



BSI Standards Publication

Health informatics — Accelerating safe, effective and secure remote connected care and mobile health through standards-based interoperability solutions addressing gaps revealed by pandemics

National foreword

This Published Document is the UK implementation of CEN ISO/TS 5615:2025. It is identical to ISO/TS 5615:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 28698 4

ICS 35.240.80

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

**Health informatics - Accelerating safe, effective and secure
remote connected care and mobile health through
standards-based interoperability solutions addressing
gaps revealed by pandemics (ISO/TS 5615:2025)**

Informatique de santé - Augmentation de la sûreté, de l'efficacité et de la sécurité des soins à distance et de la santé mobile par l'intermédiaire de solutions d'interopérabilité fondées sur les normes, en remédiant aux insuffisances mises en évidence par la pandémie (ISO/TS 5615:2025)

Medizinische Informatik - Beschleunigung einer sicheren, effektiven und geschützten vernetzten Fernbetreuung und mobilen Gesundheitsfürsorge durch auf Standards basierende Interoperabilitätslösungen, die die durch Pandemien aufgedeckten Lücken schließen (ISO/TS 5615:2025)

This Technical Specification (CEN/TS) was approved by CEN on 22 March 2025 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (CEN ISO/TS 5615) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/TS 5615:2025 has been approved by CEN as CEN ISO/TS 5615 without any modification.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	4
5 RCC-MH care locations and evolution	5
5.1 What is RCC-MH?	5
5.2 Care locations: hospitals, home and community, nursing, outpatient	6
6 RCC-MH relevant care delivery modes and use cases	8
6.1 General	8
6.2 Hospital care	8
6.2.1 Isolation room	8
6.2.2 Remote patient surveillance	9
6.3 Home and community care	9
6.3.1 Telehealth and virtual health	9
6.3.2 Remote delivery of care	9
6.4 Post-acute care	9
6.4.1 LTAC	9
6.4.2 Skilled nursing facility	10
6.5 Outpatient care	10
6.5.1 Remote consultation	10
6.5.2 GP/PCP visit	10
7 RCC-MH challenges and gaps	10
7.1 General	10
7.2 RCC-MH challenges and gaps – Safety and quality	10
7.3 RCC-MH challenges and gaps – Deployment	12
7.4 RCC-MH challenges and gaps – Service support	14
7.5 RCC-MH challenges and gaps – Infrastructure	15
7.6 RCC-MH challenges and gaps – Interoperability	15
7.7 RCC-MH challenges and gaps – Operations	16
7.8 RCC-MH challenges and gaps – Security	17
8 RCC-MH recommendations	19
8.1 Recommendations	19
8.2 RCC-MH recommendations – Safety and quality	19
8.3 RCC-MH recommendations – Deployment	21
8.4 RCC-MH recommendations – Service support	23
8.5 RCC-MH recommendations – Infrastructure	24
8.6 RCC-MH recommendations – Interoperability	24
8.7 RCC-MH recommendations – Operations	25
8.8 RCC-MH recommendations – Security	26
9 Conclusions and path forward	28
9.1 Recommended standards work items	28
9.2 Final thoughts	30
Annex A (informative) Regulatory and legal reactions to the pandemic	31
Annex B (informative) RCC-MH interoperability challenges	44
Annex C (informative) Nomenclature standards landscape for medical devices	47
Annex D (informative) Accelerating safe effective and secure (SES) RCC-MH	53
Annex E (informative) RCC-MH socio-technical challenges	56

Annex F (informative) RCC-MH communications standards landscape	57
Annex G (informative) RCC-MH cybersecurity standards landscape	72
Annex H (informative) RCC-MH telehealth standards landscape	79
Annex I (informative) Device specializations	81
Annex J (informative) Summary of applicable standards	82
Annex K (informative) Care delivery locations	85
Annex L (informative) Conformance landscape	87
Bibliography	89

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with HL7 and with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The COVID-19 pandemic has created an enormous need to allow patients and clinicians to communicate with each other and report in a more flexible and virtual way outside of the traditional care delivery infrastructure. Numerous studies and reports from healthcare organizations have shown the dramatic increase in the use of telehealth visits and their associated benefits:

- reduction of pandemic-related risks typically associated with face-to-face visits.
- alleviation of care capacity pressures due to pandemic-induced patient influx.
- stemming the tide of continually increasing healthcare costs driven by aging populations and associated growth of chronic disease.
- catering to patient preferences and enabling patients to stay in their home longer, return sooner, or manage their condition at home altogether.

Many healthcare organizations have gone beyond telehealth in an attempt to deploy remote care approaches to interact with patients in the hospital as well as track the status of patients at home or alternate care institutions. This technology is also used for clinical trial data collection, real word evidence and patient surveillance, especially under the limitations and pressure of a pandemic. This is termed as “Remote Connected Care and Mobile Health (RCC-MH)”.

This document explores the current challenges of deploying RCC-MH widely in the current environment. In addition to technical gaps, this document also identifies techno-social gaps that will need to be overcome. The question then becomes: how to educate and motivate manufacturers and ‘consumers’ (hospitals, alternate care settings, patients and their advocacy groups, etc.) so they understand the benefits of interoperability and, since RCC-MH will not be realizable without interoperability, begin to demand interoperable devices and apps that take advantage of interoperable devices?

This document answers questions such as:

- What informatics standards can be considered when developing remote care / Mobile Health solutions?
- What safety, effectiveness & security (SES) standards can be leveraged to balance solution options with risk-based public good assessments?
- How can the application of these standards be scaled in crisis situations where resources and time are highly constrained?
- How can we develop more efficient interoperability solutions to rapidly address the needs of telehealth in pandemics cases?

This document is intended to inform a diverse set of stakeholders, including:

- industry – medical device vendors, point-of-care lab systems, pharma, SW and IoT vendors, apps vendors;
- government – regulatory, public health, state and local government;
- providers – primary care physicians (PCPs), general practitioners (GPs), specialists, healthcare delivery organizations (HDOs);
- SDOs (standards development organizations);
- patients (including advocacy groups);
- payors – government, private, and public insurers;
- infrastructure vendors – networking, security, cloud, mobile devices and apps.

Health informatics — Accelerating safe, effective and secure remote connected care and mobile health through standards-based interoperability solutions addressing gaps revealed by pandemics

1 Scope

This document reviews the structural changes that have been precipitated by the COVID-19 pandemic in Remote Connected Care and Mobile Health (RCC-MH). The impact of the COVID-19 pandemic on care settings such as home and community care, acute care and outpatient care are reviewed discussing how well these healthcare environments were prepared to address the encountered connectivity challenges from a standards point of view. The current standards landscape is reviewed and gaps are identified leading to recommendations for future standards work.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

effective

successful in producing a desired or intended result

3.2

effectiveness

ability to produce the intended result

Note 1 to entry: Clinical effectiveness is based on valid scientific evidence that in a significant portion of the target population the use of the device for its intended uses will provide clinically significant results.

