



**HL7/ISO TS 5615 Specification:**  
**Remote Connected Care and Mobile Health,**  
**Edition 1**  
May 2025

**HL7 STU Ballot**

**Sponsored by:**  
**Mobile Health Work Group**

Copyright © 2025 Health Level Seven International ® ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher. HL7 and Health Level Seven are registered trademarks of Health Level Seven International. Reg. U.S. Pat & TM Off.

Use of this material is governed by HL7's [IP Compliance Policy](#).

**IMPORTANT NOTES:**

HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document**, you are not authorized to access or make any use of it. To obtain a free license, please visit <http://www.HL7.org/implement/standards/index.cfm>.

**If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material")**, the following describes the permitted uses of the Material.

**A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS**, who register and agree to the terms of HL7's license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.

INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.

**B. HL7 ORGANIZATION MEMBERS**, who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

**C. NON-MEMBERS**, who register and agree to the terms of HL7's IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.

NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.

Please see <http://www.HL7.org/legal/ippolicy.cfm> for the full license terms governing the Material.

**Ownership.** Licensee agrees and acknowledges that **HL7 owns** all right, title, and interest, in and to the Materials. Licensee shall **take no action contrary to, or inconsistent with**, the foregoing.

**Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials may contain and/or reference intellectual property owned by third parties ("Third Party IP"). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third Party IP right by the Licensee remains the Licensee's liability.**

Following is a non-exhaustive list of third-party terminologies that may require a separate license:

Terminology	Owner/Contact
Current Procedures Terminology (CPT) code set	American Medical Association <a href="https://www.ama-assn.org/practice-management/cpt-licensing">https://www.ama-assn.org/practice-management/cpt-licensing</a>
SNOMED CT®	SNOMED CT® International; <a href="http://www.snomed.org/snomed-ct/get-snomed-ct">http://www.snomed.org/snomed-ct/get-snomed-ct</a> or <a href="mailto:info@ihtsdo.org">info@ihtsdo.org</a>
Logical Observation Identifiers Names & Codes (LOINC®)	Regenstrief Institute
International Classification of Diseases (ICD) codes	World Health Organization (WHO)
NUCC Health Care Provider Taxonomy code set	American Medical Association. Please see <a href="http://www.nucc.org">www.nucc.org</a> . AMA licensing contact: 312-464-5022 (AMA IP services)



# FINAL DRAFT

## Technical Specification

### ISO/DTS 5615

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

*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/TC 215

Secretariat: **ANSI**

Voting begins on:  
**2024-11-29**

Voting terminates on:  
**2025-02-21**

## ISO/CEN PARALLEL PROCESSING

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO and HL7 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviations</b> .....	<b>4</b>
<b>5 RCC-MH care locations and evolution</b> .....	<b>5</b>
5.1 What is RCC-MH?.....	5
5.2 Care locations: hospitals, home and community, nursing, outpatient.....	6
<b>6 RCC-MH relevant care delivery modes and use cases</b> .....	<b>8</b>
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
<b>7 RCC-MH challenges and gaps</b> .....	<b>10</b>
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
<b>8 RCC-MH recommendations</b> .....	<b>19</b>
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
<b>9 Conclusions and path forward</b> .....	<b>28</b>
9.1 Recommended standards work items.....	28
9.2 Final thoughts.....	30
<b>Annex A (informative) Regulatory and legal reactions to the pandemic</b> .....	<b>31</b>
<b>Annex B (informative) RCC-MH interoperability challenges</b> .....	<b>44</b>
<b>Annex C (informative) Nomenclature standards landscape for medical devices</b> .....	<b>47</b>
<b>Annex D (informative) Accelerating safe effective &amp; secure (SES) RCC-MH</b> .....	<b>53</b>
<b>Annex E (informative) RCC-MH socio-technical challenges</b> .....	<b>56</b>

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

## 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 document 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](http://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](http://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](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration 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](http://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 [\[26\]](#)]

### 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 [\[27\]](#)]

### 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 [\[36\]](#)]

### 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 Organization<sup>1)</sup>.

---

1) [https://www.who.int/health-topics/social-determinants-of-health#tab=tab\\_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**

