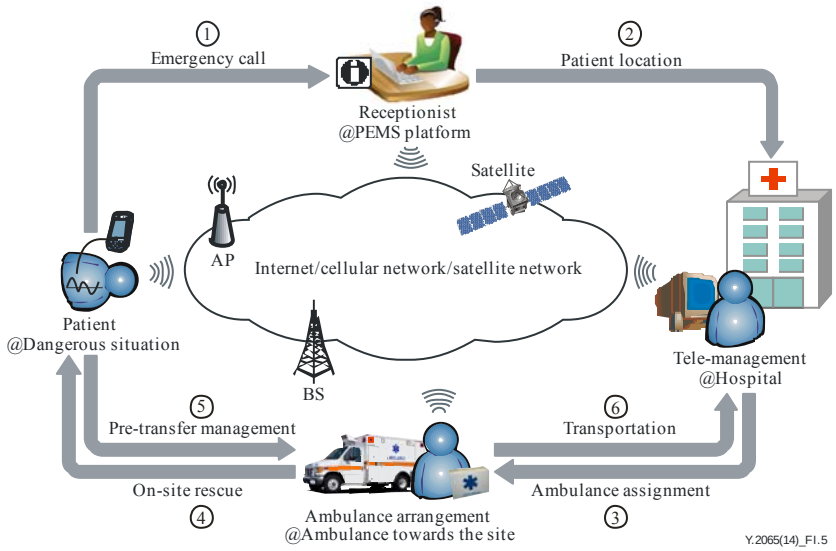


**Figure I.5 – Pre-hospital emergency medical service operational flow**

From a functional perspective, the PEMS system is made up of three main parts: a navigation system, physiological parameter monitoring system, and a remote medical treatment-assistant system (as shown below in Figure I.6).

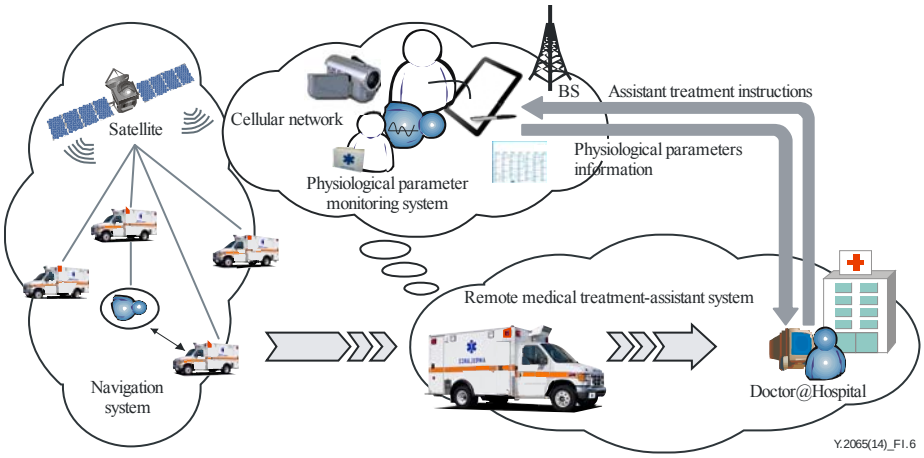


**Figure I.6 – Main parts of the PEMS system**

1) Ambulances install a navigation system with a positioning system, e.g., GPS, and wireless communication network capabilities, e.g., GPRS. By means of the GPS satellite positioning system, the emergency medical service centre can locate the patient and any available ambulances; the closest ambulance can be quickly sent. At the same time, the navigation system can provide the ambulance team with the most effective route to the hospital.

2) The physiological parameter monitoring system includes medical terminals and a mobile network and it provides the emergency medical service doctor with the real-time physiological parameters of remote patients, such as ECG, heart rate, oxygen saturation, blood pressure, respiratory rate, etc. Despite the unstable environment of a moving ambulance, the physiological parameters must be transmitted by a mobile network in a guaranteed manner so that the doctor can collect high quality physiological parameters. Also, the medical terminals on the ambulance must resist the fast fading when physiological parameters are transmitted to the hospitals via mobile networks.