[SOURCE: ISO 81001-1:2021, 3.2.5, modified — Note 1 to entry was added.]

3.3

harm

physical injury or damage, or both, to the health of people or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1, modified — “injury or damage” was changed to “physical injury or damage, or both”.]

3.4

hazard

potential source of *harm* (3.3)

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

3.5

gateway

network entity (software or hardware) that interfaces between networks that use different protocols, or are of different, potentially incompatible, technology

Note 1 to entry: A gateway operates with a focus on network translation (network gateway) or service translation (service gateway).

[SOURCE: Reference [\[27\]](#)]

3.6

interoperability

ability of two or more systems or components to exchange information and to use the information that has been exchanged

Note 1 to entry: “Open Interoperability IS achieved using open (publicly available) protocols, syntax, semantics, etc.”

Note 2 to entry: “Proprietary Interoperability IS achieved using proprietary protocols, syntax, etc. AND is not Open(accessible) to All and has issues sharing data”

Note 3 to entry: “Seamless Interoperability IS achieved ‘out of the box’ between components that have never been tested together.”

[SOURCE: Reference [\[28\]](#)]

3.7

in vitro diagnostic medical device

IVMD

medical device ([3.9](#)), whether used alone or in combination, intended by the *manufacturer* ([3.8](#)) for the in-vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes.

Note 1 to entry: IVD medical devices include reagents, calibrators, control materials, specimen receptacles, software, and related instruments or apparatus or other articles and are used, for example, for the following test purposes: diagnosis, aid to diagnosis, screening, monitoring, predisposition, prognosis, prediction, determination of physiological status.

Note 2 to entry: In some jurisdictions, certain IVD medical devices may be covered by other regulations.

[SOURCE: Reference [\[37\]](#)]

3.8

manufacturer

natural or legal person with responsibility for the design and/or manufacture of a *medical device* ([3.9](#)) with the intention of making the medical device available for use, under their name, whether or not such a medical device is designed and/or manufactured by that person themselves or on their behalf by another person(s)

[SOURCE: ISO 14971:2019, 3.9, modified — Notes to entry were removed.]

3.9

medical device

any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the *manufacturer* ([3.8](#)) to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological process,
- supporting or sustaining life,
- control of conception,

- disinfection of medical devices,
- providing information by means of in vitro examination of specimens derived from the human body, and which does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means

Note 1 to entry: Products which may be considered to be medical devices in some jurisdictions but not in others include:

- disinfection substances,
- aids for persons with disabilities,
- devices incorporating animal and/or human tissues,
- devices for in-vitro fertilization or assisted reproduction technologies.

[SOURCE: ISO/IEC Guide 63:2019, 3.7]

3.10

patient monitoring

process of observing and measuring physiological parameters via *medical devices* (3.9) to guide patient care

EXAMPLE Monitoring via general hospital and personal use monitoring devices, anaesthesiology monitoring devices, cardiovascular monitoring devices, etc.

3.11

remote patient monitoring

patient monitoring (3.10) from a distance over time

EXAMPLE Monitoring a patient's health while they are at their home, while they are in a hospital from a central location, while they are in an ambulatory, etc.

3.12

safety

freedom from unacceptable risk

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.13

security

condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

Note 1 to entry: Hostile acts or influences can be intentional or unintentional.

[SOURCE: ISO/TS 82304-2:2021, 3.1.22]

3.14

social determinants of health

SDH

non-medical factors that influence health outcomes

Note 1 to entry: Social determinants of health are the conditions in which people are born, grow, work, live, and age, and the wider set of forces and systems shaping the conditions of daily life. These forces and systems include economic policies and systems, development agendas, social norms, social policies and political systems.

Note 2 to entry: Adapted from World Health Organization¹⁾.

1) https://www.who.int/health-topics/social-determinants-of-health#tab=tab_1

3.15

telehealth

use of telecommunication techniques for the purposes of providing telemedicine, medical educations and health education over distance

[SOURCE: ISO/TR 16056-2:2004, 3.75]

3.16

telehealth service

healthcare activity supported at a distance by information and communication technology service(s)

Note 1 to entry: It is possible that the subject of care is not directly involved in a telehealth service, e.g. in the case of tele-dermatology where one physician consults another physician who is at a distant location.

Note 2 to entry: Healthcare activities may include healthcare provider activities such as diagnosis, treatment, review or advice, and self-care activities as prescribed or recommended by a health professional, preventive (educational) advice and management of healthcare processes.

Note 3 to entry: Healthcare activities may include both synchronous (real-time) and asynchronous (delayed) interactions between actors. For example, a radiology examination can be transmitted and subsequently reported by a radiologist over a communications network. A discussion on the diagnostic findings can occur real time over a telephone or video conferencing connection between a patient and health professionals.

[SOURCE: ISO 13131:2021, 3.5.2]

4 Abbreviations

For the purposes of this document, the following abbreviations apply.

AAMI	Association for the Advancement of Medical Instrumentation
AUDA	African Union Development Agency
ANVISA	Agência Nacional de Vigilância Sanitária (Brazil)
CCU	critical care unit
CDC	Centers for Disease Control (US)
CDSCO	Central Drugs Standard Control Organization (India)
DICOM	Digital Image Communication in Medicine
EHR	electronic health record
EMR	electronic medical record
ER	emergency room
EU	European Union
EUA	emergency use authorization
FCC	Federal Communications Commission (US)
FDA	Food and Drug Association (US)
FW	firmware
GP	general practitioner
HCP	health care provider

HHS	Health and Human Services
HL7	Health Level 7
ICU	intensive care unit
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
LTAC	long-term acute care
MDIRA	Medical Device Interoperability Reference Architecture
MFDS	Ministry of Food and Drug Safety (South Korea)
NIST	National Institute of Standards and Technology (US)
ONC	Office of the National Coordinator (US)
PCP	primary care physician
PHD	personal health devices
PMDA	Pharmaceutical and Medical Device Agency (Japan)
PoCD	point-of-care devices
PPE	personal protective equipment
RCC-MH	Remote Connected Care – Mobile Health
SDC	Service oriented Device Communication
SDO	standards development organization
SFDA	Saudi Food and Drug Association
SNF	skilled nursing facility
SW	software
TGA	Therapeutic Goods Administration (Australia)
UDI	unique device identifier
US	United States
VCT	virtual clinical trial

5 RCC-MH care locations and evolution

5.1 What is RCC-MH?

RCC-MH (Remote Connected Care – Mobile Health) belongs to the broader context of telehealth services that allow health care providers (HCPs) and patients to connect using technology to deliver health care remotely. Modalities include:

- synchronous, including real-time phone or live audio-video interaction, typically with a patient using a smartphone, tablet, or computer;

- asynchronous, including “store and forward” technology where messages, images, or data are collected at one point in time and interpreted or responded to later;
- remote patient monitoring, which allows direct transmission of a patient’s clinical measurements (such as vital signs and point-of-care lab results) remotely (real time, intermittent, continuous, etc.);
- patient monitoring at a bedside in ICU (alerts, risk index, reports), which allows for healthcare staff to provide care (as much as possible) while socially distancing themselves from the potentially infectious patient, thus cutting down on infection risk and PPE consumption.