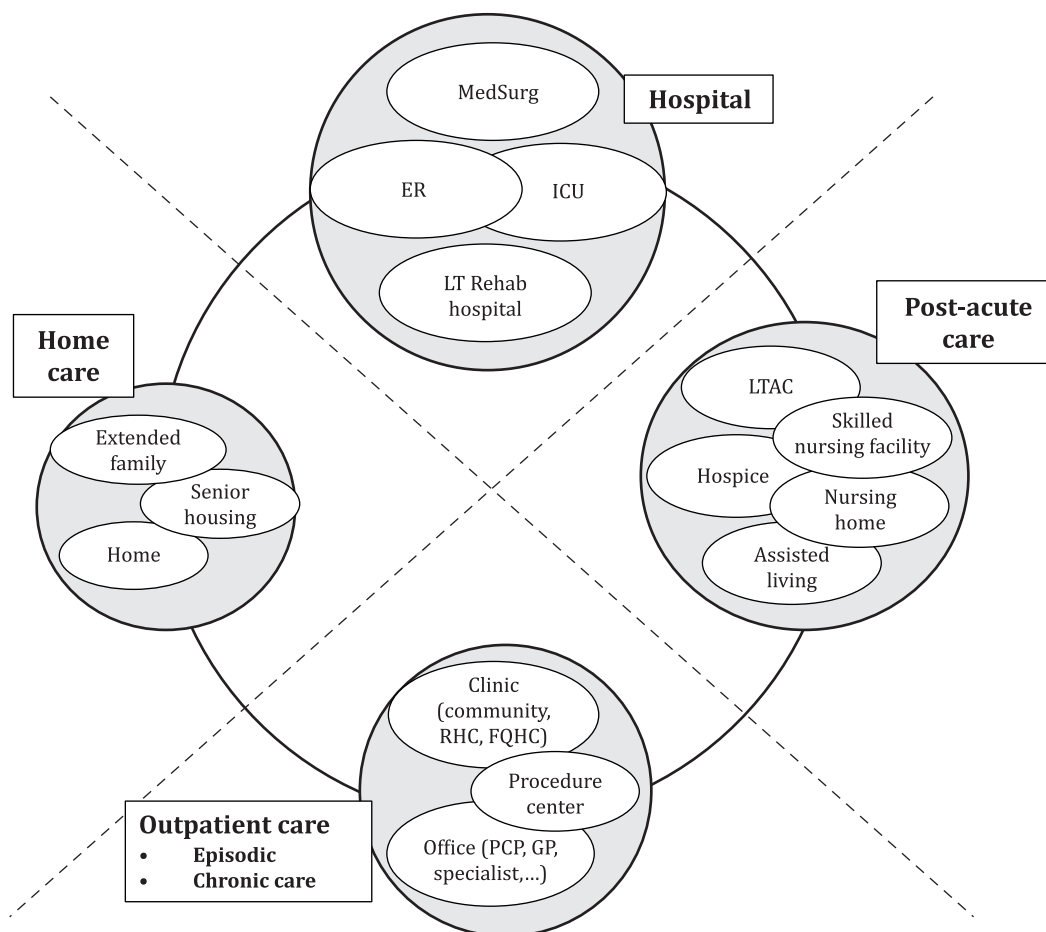
RCC-MH is all about connecting patients and caregivers regardless of where they are located, also recognizing that patients and caregivers can be mobile. There are many ways of grouping these locations and this is the approach adopted in this document (see [Annex K](#)):

- 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) facility<sup>2)</sup>, 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.

---

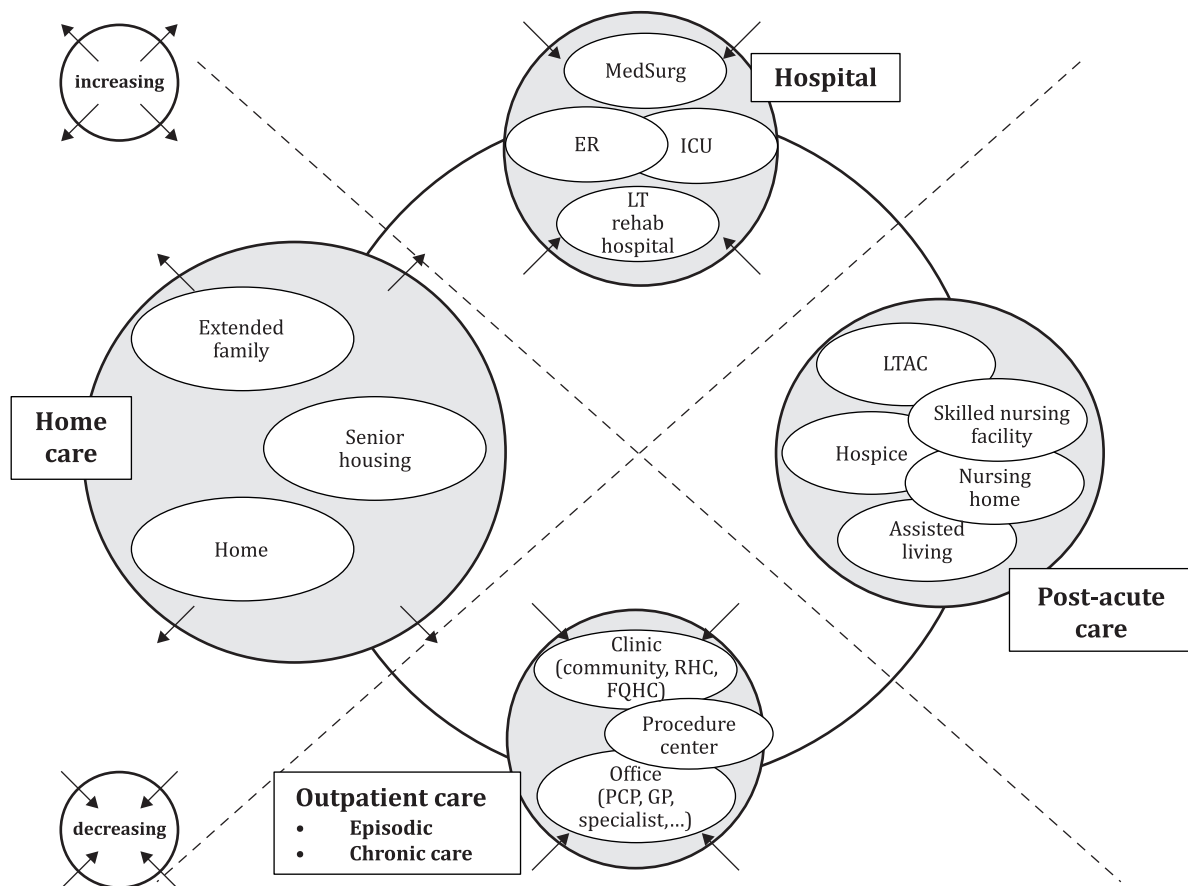
2) An LTAC is a hospital that treats patients with serious medical conditions that require ongoing complex care but no longer need intensive care or extensive diagnostic procedures