3) A remote medical treatment-assistant system makes it possible for patients in an ambulance who require specialist medical care to have face-to-face consultations with specialists that are situated in the hospital or at another distant medical institution. In other words, it enables the emergency medical doctor to send medical data (including sounds, images and video), captured using medical peripherals, to a doctor in a hospital for generating patient diagnostics.

### I.4.2 Special requirements for a pre-hospital emergency medical service

Pre-hospital emergency medical treatment is different from hospital treatment. As well as the fight against time, the emergency vehicle is moving at high speed. Thus, the following special requirements for PEMS should be seriously considered:

1) Accuracy

The real-time medical data of patients, such as ECG, heart rate, oxygen saturation, blood pressure, respiratory rate, etc., are the basis for emergency medical treatment which requires accuracy in data collection. The physiological parameter monitoring system should have a real-time data processing capability, including real-time dynamic signal filtering, fast detection and recognition for medical characteristic waveforms, self-learning and adaptive algorithms.

2) Mobility

Since the ambulance used in emergency medical treatment is moving at high speed and the pre-hospital emergency medical service centre communicates with it in a special fast fading channel, the mobile network needs to ensure high reliability of the transmissions. For reliable transmissions, mobile network switching and routing technologies should be adopted.

3) High QoS

It is essential in a critical medical environment that the PEMS performs with high precision; otherwise, the outcome could be fatal for patients. For this to be possible, it is necessary that the physiological parameters reach the end location with a high degree of reliability and predictability. PEMS systems are said to have stringent real-time QoS constraints, which if not respected can lead to disaster; for example, the unbounded delay and jitter in the control system of a remote medical treatment-assistant can lead to mission failure. Lastly, sufficient availability of network resources is imperative for achieving correct analysis results, because the generated traffic may be crucial for a patient's health and life.

## I.5 Smart ward service

### I.5.1 Overview of the smart ward service

A smart ward service inside a hospital provides efficient health care to patients, minimizes the nursing workload and facilitates a doctor's diagnosis. Patients, doctors, nurses and medical assets are connected together as shown below in Figure I.7. This makes a ward smart. The patient can move freely around the hospital and wears only a few wearable devices. The wearable devices can detect the patient's physiological parameters and location. The physiological parameters are uploaded directly to the electronic medical record (EMR) system. Doctors can access the patient information anywhere. The connection between nurses and patients creates a safer and more efficient care environment.