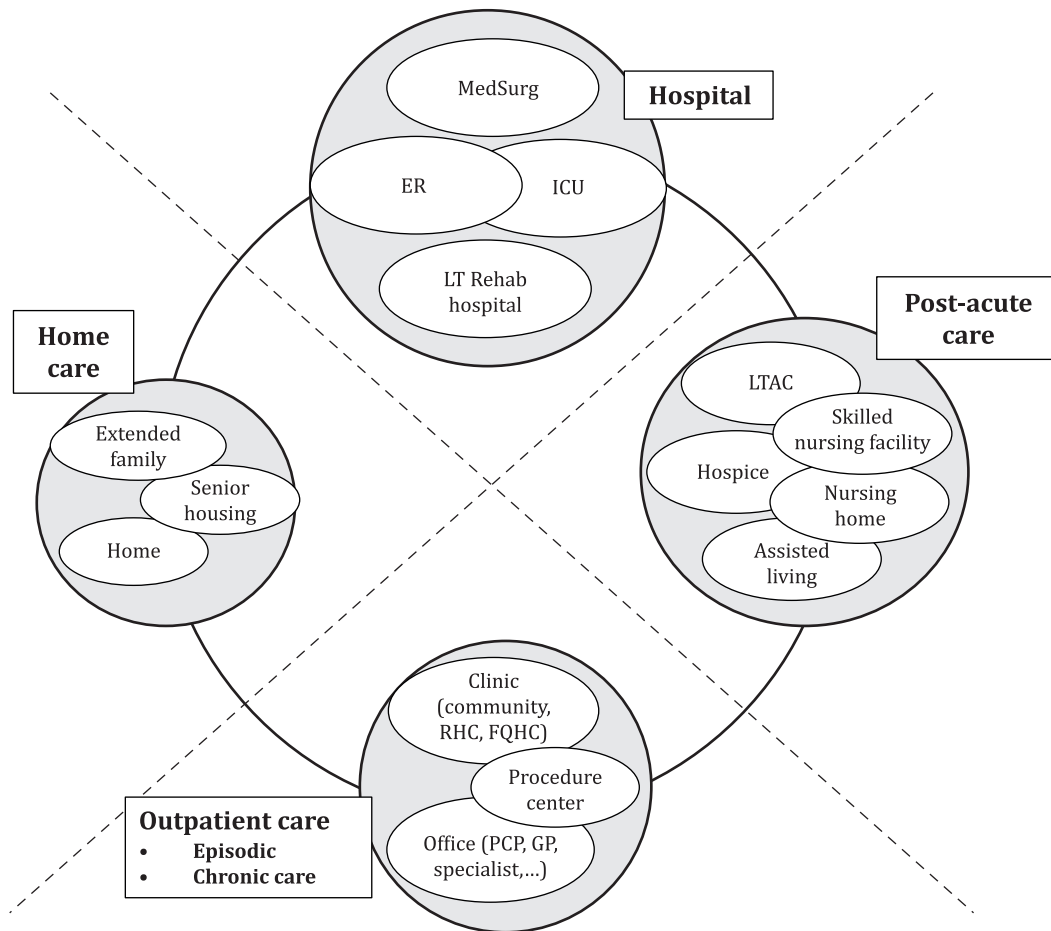
5.2 Care locations: hospitals, home and community, nursing, outpatient

RCC-MH is all about connecting patients and caregivers regardless of where they are located, also recognizing that patients and caregivers can be mobile. There are many ways of grouping these locations and this is the approach adopted in this document (see [Annex K](#)):

- Home and community care: patient home, extended family, senior housing.
- Outpatient care: clinic, procedure centre, office [primary care physician (PCP), general practitioner (GP), specialist, etc.].
- Post-acute care: skilled nursing facility (SNF), long-term acute care (LTAC) facility²⁾, hospice, nursing home, assisted living.
- Hospital: emergency room (ER), intensive care unit (ICU), medical surgery unit (MedSurg), long term rehabilitation hospital.

[Figure 1](#) shows the main locations and pre-pandemic typical patient care locations and flows that have been considered. Most pre-pandemic care was taking place in the hospital or in post-acute care facilities, with much less care taking place in the home or in outpatient locations.

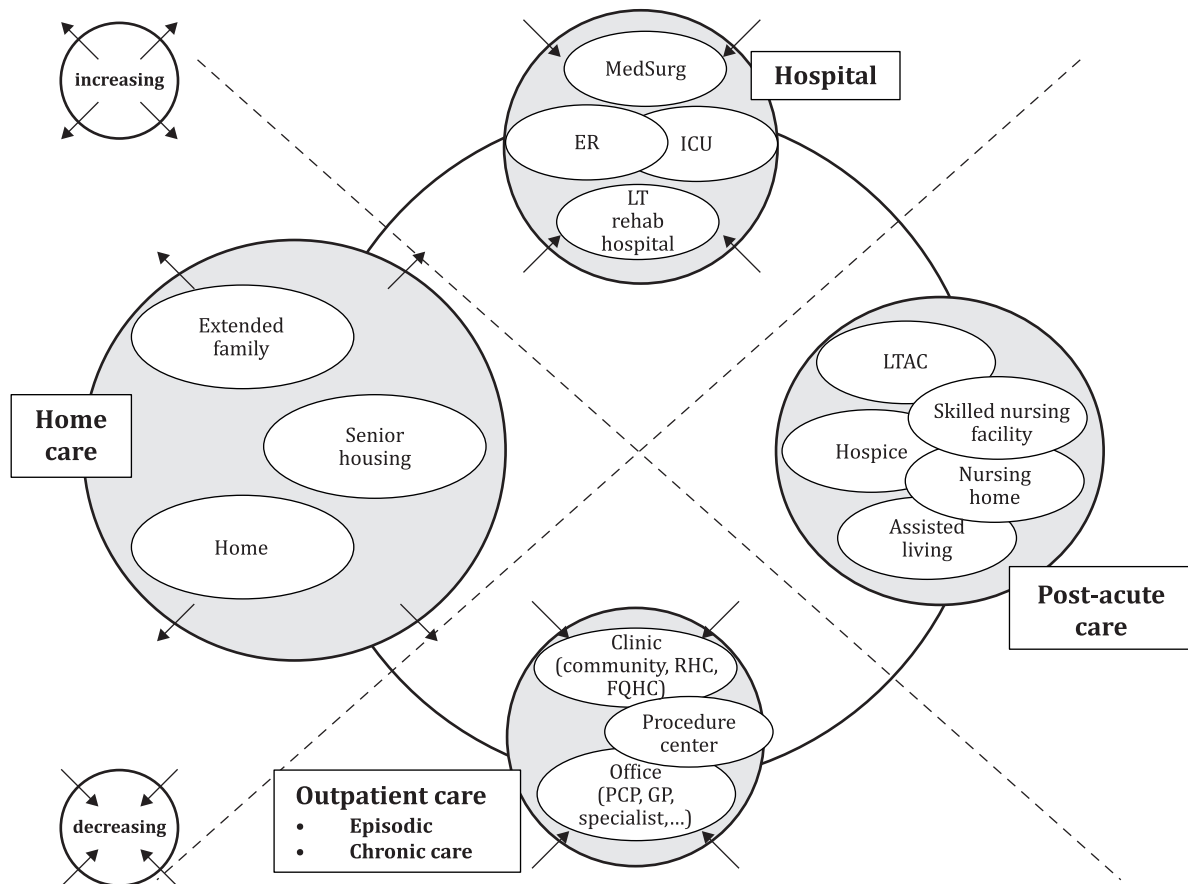
2) An LTAC is a hospital that treats patients with serious medical conditions that require ongoing complex care but no longer need intensive care or extensive diagnostic procedures