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 <a href="#">Annex B</a> ).
	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.
<sup>a</sup> <a href="https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics">https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics</a>			

**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) <sup>a</sup> .
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 <a href="#">Annex L</a> ).	Regulatory recognized certification bodies that can attest to device conformity with specific standards. Acceptance of certifications by the regulatory bodies.
<sup>a</sup> <a href="https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics">https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics</a>			

### 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 <sup>rd</sup> 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 <a href="#">Annex F</a> ), and technical gaps can be addressed, general industry adoption will be the next challenge. This will require: <ul style="list-style-type: none"> <li>— regulatory support and guidance at national and international levels;</li> <li>— engagement of stakeholders from device / IT industry.</li> </ul>
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 <a href="#">Annex B</a> ). 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 <a href="#">Annex F</a> ) 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 <a href="#">Annex B</a> ).	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 <a href="#">Annex F</a> 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 <a href="#">Annex L</a> ).	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 <a href="#">Annex F</a> ) 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 <a href="#">Annexes F</a> and <a href="#">J</a> ). 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 <a href="#">Annex J</a> ).
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 center, 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.



**Table 10 (continued)**

Challenge	Desired state	Gap/need	Recommendations
e) Remote patient monitoring and timely response to patient alerts	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 relatively long times it can take to deliver care to a patient in an emergency condition.	The sooner it is detected that a patient's condition is deteriorating, the better the outcome. Best practices and procedures should be documented and shared.
f) Acquisition of technical error logs	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.	An industry-wide standards-based interoperable approach should be developed for the remote acquisition and formatting of device technical error logs. These logs should include contents in accordance with IEC 80601-1-8 and AAMI 2700-2-1.
g) Acquisition of user logs	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.	An industry-wide standards-based interoperable approach should be developed for the remote acquisition and formatting of device user logs. These logs should include contents in accordance with IEC 80601-1-8 and AAMI 2700-2-1.

## 8.5 RCC-MH recommendations – Infrastructure

[Table 11](#) includes the current challenges, desired states and resulting gaps/needs and provides recommendations related to the fact that the deployment infrastructure is typically not controlled by the deployment organization.

**Table 11 — RCC-MH recommendations – Infrastructure**

Challenge	Desired State	Gap/Need	Recommendations
15. Dealing with unknown and uncontrolled networking infrastructure	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	Standards related to consistent documentation and presentation of network infrastructure interdependencies should be developed. (Some guidance may be found in the ISO/IEC 80001 series)

## 8.6 RCC-MH recommendations – Interoperability

[Table 12](#) includes the current challenges, desired states and resulting gaps/needs and provides recommendations related to the current state of 'dysfunctional interoperability' which forces integrators to deal with non-standard, proprietary, interfaces.



**Table 12 — RCC-MH recommendations – Interoperability**

Challenge	Desired State	Gap/Need	Recommendations
16. Harmonizing and adopting data standards for interoperability and cybersecurity for RCC-MH	Wide availability of devices which support open interoperable communication approaches which can be effortlessly integrated into RCC-MH solutions.	While standards exist 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	Active involvement and support by regulatory agencies for the development and related ecosystem activities leading to multi-party standards-based interoperability.
17. Collection of lab data from home-based point-of-care equipment / SHIELD / OO	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. The approach need to be trusted and maintain patient privacy.	Clinical laboratory data orders, results, and interpretations are among the most important types of data for clinical care, public health, and the development of drugs and medical devices. However, because of non-standardized coding practices across our national landscape, laboratory data is easy to transmit but incredibly difficult to curate and analyse. SHIELD <sup>3)</sup> was created to address aspects of this gap.

## 8.7 RCC-MH recommendations – Operations

[Table 13](#) includes the current challenges, desired states and resulting gaps/needs and provides recommendations related to using RCC-MH solutions for operational environments such as clinical trials and collection of real-world evidence.

3) <https://aspe.hhs.gov/shield-standardization-lab-data-enhance-patient-centered-outcomes-research-value-based-care>

**Table 13 — RCC-MH recommendations – Operations**

Challenge	Desired State	Gap/Need	Recommendations
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.	Data provided by sensors/devices include necessary metadata that can be used to support clinical trials.	A Technical Report or Specification be developed which specifies any special data elements required to support VCTs.	Use of open standards-based communication protocols and semantics that support the raw and metadata elements required for clinical trials by sensors/device.
b) Accepting measurement and other data from different devices making the same physiological measurements.	Subjects can use the sensor/device of their choosing since the data can be easily accepted and normalized among various devices.	Certified devices that conform to the same technical interoperability, clinical and cybersecurity standards be treated as interchangeable.	Use of common open standards-based communication protocols and semantics. This allows subjects to choose from multiple conforming sensors/devices.
c) Enabling the reuse of clinical trial data bases for other clinical trials.	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.	Clinical trial data bases should use open standards-based nomenclature and information models. This would enable sharing and reuse of clinical trial data.
19. Surveillance, Real World Evidence (RWE) and other public health functions for medical devices	RCC-MH solutions need to support the need for collection of public health related information while maintaining patient privacy.	Need 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.	Use of open standards-based data bases that share format, nomenclature and information models.
20. Device*/Apps usage logs	Universal support based on open standards.	Use of open standards which support interoperable solutions for usage logs.	Development of open standards which cover interchangeable, interoperable usage logs, potentially as extensions of existing standards.

## 8.8 RCC-MH recommendations – Security

[Table 14](#) includes the current challenges, current states, desired states, and resulting gaps/needs and provides recommendations related to the need to maintain a secure environment to protect the devices and the people.