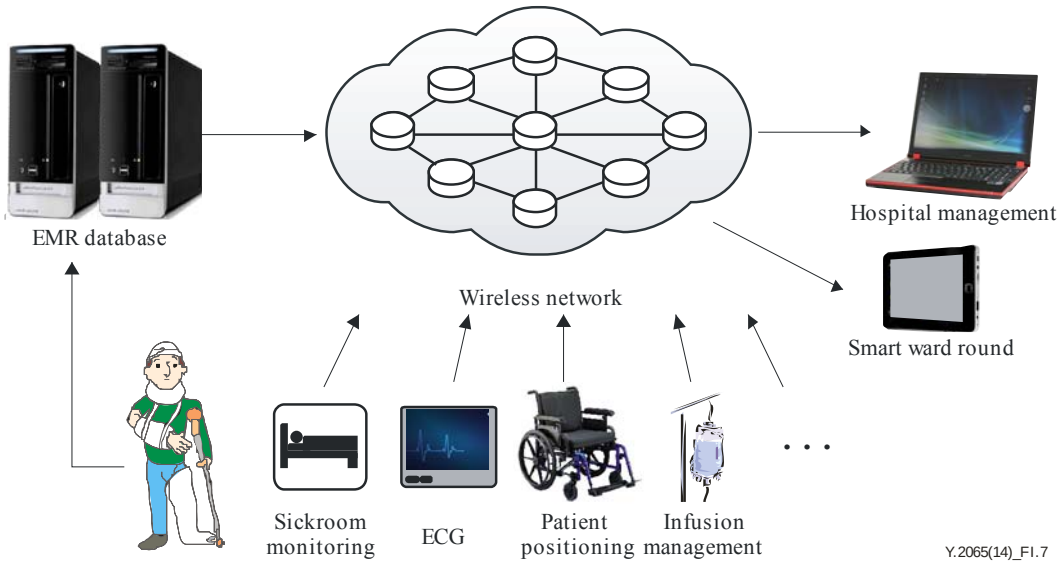


**Figure I.7 – Smart ward network**

The effects of nursing rounds can be improved through the smart ward service. Diagnostic results and electronic medical records can be displayed to patients anywhere. Tracking of patients is critical for the clinical risk management process, particularly for a hospital ward where patients need intensive care. When a patient's condition suddenly deteriorates, the smart ward service can identify and locate the patient. The patient care flow is often delayed when a medical asset cannot be found, and the smart ward service provides medical asset management to reduce the delay associated with asset search. By reducing the search time, nurses have more time to treat the patients.

The smart ward service can be broken into the three main components of physiological parameters monitoring, indoor patient tracking and medical asset management:

1) the movement physiological parameters monitoring involves the acquisition of physiological parameters in movement and then the analysis of the data;

2) the indoor patient tracking is used to locate the patients inside a building;

3) the medical asset management system can locate the desired medical asset.

### I.5.2 The requirements of smart ward services

1) Time critical service

In health-care environments, delayed or lost information may be vital. Therefore, reliable transmission must be guaranteed. Immediate action has to be generally undertaken as a response to the received data. For example, if a patient falls down, the patient's location should be reported to hospital staff immediately.

2) Simplicity

Service operation should be convenient for users, who may not be experts in the wireless network field.

3) Low power radiation

The wireless network is used in proximity to a human body. As a result, the radiation of the wireless network should not pose a health risk.

4) Low power consumption

The power budgets of wearable devices are constrained, requiring low power communication solutions. The wireless network should support low power mechanisms.

## I.6 Chronic disease care

In the chronic disease care scenarios of e-health applications, there is a body area network concept of e-health; this is the collection of physiological parameters like blood pressure, blood oxygen, pulse rate, ECG, body temperature, blood sugar and others by computers, mobile phones, PDA or other gateway devices via sensors worn around the human body. The sensors can get the physiological parameters and transmit them by wireless means to the data centre. The data centre gets the data, analyses them and then sends the patients their results. Based on this, the patient can achieve real-time detection, and the doctor can provide each patient with health guidance.

The core of the chronic disease care service is the delivery and sharing of patient information, including information between different departments in the hospital, between hospitals, even between hospitals and the community, health insurance and government departments. This requires the devices to combine the sensor capability, computation capability and network connectivity capability. The sensor capability of the device collects the patient's physiological parameters in real-time. The computation capability of the device preprocesses the collected physiological parameters. Through the network connectivity capability of the device, the preprocessed physiological parameters are sent to the data centre. The medical staff obtain the patient's processed physiological parameters and other related information from the data centre and then, based on this information they make appropriate decisions which will be eventually sent back to the patients. Figure I.8 below illustrates the general architecture of a chronic disease care service.