NOTE The size of circles is not to scale with the amount of care taking place in the different locations.

Figure 1 — Pre-pandemic locations of care

What healthcare systems have experienced, and rapidly accelerated as a result of the COVID-19 pandemic, is a huge shift of care locations away from traditional hospital and outpatient care areas to home and community care and post-acute care. This transition was also enabled by adjustments to the regulatory and reimbursement environments in various countries (see [Annex A](#)). There are numerous reports showing the exponential increase in virtual visits using telehealth services platforms (see [Annex H](#) for some relevant standards). Patients that would normally be monitored in the hospital, are being transitioned to home care with a similar level of monitoring, sometimes termed the “hospital at home”. [Figure 2](#) illustrates the shifts in the flow of patients.



NOTE The size of circles is not to scale with the amount of care taking place in the different locations.

Figure 2 — Post-pandemic locations of care

While the changes were dramatic in the initial phases of the COVID-19 pandemic, only a partial return to the state that existed pre-pandemic has occurred as the disease subsided and became endemic. Patients find the convenience of telehealth visits and the benefits of being taken care of outside of an institutional setting to be very alluring. There are also economic benefits that have been recognized and will certainly be popular with reimbursement entities such as government and public or private insurers.

6 RCC-MH relevant care delivery modes and use cases

6.1 General

This clause reviews several high-level care delivery modes which illustrate the scope of RCC-MH. These range from in-hospital environments where caregivers could be just around the corner to more 'remote' situations such as a nursing home or patient home. Each of these modes provide opportunities for remote monitoring, diagnosis and care.

A longer list of care delivery locations can be found in [Annex D](#).

6.2 Hospital care

6.2.1 Isolation room

During the COVID-19 pandemic the need to isolate patients became almost routine. However isolated patients become more complicated to manage due to the desire to limit contact as much as possible. Therefore, the

ability to monitor the status of the patient from outside the room and potentially to change device settings (e.g. ventilator or infusion pump settings) becomes increasingly important.

6.2.2 Remote patient surveillance

There are various forms of remote connected care for hospital-based patients, and they have been deployed for decades. Typically, a nurse at a central station can manage patient alarms and alerts, adjust various settings and sometimes control therapy devices. These types of traditional surveillance systems (central stations) are located in the patient care unit/ward, while remote ICUs and remote central stations also focus on patient surveillance but can be located anywhere in the hospital or off hospital premises.

6.3 Home and community care

6.3.1 Telehealth and virtual health

As a result of the pandemic, the number of telehealth or remote physician visits skyrocketed. Most of these sessions were simple one-on-one video conferencing sessions but many were more complex and assisted by linking in remote devices such as ECG monitors, blood pressure monitors and foetal monitors.

6.3.2 Remote delivery of care

6.3.2.1 Remote disease management

A diabetes patient has a continuous glucose monitor (CGM) which is connected to their smartphone. The smartphone, in turn, is connected to a portal (via the cloud) where the data can be viewed by their endocrinologist. The physician can contact the patient to provide feedback, adjust medication, etc. based on the results.

6.3.2.2 “Hospital at home”/virtual ward

Due to the overcrowding and lack of beds in the acute care hospitals, many hospital systems have developed an approach to take appropriate care of patients in their homes. In many cases, this requires setting up a number of monitoring, in vitro medical devices and therapeutic modalities in the home setting and connecting them to a monitoring facility which would typically be in the hospital and staffed by professional nurses and physicians.

6.3.2.3 Virtual clinical trial (VCT)

With the advent of patient-worn sensors and other healthcare devices that can be used by clinical trial subjects, virtual clinical trials are becoming more commonplace. Some of these are relatively small while others can crowdsource data from many thousands of subjects such as users of smartwatches and connected devices who are willing to share their data. There are many challenges in VCTs, including collecting this data, normalizing data nomenclature and data sets, sharing data sets from previous clinical trials, etc.

6.4 Post-acute care

6.4.1 LTAC

A long-term acute care (LTAC) facility is a hospital that specializes in treating patients with serious medical conditions that require intensive care for an extended period of time. LTACs provide more individualized care than other facilities, such as skilled nursing facilities, and are often the right choice for critically ill patients. Patients in an LTAC can be monitored remotely in a manner similar to the in-hospital care surveillance use case discussed in [6.2.2](#).

6.4.2 Skilled nursing facility

While this is not typically done today, a skilled nursing facility can arrange to have its patient-connected medical devices communicate to a remote monitoring service to better track their patients' status. In some ways, this would be similar to the "hospital at home" use case.

6.5 Outpatient care

6.5.1 Remote consultation

A patient is visiting their general practitioner/primary care physician (GP/PCP). The GP/PCP decides that they require a consultation with a remote specialist (potentially across jurisdictional boundaries). Vital signs and other information can be shared immediately and in real-time by the GP/PCP with the specialist.