**Table 14 — RCC-MH recommendations – Security**

Challenge	Desired State	Gap/Need	Recommendations
21. Maintaining a secure end-to-end connection	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 developers and implementers regarding cybersecurity approaches that provide end-to-end security.	Standards should be developed to define the need for and implementation of secure device end-to-end connectivity.
22. Developers of RCC-MH components need clear requirements to protect their products from cybersecurity risks.	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.	Technical specifications with clear conformance assessment requirements for cybersecurity assessments.
23. Developers need guidance on how to achieve effective security.			
a) How to determine how secure to make the device	Devices meet a defined, use-case, and risk-based security baseline and can be assessed and certified against that baseline.	Establish standards to define device baseline security. 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.	Device security standards that define baseline security requirements (technical, procedural, and documentation) based on device type, use case, and risk classification.
b) How to communicate securely	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.	Communication security standards that define security requirements for data in transit (technical, procedural, and documentation) based on device type, use case, and risk classification.
c) How to maintain the security of the device over time.	Devices maintain their security baseline over its useful life.	Establish standards to define security maintenance. This will likely require a breakdown as per device type, use case, and risk.	Standards that define how a device's security posture will be maintained. They should consider requirements from regulations and guidance documents from various jurisdictions such as those listed in <a href="#">Annex G</a> .
d) How to track the security status of the device.	Devices communicate their security status and detected security events using open standards-based protocols.	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.	Standards that define how devices communicate their security status (e.g. version, event detection) within their technical ecosystem over their communication channels.

## 9 Conclusions and path forward

### 9.1 Recommended standards work items

This clause proposes a number of potential work items, based on [Tables 8 to 14](#), that should be considered by various SDOs in accordance with the scope of the SDO. It is possible that some of these work items are already in process or under consideration in which case they are encouraged to continue the effort as quickly as possible.

The following list summarizes the recommendations for new standards work items.

- a) Plug and play interoperability:
  - 1) A roadmap should be developed to attain plug-and-play interoperability. It is unrealistic to test all device combinations when hundreds of different devices exist. (The IEEE 11073 SDC series aims to achieve this goal).
  - 2) Adoption of a small number of open standards will enable RCC-MH applications. In addition, this will also encourage the development of an ecosystem of certifying bodies and regulatory acceptance.
  - 3) Certified devices that conform to the same technical interoperability, clinical and cybersecurity standards should be treated as interchangeable.
  - 4) Technical specifications should be developed with clear conformance assessment requirements to assess conformity of interoperable devices.
- b) Deployment and installation:
  - 1) Standards should address installation, setup and maintenance for users who are not technically savvy.
  - 2) Approaches for deployment of devices in non-traditional settings should be analysed and best practices developed. These should be published in Technical Reports to guide developers.
  - 3) Deployments in non-traditional environments (such as the home) should take into account non-technical users.
  - 4) They also should take into account environments with different challenges than traditional hospital deployments.
  - 5) It should be assessed whether standards are available that address remote provisioning and deployment.
- c) Post-release phase of the device life cycle:
  - 1) Industry wide approach standards-based approach to safe and secure remote software and firmware updates.
  - 2) Software and firmware update solutions that 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) An industry-wide standards-based approach should be developed to acquire sensor/device SW and/or FW and to update connected devices.
  - 4) 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.

- 5) It should be assessed whether appropriate standards are available that address remote technical monitoring, troubleshooting and remediation.
- d) Device error and user logs:
- 1) Standards should be developed to remotely acquire 'logs' from devices as well as standard formats, syntax and semantics.
  - 2) Logs should contain contents in accordance with IEC 80601-1-8 and AAMI 2700-2-1.
  - 3) It is recommended that logs contain contents in accordance with IEC 60601-1-8 and AAMI 2700-2-1.
- e) Open health device data bases:
- 1) Open standards-based clinical trial data bases that share format, nomenclature and information models should be used.
  - 2) Open standards-based data bases that share format, nomenclature and information models should be used.
  - 3) A Technical Report or Specification should be developed which specifies any special data elements required to support virtual clinical trials.
- f) Other:
- 1) Each device should be uniquely identified. The UDI is a good start but the users of UDI should ensure that the application of UDI is secure. IHE should consider a project to assess the use cases, requirements and potential technical solutions for device tracking.
  - 2) Sensor/device communication standards should accommodate location reporting. The IHE DEV PCD MEM Location Services profile is one approach.
  - 3) Reporting of the device location can be accomplished using separate location tags, otherwise the device should support an independent device location sub-system.
  - 4) Establishment of open device registries or searchable keywords to easily discover compliant devices.
  - 5) Establishment of a methodology to recognize certification houses for specific RCC-MH relevant standards.
  - 6) Adjusting regulatory assessment processes so that manufacturers are motivated to take advantage of certified paths for product releases.

Possible work items to consider include:

- requirements/needs assessment for Virtual Clinical Trials data content;
- format and content requirements for health device user and error logs;
- format and content requirements for health device SBOM, HBOM, FBOM;
- mobile health app quality assessment;
- mobile medical device mobile app update 'control' requirements;
- universal electronic device identity scheme;
- provisioning of medical devices; local and remote;
- technical specifications with clear conformance assessment requirements for cybersecurity assessments.

## **9.2 Final thoughts**

This document has reviewed the current standards, regulatory and other landscapes affecting the field of Remote Connected Care and Mobile Health. As a result, a number of gaps were identified which can be filled with appropriate standards, some existing and some yet to be developed.

Standards-based device (including health apps) and data interoperability is an important enabling technology for artificial intelligence and machine learning in order to have trustworthy, safe, structured data with which these algorithms can learn and analyse patient data. It allows open and democratic access to data to support major breakthroughs in healthcare.