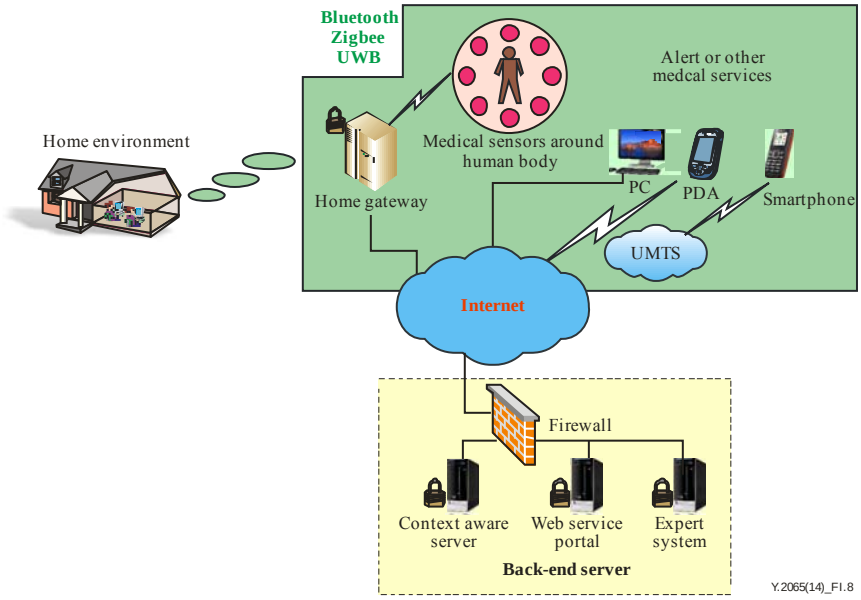


**Figure I.8 – Chronic disease care service scenario**

In Figure I.8, for the home environment, a variety of wireless access technologies and networks are shown. Physiological parameter sensors (such as blood pressure sensors, heart rate sensors, etc.), or other sensors (such as motion detection sensors) are worn if needed for the collection of a patient's monitoring parameters. Data collected through short-range wireless technologies (Bluetooth, Zigbee, UWB, etc.) are transmitted to a gateway (the gateway may be embedded in the family's ADSL box, personal computers, mobile phones, PDAs, etc.). Through the gateway, the patient's daily data are sent to the hospital in order to achieve real-time monitoring and expert guidance. A variety of health-care services in the home environment need to be supported by a back-end server. The care of chronic diseases (such as diabetes, heart disease, etc.) can be typically done by using a monitoring application.

The features of a chronic disease care service include, but are not limited to, the following concerning:

– Providers of a chronic disease care service:
  - Doctors handle the abnormal results. If a diagnosis from this data gives an abnormal result which might imply a risk of disease for the patient, an associated doctor is informed of the result. Effective action is then taken by the doctor.
  - A data centre is the core of the whole system. It deals with all the data including user information, doctor information, device information and physiological parameters. Large storage and high speed processing requirements must be satisfied. The algorithms to process the data are another key factor which determines the effectiveness of the whole system.
  - Devices can be rented or sold to the users. They can measure the user's physiological parameters automatically and can send the data to the data centre by wired/wireless communication.

– Users of chronic disease care service
  - In the chronic disease care service, the elderly are the prime users. As life expectancy is increasing more and more in many countries, the number of users who need the chronic disease care service will increase.
  - More and more people will have health issues and will be classed as 'not fully healthy'. Those in this category may become users of the chronic disease care service.

- Users of the system want their health to be monitored automatically without the need to go to hospital every day. In this way, some hidden health risks for the user should be detected in time.

– Device requirements

Patient demand for monitoring devices might vary, for example, some patients only need a few parameters to be monitored, while others only require monitoring for specific time periods. The flexibility of device configuration in order to meet the needs of different users should be considered.

– Network requirements

As well as bandwidth and transmission speed, user mobility requirements should be considered. The heterogeneous coverage of wireless mobile networks can ensure access to a wide range of applications at anytime and anywhere.

– System availability requirements

The chronic disease care service must be available all the time. The user may need to measure his/her physiological parameters at any time of the day.

– System precision requirements

Precision must be achieved. Only precise data can guarantee users with appropriate services. Otherwise, inaccurate data or inaccurate diagnosis results might lead to errors or severe incidents.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks, open system communications and security |
| **Series Y** | **Global information infrastructure, Internet protocol aspects and next-generation networks** |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2014