6.5.2 GP/PCP visit

Currently, GPs/PCPs are just starting to look at data acquired by the patient during their daily activities in real-time or on an as-needed basis. One potential use case would be looking at the CGM readings that have been uploaded to a cloud-based portal, or current readings in the case of an emergency situation.

7 RCC-MH challenges and gaps

7.1 General

Based on the use cases, many clinical challenges have been identified which are listed in [Tables 1](#) through [7](#). Each challenge is further described by the current state/situation and the desired future state/situation. Finally, gaps are identified. [Tables 8](#) through [14](#) in [Clause 8](#) complete the analysis by providing recommendations to address the gaps.

The challenges have been grouped into the following topics (based on ISO 13131):

- safety and quality;
- deployment;
- service support;
- infrastructure;
- interoperability;
- operations;
- security.

7.2 RCC-MH challenges and gaps – Safety and quality

[Table 1](#) includes the current challenges, current states, desired states and resulting gaps and needs related to caregiver or patient safety and services quality.

Table 1 — RCC-MH challenges, gaps and needs – Safety and quality

Challenge	Current state	Desired state	Gap/need
1. Minimize contact with infectious patients for device reading and adjustment.	Caregivers need to enter the patient room to obtain readings and adjust settings on devices. This usually requires a change of PPE for each instance.	Caregivers can remotely obtain readings and adjust settings on devices. Caregivers have reduced patient contact and do not need to change PPE if they don't enter the room.	Devices that can be monitored and adjusted remotely.
2. Devices are always at the latest software release and patch levels with the intention of improving their safety and security.	Devices that were warehoused need to be manually updated. Devices in active use also need to be taken out of service to be manually updated.	Devices actively monitor their SW/FW status and can auto-update or request an update as the need arises.	In some cases, vendors support remote SW updates, but they are done via proprietary protocols and approaches. Ideally, an industry-wide standards-based interoperable approach can be developed and adopted (see Annex B).
	Device cannot be updated to a new OS level because the manufacturer has not yet verified and released it for deployment.	Devices can actively monitor their SW/FW status and can auto-update only when the update has been authorized by the manufacturer	This can be difficult in practice especially on mobile platforms such as iOS or Android where multiple apps have different dependencies on the underlying operating system (OS).
3. MH apps are always at the latest software releases and patch levels with the intention of improving their safety and security.	MH apps on Android or iOS platforms have the ability to update their SW. There can be challenges if there are compatibility issues with connected sensors/devices.	MH app updates need to be synchronized with connected sensor/device SW and FW. In some cases, the update will need to be delayed. In other cases, the app can update the sensor/device SW and/or FW.	Support of an open approach to acquiring and updating connected sensor/device SW or FW, or both.
4. Selection of appropriate apps when there are millions to choose from.	It is not possible to assess the millions of mobile health apps in an objective manner. Information such as app support for privacy, security, etc. is very difficult to obtain.	Given the rapid increase in the number and the variable quality of mobile health apps, users and professionals need some way of assessing these apps in a consistent manner, especially in the areas of privacy and security.	Users require a consistent way of labelling mobile health apps in order to better compare them. Ideally, they would be evaluated by independent parties to provide users with objective feedback.
^a https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics			

Table 1 (continued)

Challenge	Current state	Desired state	Gap/need
5. Track device usage, status for recall or infection control purposes.	Most devices are tracked by association with other devices at a location. When they are moved that information is lost.	Devices can also be tracked via a globally unique ID which can help trace the device as well as understand its provenance.	Although there are unique device identification (UDI) schemes in Europe, the United States, China, etc., there are no requirements for electronic reporting of the UDI (unique device identifier) ^a .
6. Integrators of RCC-MH solutions need to understand which standards the components comply with.	Medical devices are typically tested for conformity with IEC 60601 series and ISO/IEC 80601 series standards. Conformity testing with other standards is very rare and difficult to uncover.	Standards are written to support easy conformity assessment and discovery of appropriate devices including apps and applications.	Standards that explicitly support conformity assessment. Device registries that include conformity details.
7. Regulatory approval of RCC-MH components takes advantage of uniform conformance testing approaches and product certification.	From a regulatory perspective conformity and certification of a device's cybersecurity and interoperability functions does not currently bring any additional benefits to the manufacturer. For example, 1:1 pairwise testing is required in order to claim interoperability for a specified use.	Devices that can demonstrate interoperability and/or cybersecurity certifications benefit from a regulatory oversight perspective. Certified interoperable devices can claim compatibility with other certified devices conforming with the same standards. An example would be the FDA ASCA scheme (see Annex L).	Regulatory recognized certification bodies that can attest to device conformity with specific standards. Acceptance of certifications by the regulatory bodies.
^a https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics			

7.3 RCC-MH challenges and gaps – Deployment

[Table 2](#) includes the current challenges, current states, desired states and resulting gaps and needs related to the deployment and operation of RCC-MH solutions.

Table 2 — RCC-MH Challenges, gaps and seeds – Deployment

Challenge	Current state	Desired state	Gap/need
8. Elimination of inter- and intra-system dependencies that prevent SW/FW updates or break integration when updated.	System component (device, smartphone, PC, etc.) updates can break or affect the performance of the app or application.	Components can automatically check the compatibility of updates with other components being used.	This is a complex topic that is not currently addressed, potentially leading to unsafe updates or an inability to do any updates.
9. Seamlessly integrate devices from uncontrolled sources such as the strategic stockpile, loaned equipment or donated new equipment with the rest of the clinical IT infrastructure.	Hospitals can integrate devices they already use relatively quickly. However, new (to them) devices normally take months of careful evaluation and integration planning.	Out-of-the-box plug and play integration of devices using open standards-based interoperability.	Currently all devices require an integration project since very few support open interoperability standards.
10. Track device location for optimal utilization, especially during device shortage situations.	Unless a device is in active use, it usually has no knowledge of its location and does not report it. Devices can be stored in strange locations.	Device logical or absolute location and identification are available at all times even if the device is in standby or turned off. It is essential that tracking be done in such a way that patient privacy is preserved.	Continuous reporting of device GPS location even if the device is turned off.
11. Integrate a mix of consumer and medical devices from various sources (including national stockpile) into physician offices and home environments.	Personal health and medical devices need to be integrated using 3 rd party middleware which adds cost and effort and limits the choice of which devices can be used.	Ability to take a device 'out-of-the-box' and integrate it with RCC-MH solutions with minimal effort, limited to simple configuration and provisioning.	While standards which support seamless interoperability are available, adoption is very sparse and needs to be encouraged.
12. Users and/or caregivers with minimal training can set up, configure, integrate, and maintain devices including device security posture.	Currently, specially trained personnel are required to integrate and install remote connected care solutions.	As devices typically designed for simple consumer applications and devices designed for professional (in-hospital) applications can be integrated together in the remote care, setup and maintenance will become very important considerations.	Various available standards such as the ISO/IEEE 11073 series, IHE profiles, etc. need to be reviewed from a provisioning and deployment perspective to assess the level of sophistication and training required to deploy systems based on these standards.
13. Integrators of RCC-MH solutions need to understand which standards the components comply with.	It is very difficult to find devices and solutions that comply with specific standards. Most standards are not written with conformance and certification in mind.	Standards are written to support easy conformity assessment and discovery of appropriate devices including apps and applications.	Need consistency and easy access to standards compliance claims as well as any relevant conformity assessment activities

7.4 RCC-MH challenges and gaps – Service support

[Table 3](#) includes the current challenges, current states, desired states and resulting gaps and needs related to the maintenance of RCC-MH solutions, especially the challenges due to their remote nature.