Standards are only part of the solution. An ecosystem of trusted conforming devices should be developed. Ideally, certification bodies would be available to improve the level of conformity consistency and ultimately interoperability. Regulatory acceptance of conforming product is extremely important to encourage manufacturers to develop compliant solutions, especially if peer to peer testing is no longer required. Otherwise, the current state of affairs will continue to persist and, during the next pandemic or public health crisis, stakeholders will encounter the same barriers that they encountered during the COVID-19 pandemic.

## **Annex A** **(informative)**

# **Regulatory and legal reactions to the pandemic**

## **A.1 Introduction**

The regulatory approach to dealing with the COVID-19 pandemic varied widely from country to country. For example, in the United States, the FDA issued Emergency Use Authorizations which allowed accelerated use of drugs and devices before full market clearance. This annex summarizes some of those changes and accommodations in light of the public health emergency.

## **A.2 North America**

### **A.2.1 United States**

#### **A.2.1.1 Impact on medical devices**

The following changes to regulations for medical devices and mobile health apps and telehealth occurred as a result of the pandemic.

- CMS: In response to the COVID-19 pandemic, CMS loosened regulations and policies regarding telehealth services and reimbursement (e.g. many of the expanded telehealth services covered due to COVID-19 will be permanently covered after the pandemic). CMS also regulates telehealth policies across states and healthcare related to fees, payments and rules<sup>4)</sup>.
- Telemedicine is viewed as a cost-effective alternative to the more traditional face-to-face way of providing medical care (e.g. face-to-face consultations or examinations between provider and patient) that states can choose to cover under Medicaid<sup>5)</sup>.
- CMS recently launched the “Acute Hospital Care at Home” program. Another example is CMS 165<sup>6)</sup> which allows doctors to include blood pressures taken from home.
- FDA authorized Emergency Use Authorizations (EUAs) for several medical device categories related to the COVID-19 pandemic (e.g. remote monitoring, ventilators, mobile medical apps) in addition to the EUAs for vaccines and other related drugs and treatments.

In 2020, in response to the Covid-19 pandemic, the FDA issued several guidance and policies (EUAs) to enhance remote monitoring care and digital health apps for the safety of patients and clinicians:

- Enforcement Policy for Non-Invasive Remote Monitoring Devices Used to Support Patient Monitoring During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency
- Enforcement Policy for Digital Health Devices for Treating Psychiatric Disorders During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency
- Enforcement Policy for Non-Invasive Fetal and Maternal Monitoring Devices Used to Support Patient Monitoring During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency

---

4) <https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth>

5) <https://www.medicaid.gov/medicaid/benefits/telemedicine/index.html>

6) <https://ecqi.healthit.gov/ecqm/ec/2022/cms165v10>



- Enforcement Policy for Remote Ophthalmic Assessment and Monitoring Devices During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency
- ONC: <https://www.healthit.gov/coronavirus> Interoperability for COVID-19 – ONC’s resource for industry to reference standards and implementation specifications related to COVID-19<sup>7)</sup>

#### **A.2.1.2 Impact on telehealth**

- HHS: Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency<sup>8)</sup>.
- FCC: <https://www.fcc.gov/coronavirus> COVID-19 Telehealth Program. The FCC established a \$200 million COVID-19 Telehealth Program to help health care providers provide connected care services to patients at their homes or mobile locations in response to the COVID-19 pandemic. Congress appropriated the funds as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.
- CDC: Using Telehealth to Expand Access to Essential Health Services during the COVID-19 Pandemic<sup>9)</sup>.
  - Framework for Healthcare Systems Providing Non-COVID-19 Clinical Care During the COVID-19 Pandemic.

### **A.2.2 Canada**

#### **A.2.2.1 Response to the pandemic**

The COVID-19 pandemic has created an unprecedented demand on Canada's health care system and has led to an urgent need for access to health products.

As part of the government's broad response to the COVID-19 pandemic, Health Canada introduced innovative and agile regulatory measures. These measures expedited the regulatory review of COVID-19 health products without compromising safety, efficacy and quality standards.

#### **A.2.2.2 Impact on medical devices**

Medical devices play an important role in diagnosing, treating, mitigating or preventing COVID-19.

Health Canada expedited access to medical devices through an interim order for importing and selling medical devices. A first interim order (IO) was introduced to that effect on March 18, 2020. A second, similar IO was introduced on March 1, 2021. This second IO maintained the flexibility and regulatory oversight of the first IO until at least fall 2021 so that devices could continue to be sold and imported into Canada. Both IOs cover medical devices such as:

- testing devices;
- personal protective equipment (PPE);
- ventilators;
- sterilizers and decontamination devices.

Since the release of the interim order, Health Canada has authorized hundreds of medical devices for use against COVID-19.

They have also expedited the review and issuance of thousands of Medical Device Establishment Licenses (MDELs). These have been issued for companies asking to manufacture (Class I), import or distribute medical devices in relation to COVID-19.

---

7) <https://www.healthit.gov/isa/covid-19>

8) <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html>

9) <https://www.cdc.gov/coronavirus/2019-ncov/hcp/telehealth.html>



Early diagnosis is critical to slowing and reducing the spread of COVID-19. The initial focus during the pandemic has been the scientific review and authorization of testing devices.

Health Canada collaborates with the Public Health Agency of Canada's National Microbiology Laboratory (NML) and with provincial public health and laboratory partners as they:

- review and engage in their own studies of serological technologies;
- develop tests;
- assess commercial tests.

### **A.2.2.3 Impact on telehealth**

Canada implemented several changes to its telehealth regulations to facilitate increased access to healthcare services while minimizing in-person contact. Some of the key changes include the following.

- Expanded coverage and reimbursement: provincial and territorial governments expanded coverage and reimbursement for telehealth services, allowing more healthcare providers to offer virtual care and ensuring patients could access necessary services remotely.
- Relaxed licensing requirements: many provinces and territories temporarily relaxed licensing requirements for healthcare providers, allowing them to deliver telehealth services across provincial or territorial borders without requiring additional licensing.
- Privacy regulations: the federal government and various provinces updated privacy regulations to facilitate the use of telehealth platforms while ensuring patient privacy and confidentiality. This included providing guidance on secure conferencing platforms and encryption standards.
- Increased funding and support: the Canadian government allocated additional funding and resources to support the expansion of telehealth infrastructure and services. This included investments in digital health technologies, such as remote monitoring devices and telemedicine platforms.
- Guidance for healthcare providers: regulatory bodies and professional associations issued guidance and best practices for healthcare providers on delivering telehealth services effectively and safely. This included recommendations for conducting virtual consultations, maintaining patient records securely, and addressing technological challenges.
- Public awareness campaigns: governments and healthcare organizations launched public awareness campaigns to educate Canadians about the availability and benefits of telehealth services. This helped encourage patients to seek virtual care when appropriate and reduce the burden on in-person healthcare facilities.

These changes aimed to improve access to healthcare services during the pandemic while minimizing the risk of COVID-19 transmission. They also laid the groundwork for the continued integration of telehealth into Canada's healthcare system beyond the pandemic, as virtual care remains an important tool for increasing access to healthcare services in remote and underserved communities.

## **A.3 European Union**

### **A.3.1 Impact on medical devices**

In response to the COVID-19 pandemic, the European Union (EU) made several changes to its medical device regulations to address the challenges posed by the crisis. Some of these changes include the following.

- Extension of deadlines: due to the impact of the COVID-19 pandemic, the date of application of Medical Device Regulation 2017/745 was postponed by one year to 26 May 2021. Also due to the shortage of medical device inspection capacity, many devices which had an inspection certificate that was issued in accordance with Medical Device Directive 90/385/EEC or Directive 93/42/EEC could continue to be placed on the market until 2027 (Class III devices) or until 2028 (class I and II devices). Similar extensions were introduced to the corresponding deadlines regarding in vitro diagnostic medical devices, too.

The deadlines for the compulsory inclusion of UDI (unique device identification) on the devices were extended, as well.

- Fast-track approval procedures: the EU introduced expedited approval procedures for certain medical devices essential for the diagnosis, treatment, and prevention of COVID-19. These fast-track procedures allowed for quicker market access for critical medical devices needed to address the pandemic.
- Temporary relaxation of regulatory requirements: temporary relaxation of certain regulatory requirements was implemented to facilitate the availability of medical devices during the COVID-19 pandemic. This included flexible approaches to conformity assessments and product registrations to ensure timely access to essential medical equipment.
- Facilitation of cross-border cooperation: the EU encouraged cross-border cooperation and coordination among member states to ensure the efficient exchange of medical devices and supplies. This involved streamlining regulatory processes and facilitating the mutual recognition of certifications to expedite the movement of medical devices across EU borders.
- Enhanced surveillance and monitoring: the EU implemented enhanced surveillance and monitoring mechanisms to track the safety and performance of medical devices used in the context of COVID-19. This included increased scrutiny of products entering the market and enhanced post-market surveillance to identify and address any safety concerns promptly.
- Promotion of innovation: the EU promoted innovation in the development of medical devices to address the challenges posed by the pandemic. This involved supporting research and development efforts, facilitating collaboration between industry stakeholders, and providing funding for innovative solutions.

These changes to the EU's medical device regulations aimed to ensure the availability of safe and effective medical devices to address the healthcare needs arising from the COVID-19 pandemic while maintaining appropriate regulatory oversight and patient safety standards.

### **A.3.2 Impact on telehealth**

The European Union (EU) and its member states made several changes to telehealth regulations in response to the COVID-19 pandemic to facilitate access to healthcare services while minimizing physical contact. Some of these changes include the following.

- Temporary relaxation of regulatory requirements: in response to the COVID-19 pandemic, the EU temporarily relaxed certain regulatory requirements related to telehealth services. This included easing restrictions on remote consultations and prescribing medication via telehealth platforms to ensure patients could access care without visiting healthcare facilities in person.
- Expansion of reimbursement policies: many EU member states expanded reimbursement policies for telehealth services during the pandemic. This allowed healthcare providers to be compensated for virtual consultations and remote monitoring services, encouraging the adoption of telehealth technologies.
- Cross-border telehealth services: the EU introduced measures to facilitate the provision of cross-border telehealth services during the pandemic. This included clarifying regulatory requirements for healthcare providers offering telehealth services across EU borders and promoting interoperability of telehealth systems to enable seamless provision of care.
- Telehealth guidelines: the European Commission issued guidelines and recommendations to support the implementation of telehealth services across the EU during the pandemic. These guidelines addressed various aspects of telehealth, including privacy and data protection, interoperability, and quality standards for remote healthcare delivery.
- Investment in telehealth infrastructure: the EU and member states invested in telehealth infrastructure and digital health technologies to support the expansion of telehealth services during the pandemic. This included funding for the development and deployment of telehealth platforms, remote monitoring devices, and other digital health solutions.

These changes aimed to promote the use of telehealth as a safe and effective means of delivering healthcare services during the COVID-19 pandemic, while also laying the groundwork for the long-term integration of telehealth into Europe's healthcare systems.