Table 3 — RCC-MH challenges, gaps and needs – Service support

Challenge	Current state	Desired state	Gap/need
14. Managing, monitoring and caring for remote patients when the responsible party (physician, hospital command center, etc.) is far away			
a) Improve the logistics of device acquisition	Currently, it is quite difficult to assess which devices and apps will be amenable to RCC-MH deployment.	There are a number of logistics approaches for creating RCC solutions beyond just the technical aspects.	Approaches for deployment of devices in non-traditional settings need to be analysed and best practices developed.
b) Reliable on-site device provisioning / deployment	Currently, deploying complicated RCC-MH solutions requires considerable expertise.	As devices typically designed for simple consumer applications and devices designed for professional (in-hospital) applications can be integrated together in the home setup, deployment becomes a critical issue.	Deployments in non-traditional environments need to take into account non-technical users. They also need to take into account environments with different challenges than traditional hospital deployments.
c) Remote device provisioning / deployment	Patients, in some cases, need to install and provision their own devices with little guidance. This can lead to unreliable connectivity or total failure to connect. Another concern is the wide variability of home connectivity options.	Devices are either very easy to deploy or properly provisioned and authenticated / authorized remotely to participate in the system.	Need to assess whether standards are available that address remote provisioning and deployment.
d) Remote device technical monitoring and troubleshooting	For most devices, the need to deal with troubleshooting when 'things go wrong' has not been adequately considered.	Medical devices that can be set up, provisioned and diagnosed remotely with the understanding that they are part of an overall systems-based solution.	Need to assess whether appropriate standards are available that address remote technical monitoring, troubleshooting and remediation.

Table 3 (continued)

Challenge	Current state	Desired state	Gap/need
e) Remote patient monitoring and timely response to patient alerts	Local emergency care services are used which can result in long reaction times. In addition, those personnel have minimal understanding of the patient's medical status.	If very sick patients are monitored remotely, mechanisms need to be in place to respond very quickly to serious clinical issues.	RCC-MH solutions need to take into account that it can take relatively long time to deliver care to a patient in an emergency condition.
f) Acquisition of technical error logs	Error logs, if available, can only be accessed at the device itself.	As part of a remote monitoring and care platform, remote diagnosis of issues is critical, and access to technical error logs is an important aspect of diagnosing technical issues.	Need to develop standards to remotely acquire 'logs' from devices as well as standard formats, syntax and semantics.
g) Acquisition of user logs	User logs, if available, can only be accessed at the device itself.	As part of a remote monitoring and care platform, remote diagnosis of issues is critical, and access to user logs is an important aspect of diagnosing user issues.	Need to develop standards to remotely acquire 'logs' from devices as well as standard formats, syntax and semantics.

7.5 RCC-MH challenges and gaps – Infrastructure

Table 4 includes the current challenges, current states, desired states and resulting gaps and needs related to the fact that the deployment infrastructure is typically not controlled by the deployment organization.

Table 4 — RCC-MH challenges, gaps and needs – Infrastructure

Challenge	Current state	Desired state	Gap/need
15. Dealing with unknown and uncontrolled networking infrastructure	The infrastructure in a hospital is 'controlled' when compared to post-acute care facilities, patient homes which can be in apartments (competing wireless networks), rural areas (poor internet connectivity) and other non-traditional challenging environments.	Reduce or eliminate network technology induced errors and lack of communications reliability.	Possible approaches include: — specific bandwidth set asides for medical purposes; — prioritization of traffic for medical purposes; — improvements in rural connectivity infrastructure.

7.6 RCC-MH challenges and gaps – Interoperability

Table 5 includes the current challenges, current states, desired states and resulting gaps and needs related to the current state of 'dysfunctional interoperability' which forces integrators to deal with non-standard interfaces.

Table 5 — RCC-MH challenges, gaps and needs – Interoperability

Challenge	Current state	Desired state	Gap/need
16. Harmonizing and adopting data standards for interoperability and cybersecurity for RCC-MH	The vast majority of RCC devices use proprietary approaches for communicating their information. This necessitates the addition of translators, dongles, etc. to get access to this data and adds considerable cost and complexity.	Wide availability of devices which support open interoperable communication approaches which can be effortlessly integrated into RCC-MH solutions.	While standards exist (see Annex F), and technical gaps can be addressed, general industry adoption will be the next challenge. This will require: — regulatory support and guidance at national and international levels; — engagement of stakeholders from device / IT industry.
17. Collection of lab data from home-based point-of-care equipment / SHIELD / OO	Many manufacturers are working on home diagnostic systems for and other pandemic relevant lab tests. These devices do not necessarily report their results and the ones that do use proprietary approaches.	Manufacturers provide home diagnostic systems for and other point-of-care lab tests. These devices report their results in a consistent, trusted way which supports public health monitoring.	A secure, reliable, open and interoperable approach needs to be defined in order to support this need (see Annex B). The approach needs to be trusted and maintain patient privacy.

7.7 RCC-MH challenges and gaps – Operations

[Table 6](#) includes the current challenges, current states, desired states and resulting gaps and needs related to using RCC-MH solutions for operational environments such as clinical trials and collection of real-world evidence.

Table 6 — RCC-MH challenges, gaps and needs – Operations

Challenge	Current state	Desired state	Gap/need
18. Conducting virtual remote clinical trials (VCTs) to innovate and support new medical device technologies, procedures, pharma, etc.			
a) Supporting specific regulatory documentation requirements for clinical trials.	Clinical trials can require additional meta-data that is not normally required for day-to-day use.	Data provided by sensors/devices include necessary metadata that can be used to support clinical trials.	Need to develop a Technical Report or Specification which specifies any special data elements required to support VCTs.
b) Accepting measurement and other data from different devices making the same physiological measurements.	Currently, clinical trials need to standardize on a very limited set of sensors/devices for a desired measurement.	Subjects can use the sensor/device of their choosing since the data can be easily accepted and normalized among various devices.	Need to treat certified devices that conform to the same technical interoperability, clinical and cybersecurity standards as interchangeable.
c) Enabling the reuse of clinical trial data bases for other clinical trials.	Currently the data accumulated for one clinical trial can only be used for that particular trial.	Clinical trial data bases can be used for other trials.	Use of open standards-based clinical trial data bases that share format, nomenclature and information models.
19. Surveillance, real world evidence (RWE) and other public health functions for medical devices	The collection of RWE is not typically a high priority for device and app manufacturers.	RCC-MH solutions need to support the need for collection of public health related information while maintaining patient privacy.	Need for high-quality and structured data based on well-defined harmonized open standards to use them appropriately for public health informatics and premarket/post-market evaluations of medical devices based on real world data.
20. Device/Apps usage logs	This may be supported by some vendors in a proprietary way.	Universal support based on open standards.	Use of open standards which support interoperable solutions for usage logs.

7.8 RCC-MH challenges and gaps – Security

[Table 7](#) includes the current challenges, current states, desired states and resulting gaps and needs related to the need to maintain a secure environment to protect the devices and the people.

Table 7 — RCC-MH challenges, gaps and needs – Security

Challenge	Current state	Desired state	Gap/need
21. Maintaining a secure end-to-end connection.	The communications link from the device/patient to the caregiver transits the internet affording very little control of the environment. This opens the door to numerous potential security risks.	Devices and systems employ accepted cyber-security practices and are built with the realization that the data will be traversing uncontrolled network infrastructure.	Standards are needed that provide clear requirements to developers and implementers regarding cybersecurity approaches that provide end-to-end security.
22. Developers of RCC-MH components need clear requirements to protect their products from cybersecurity risks.	Traditional risk assessment approaches are deployed with inconsistent cyber risk mitigation practices and techniques used.	Specific requirements are provided against which consistent conformity assessments can be conducted.	Cybersecurity technical specifications which result in clear requirements that support conformance testing and open a path to potential future certification.
23. Developers need guidance on how to achieve effective security, including:			
a) How to determine how secure to make the device.	Current approaches to determining how to secure devices leave a considerable amount up to the discretion of the manufacturer.	Devices meet a defined, use-case, and risk-based security baseline and can be assessed and certified against that baseline.	Need to establish standards to define device baseline security. Need for global standards organizations to establish a certification scheme against the baseline. These will likely require a breakdown as per device type, use case, and risk.
b) How to communicate securely.	The use of proprietary communication protocols leads to proprietary security approaches which can be insecure. Further, some standards-based security protocols do not include or have only recently included security for data in transit.	Devices communicate securely with other devices and systems using open, standards-based protocols.	Existing secure communication standards (HL7, DICOM) could be assessed for their security provisions. Adoption hurdles could be identified and addressed. Devices types using other or proprietary protocols could be assessed for inclusion in HL7/DICOM or new secure communication standards would need to be established.
c) How to maintain the security of the device over time.	Currently manufacturers have inconsistent and incompatible approaches to security updates.	Devices maintain their security baseline over their useful life.	Need to establish standards to define security maintenance. This will likely require a breakdown as per device type, use case, and risk.

Table 7 (continued)

Challenge		Current state	Desired state	Gap/need
d)	How to track the security status of the device.	It is very challenging to determine whether a device has been compromised and to report its security status.	Devices communicate their security status and detected security events using open standards-based protocols.	Need to establish standards that define how device security status can be communicated. This will likely require a breakdown as per device type, use case, and risk.

8 RCC-MH recommendations

8.1 Recommendations

[Tables 1](#) to [7](#) identified RCC-MH challenges, gaps and needs. [Tables 8](#) to [14](#) are based on [Tables 1](#) to [7](#) and add a column for recommendations.

They are based on a review of the various existing standards and regulations that are relevant to RCC-MH and recommend new standards development efforts which will address the identified gaps. The background information can be found in [Annexes A](#) through [L](#).

Despite the desire to deploy RCC-MH numerous challenges and roadblocks exist which need to be addressed as soon as possible.

As in [Tables 1](#) to [7](#), the challenges have been grouped into the following topics (based on ISO 13131):

- safety and quality;
- deployment;;
- service support
- infrastructure;
- interoperability;
- operations;
- security.

8.2 RCC-MH recommendations – Safety and quality

[Table 8](#) includes the current challenges, desired states and resulting gaps/needs and provides recommendations related to caregiver or patient safety and/or services quality.

Table 8 — RCC-MH recommendations – Safety and quality

Challenge	Desired state	Gap/need	Recommendations
1. Minimize contact with infectious patients for device reading and adjustment.	Remotely obtain readings and adjust settings on devices. Caregivers have reduced patient contact and do not need to change PPE if they don't enter the room.	Devices that can be monitored and adjusted remotely.	The IEEE 11073 SDC (see Annex F) suite of standards can provide a technical solution for remote control of point-of-care devices. Implementation and acceptance of these standards is the main hurdle. Additional specialization standards, a supportive ecosystem and regulatory acceptance can help.
2. Devices are always at the latest software release and patch levels with the intention of improving their safety and security.	Devices actively monitor their SW/FW status and can auto-update or request an update as the need arises.	In some cases, vendors support remote SW updates, but they are done via proprietary protocols and approaches. Ideally an industry-wide standards-based interoperable approach can be developed and adopted (see Annex B).	Standards are required that support the post-release phase of the device life cycle. One aspect of these standards should specify an industry wide approach to safe and secure remote software and firmware updates.
	Devices can actively monitor their SW/FW status and can auto-update only when the update has been authorized by the manufacturer	This can be difficult in practice especially on mobile platforms such as iOS or Android where multiple apps have different dependencies on the underlying OS.	Software and firmware update solutions should take into account the status of the underlying platform and vice versa, recognizing that most solutions are a conglomeration of different parts and pieces.
3. MH apps are always at the latest software releases and patch levels with the intention of improving their safety and security.	MH app updates need to be synchronized with connected sensor/device SW and FW. In some cases, the update will need to be delayed. In other cases, the app can update the sensor/device SW and/or FW.	Support of an open approach to acquiring and updating connected sensor/device SW and/or FW.	An industry-wide standards-based approach should be developed to acquire sensor/device SW and/or FW and to update connected devices.
4. Selection of appropriate apps when there are millions to choose from {GD}	Given the rapid increase in the number and the variable quality of mobile health apps, users and professionals need some way of assessing these apps in a consistent manner, especially in the areas of privacy and security.	Users require a consistent way of labelling mobile health apps in order to better compare them. Ideally, they would be evaluated by independent parties to provide users with objective feedback.	Standards-based methods of verifying app performance based on a set of metrics should be applied. This would include clear means for disclosure of performance appropriate for clinical users (not necessarily end users).