## **A.4 Asia**

### **A.4.1 South Korea**

#### **A.4.1.1 Impact on medical devices**

In response to the COVID-19 pandemic, South Korea made several changes to its medical device regulations and clearance processes to expedite access to essential medical equipment and supplies. Some of the key changes include the following.

- **Emergency Use Authorization (EUA):** the South Korean Ministry of Food and Drug Safety (MFDS) introduced provisions for emergency use authorization, allowing certain medical devices to be used in emergency situations even before they receive full regulatory approval. This helped expedite the availability of critical medical equipment necessary for COVID-19 diagnosis, treatment, and prevention.
- **Expedited review process:** the MFDS implemented an expedited review process for medical devices related to COVID-19, prioritizing the review and approval of these products to ensure timely access to essential healthcare resources.
- **Relaxed regulatory requirements:** in some cases, the MFDS temporarily relaxed certain regulatory requirements for medical devices, such as documentation and testing requirements, to streamline the approval process without compromising safety and efficacy standards. This flexibility allowed manufacturers to bring their products to market more quickly during the pandemic.
- **Collaboration with international agencies:** South Korea collaborated with international regulatory agencies and organizations to exchange information and leverage global expertise in assessing and approving medical devices for COVID-19. This cooperation facilitated the adoption of best practices and expedited regulatory processes.
- **Digital health technologies:** South Korea promoted the use of digital health technologies, including telehealth and remote monitoring devices, to support the delivery of healthcare services while minimizing the risk of virus transmission. The government provided guidance and support for the development and deployment of these technologies to enhance access to medical care during the COVID-19 pandemic.

These changes in medical device regulations and clearance processes in South Korea were aimed at ensuring the rapid availability of essential medical equipment and supplies to combat the COVID-19 pandemic effectively. They enabled the country to respond swiftly to emerging healthcare needs and mitigate the impact of the pandemic on public health.

#### **A.4.1.2 Impact on telehealth**

South Korea implemented changes to facilitate access to telehealth services in response to the COVID-19 pandemic. These changes were aimed at ensuring the continuity of healthcare services while minimizing the risk of virus transmission. Some of the measures taken to enhance access to telehealth services include the following.

- **Expansion of telemedicine regulations:** the South Korean government and relevant regulatory authorities expanded regulations governing telemedicine to enable a wider range of healthcare services to be provided remotely. This included allowing healthcare providers to conduct consultations, diagnoses, and follow-ups via telehealth platforms.
- **Temporary relaxation of telemedicine restrictions:** during the pandemic, South Korea temporarily relaxed certain restrictions on telemedicine, such as allowing healthcare providers to offer telehealth services to new patients without a prior in-person consultation. This flexibility aimed to facilitate greater access to healthcare services while minimizing the need for face-to-face interactions.

- Promotion of telehealth platforms: the government promoted the use of telehealth platforms and digital health technologies by providing guidance and support for their development and adoption. This included initiatives to enhance the usability and accessibility of telehealth services for both healthcare providers and patients.
- Reimbursement policies: South Korea adjusted reimbursement policies to cover telehealth consultations and services, making them more accessible and affordable for patients. This change aimed to encourage the use of telemedicine as a viable alternative to in-person healthcare visits during the pandemic.
- Public awareness and education: the government conducted public awareness campaigns to educate the population about the availability and benefits of telehealth services. These efforts aimed to increase awareness and acceptance of telemedicine as a safe and convenient option for accessing healthcare while reducing the risk of virus transmission.

These changes in telehealth regulations and policies in South Korea were designed to support the widespread adoption of telemedicine as a means of delivering healthcare services during the COVID-19 pandemic. They aimed to ensure that patients could continue to receive necessary medical care while adhering to social distancing and infection control measures.

## **A.4.2 Japan**

### **A.4.2.1 Impact on medical devices**

In response to the COVID-19 pandemic, Japan made several changes to medical device regulations and clearance processes to expedite the approval and availability of essential medical devices. Some of the key changes include:

- Fast-track approval process: Japan's Pharmaceuticals and Medical Devices Agency (PMDA) implemented expedited review processes for medical devices related to COVID-19 diagnosis, treatment, and prevention. This allowed manufacturers to obtain approval more quickly than the standard regulatory timeline.
- Emergency Use Authorization (EUA): the PMDA introduced provisions for emergency use authorization, enabling certain medical devices to be used in emergency situations even before they received full regulatory approval. This facilitated the rapid deployment of critical medical equipment to combat the COVID-19 pandemic.
- Relaxed regulatory requirements: the PMDA temporarily relaxed certain regulatory requirements for medical devices, such as documentation and testing requirements, to accelerate the approval process while ensuring safety and efficacy standards were maintained.
- Collaboration with international agencies: Japan collaborated with international regulatory agencies and recognized certifications from other countries to expedite the approval process for medical devices that had already been cleared by reputable foreign regulatory authorities.
- Increased transparency and communication: the PMDA increased transparency and communication with medical device manufacturers to provide guidance and support throughout the regulatory approval process, facilitating the timely clearance of essential medical devices.

These regulatory changes aimed to ensure the availability of critical medical devices needed to diagnose, treat, and prevent COVID-19 infections while maintaining high standards of safety and efficacy. By streamlining the approval process and facilitating collaboration, Japan sought to address the challenges posed by the pandemic and ensure timely access to lifesaving medical equipment.

### **A.4.2.2 Impact on telehealth**

Japan made changes to access and regulations affecting telehealth services in response to the COVID-19 pandemic. Some of the key changes include the following.

- Expansion of telehealth coverage: the Japanese government expanded coverage for telehealth services under the national health insurance program. This allowed more people to access medical consultations

remotely, reducing the need for in-person visits to healthcare facilities and minimizing the risk of COVID-19 transmission.