Table 8 (continued)

Challenge	Desired state	Gap/need	Recommendations
5. Track device usage, status for recall or infection control purposes.	Devices can also be tracked via a globally unique ID which can help trace the device as well as understand its provenance.	While there are Unique Device Identification (UDI) schemes in Europe, the United States, China, etc. there are no requirements for electronic reporting of the UDI.	Each device should be uniquely identified. UDI is a good start but is not very secure. IHE should consider a project to assess the use cases, requirements and potential technical solutions for device tracking. Device tracking should be done in such a way that patient privacy is preserved. The UMHA Standard in HL7, parts of USCDI v2 and IHE DEV MEM LS address aspects of this gap (see Annex F for more information).
6. Integrators of RCC-MH solutions need to understand which standards the components comply with.	Standards are written to support easy conformity assessment and discovery of appropriate devices including apps and applications.	Standards that explicitly support conformity assessment. Device registries that include conformity details.	Establishment of conformity assessment infrastructure.
7. Regulatory approval of RCC-MH components takes advantage of uniform conformance testing approaches and product certification.	Devices that can demonstrate interoperability and/or cybersecurity certifications benefit from a regulatory oversight perspective. Certified interoperable devices can claim compatibility with other certified devices conforming with the same standards. An example would be the FDA ASCA scheme (see Annex L).	Regulatory recognized certification bodies that can attest to device conformity with specific standards. Acceptance of certifications by the regulatory bodies.	Establishment of a methodology to recognize certification houses for specific RCC-MH relevant standards. Adjusting regulatory assessment processes so that manufacturers are motivated to take advantage of certified paths for product releases.

8.3 RCC-MH recommendations – Deployment

[Table 9](#) includes the current challenges, desired states and resulting gaps and needs and provides recommendations related to the deployment and operation of RCC-MH solutions.

Table 9 — RCC-MH recommendations – Deployment

Challenge	Desired state	Gap/need	Recommendations
8. Elimination of inter- and intra-system dependencies that prevent SW/FW updates or break integration when updated.	Components can automatically check the compatibility of updates with other components being used.	This is a complex topic that is not currently addressed, potentially leading to unsafe updates or an inability to do any updates.	An industry-wide standards-based approach should be developed to identify SW and FW release levels and to manage updates so that they do not disrupt operations or impact patient safety.
9. Seamlessly integrate devices from uncontrolled sources such as the strategic stockpile, loaned equipment or donated new equipment with the rest of the clinical IT infrastructure.	Out of the box plug and play integration of devices using open standards-based interoperability.	Currently all devices require an integration project since very few support open interoperability standards.	The objective of the IEEE 11073 SDC series (see Annex F) is to support plug-and-play operation. A roadmap should be developed to attain this goal. It is unrealistic to test all device combinations when hundreds of different devices exist.
10. Track device location for optimal utilization, especially during device shortage situations.	Device logical or absolute location and identification is available at all times even if the device is in standby or turned off. It is essential that tracking be done in such a way that patient privacy is preserved.	Continuous reporting of device GPS location even if the device is turned off.	Sensor/device communication standards should accommodate location reporting. IHE MEM LS is one approach (see Annexes F and J). Reporting of the device location can be accomplished using separate location tags, otherwise the device should support an independent device location sub-system. Device tracking should be done in such a way that patient privacy is preserved.
11. Integrate a mix of consumer and medical devices from various sources (including national stockpile) into physician offices and home environments.	Ability to take a device 'out-of-the-box' and integrate it with RCC-MH solutions with minimal effort limited to simple configuration and provisioning.	While standards which support seamless interoperability are available, adoption is very sparse and needs to be encouraged.	Adoption of a small number of open standards will enable these kinds of applications. In addition, this will also encourage the development of an ecosystem of certifying bodies and regulatory acceptance (see Annex J).
12. Users and/or caregivers with minimal training can set up, configure, integrate, and maintain devices including device security posture.	As devices typically designed for simple consumer applications and devices designed for professional (in-hospital) applications can be integrated together in the remote care setup and maintenance will become very important considerations.	Various available standards such as the 11073 series, IHE profiles, etc. need to be reviewed from a provisioning and deployment perspective to assess the level of sophistication and training required to deploy systems based on these standards.	Standards should address installation, setup and maintenance for users who are not technically savvy.
13. Integrators of RCC-MH solutions need to understand which standards the components comply with.	Standards are written to support easy conformity assessment and discovery of appropriate devices including apps and applications.	Need consistency and easy access to standards compliance claims as well as any relevant conformity assessment activities	Standards relating to consistent presentation of standards compliance and assessment claims. A registry may be considered.

8.4 RCC-MH recommendations – Service support

[Table 10](#) includes the current challenges, desired states and resulting gaps/needs and provides recommendations related to the maintenance of RCC-MH solutions especially due to their remote nature.

Table 10 — RCC-MH recommendations – Service support

Challenge	Desired state	Gap/need	Recommendations
14. Managing, monitoring and caring for remote patients when the responsible party (physician, hospital command centre, etc.) is miles away			
a) Improve the logistics of device acquisition	There are a number of logistics approaches for creating RCC solutions beyond just the technical aspects.	Approaches for deployment of devices in non-traditional settings need to be analysed and best practices developed.	Analysis of best practices for deploying and managing remote monitoring and care sites should be performed with recommended best practices. These should be published in Technical Reports to guide developers.
b) Reliable on-site device provisioning / deployment	As devices typically designed for simple consumer applications and devices designed for professional (in-hospital) applications can be integrated together in the home setup deployment becomes a critical issue.	Deployments in non-traditional environments need to take into account non-technical users. They also need to take into account environments with different challenges than traditional hospital deployments.	Various available standards should be reviewed from a provisioning and deployment perspective to assess the level of sophistication and training required to deploy systems based on these standards. See Annex J for a partial list of relevant standards. Guidance should be developed to deal with challenging network environments.
c) Remote device provisioning / deployment	Devices are either very easy to deploy or properly provisioned and authenticated / authorized remotely to participate in the system?	Need to assess whether standards are available that address remote provisioning and deployment.	Candidate standards should be reviewed from a remote provisioning and deployment perspective to assess the degree they support remote provisioning and maintenance.
d) Remote device technical monitoring and troubleshooting	Medical devices that can be set up, provisioned and diagnosed remotely with the understanding that they are part of an overall systems-based solution.	Need to assess whether appropriate standards are available that address remote technical monitoring, troubleshooting and remediation.	Many medical device vendors do provide remote servicing capabilities. However, these are all proprietary and separate from each other. Standards are not available. Ideally, an industry-wide standards-based interoperable approach can be developed and adopted.