- Relaxation of regulatory restrictions: regulatory restrictions on telehealth services were temporarily relaxed to facilitate broader access during the pandemic. This included easing requirements for telehealth providers and allowing healthcare professionals to deliver remote care across regional borders.
- Promotion of remote consultations: the government actively promoted the use of telehealth services through public awareness campaigns and incentives for healthcare providers to adopt telemedicine platforms. This helped encourage both patients and healthcare professionals to utilize remote consultation options.
- Implementation of remote prescription systems: Japan implemented systems to enable remote prescribing of medications during telehealth consultations. This facilitated the provision of necessary medications to patients without requiring them to visit a physical clinic or pharmacy.
- Support for telehealth infrastructure: the Japanese government provided support for the development and enhancement of telehealth infrastructure, including funding for the adoption of telemedicine technology and training programs for healthcare professionals.

These changes aimed to improve access to healthcare services while minimizing the risk of COVID-19 transmission, especially for vulnerable populations and those in remote areas. They also laid the groundwork for the long-term integration of telehealth into Japan's healthcare system.

### **A.4.3 India**

#### **A.4.3.1 Impact on medical devices**

India made changes to regulations concerning clearance rules for medical devices due to the COVID-19 pandemic. Some of the key regulatory changes include:

- Fast-track approval process: the Indian government introduced expedited approval processes for medical devices, particularly those essential for COVID-19 diagnosis, treatment, and prevention. This was aimed at speeding up the clearance of medical devices to ensure timely availability during the pandemic.
- Relaxation of import regulations: import regulations for medical devices were relaxed to facilitate the importation of essential medical equipment and supplies needed to combat COVID-19. This included streamlining customs procedures and reducing bureaucratic hurdles to expedite the import process.
- Emergency use authorization: India's regulatory authorities, such as the Central Drugs Standard Control Organization (CDSCO), issued guidelines for emergency use authorization of medical devices, allowing certain products to be approved for use in emergencies without undergoing the usual regulatory processes. This enabled quicker access to critical medical devices during the pandemic.
- Regulatory flexibility: in response to the urgent need for medical devices, regulatory agencies in India demonstrated flexibility in regulatory requirements, allowing for accelerated approval of devices while maintaining safety and efficacy standards.
- Encouragement of local manufacturing: the Indian government promoted domestic manufacturing of medical devices to reduce reliance on imports and ensure a stable supply of essential equipment during the pandemic. This included incentives and support for local manufacturers to ramp up production of medical devices needed to address COVID-19 challenges.

These regulatory changes aimed to address the urgent healthcare needs arising from the COVID-19 pandemic by ensuring the availability of essential medical devices while maintaining appropriate safety and quality standards.



#### **A.4.3.2 Impact on telehealth**

These changes were aimed at expanding access to healthcare services while minimizing physical contact to reduce the spread of the virus. Some of the key measures include the following.

- Telemedicine practice guidelines: in March 2020, the Ministry of Health and Family Welfare issued Telemedicine Practice Guidelines, allowing registered medical practitioners to provide healthcare consultations remotely through telemedicine platforms. These guidelines outlined the standards and protocols for teleconsultations, prescription of medications, and maintaining patient confidentiality.
- Expansion of telemedicine services: the Telemedicine Practice Guidelines enabled healthcare providers to offer a wide range of services remotely, including consultations for non-emergency medical issues, follow-up visits, mental health counselling, and chronic disease management.
- Relaxation of licensing requirements: to facilitate the provision of telehealth services across state boundaries, certain licensing requirements for healthcare practitioners were temporarily relaxed, allowing them to provide teleconsultations to patients residing in different states without the need for additional state licenses.
- Insurance coverage: some insurance providers expanded coverage for telemedicine consultations, making it more accessible and affordable for patients to seek medical advice remotely.
- Promotion of telemedicine platforms: the government encouraged the use of telemedicine platforms by healthcare providers and patients through awareness campaigns and collaborations with telehealth service providers.

These changes aimed to leverage telemedicine technology to overcome barriers to healthcare access, especially during periods of lockdown and social distancing measures imposed to curb the spread of COVID-19. The adoption of telehealth services has not only facilitated remote consultations but also contributed to reducing the burden on healthcare facilities and minimizing the risk of virus transmission among patients and healthcare workers.

#### **A.4.4 Saudi Arabia**

##### **A.4.4.1 Impact on medical devices**

Some of the regulatory changes include the following.

- Expedited approval process: the Saudi Food and Drug Authority (SFDA) expedited the approval process for medical devices related to COVID-19 diagnosis, treatment, and prevention. This allowed manufacturers to obtain clearance for their products more quickly, ensuring timely access to critical medical equipment.
- Emergency Use Authorization (EUA): the SFDA introduced provisions for emergency use authorization, allowing certain medical devices to be used in emergency situations even before they receive full regulatory approval. This helped expedite the availability of essential medical equipment during the pandemic.
- Relaxed regulatory requirements: the SFDA temporarily relaxed certain regulatory requirements for medical devices, such as documentation and testing requirements, to streamline the approval process without compromising safety and efficacy standards.

These changes aimed to facilitate the availability of essential medical devices and supplies needed to combat the COVID-19 pandemic effectively. However, it is essential to note that specific regulatory changes and their impact can vary based on the evolving situation and regulatory decisions made by the Saudi authorities.

#### **A.4.4.2 Impact on telehealth**

Saudi Arabia implemented changes to facilitate access to telehealth services in response to the COVID-19 pandemic. These changes aimed to ensure continuity of healthcare services while minimizing the risk of virus transmission. Some of the measures taken to enhance access to telehealth services include:

- Expansion of telemedicine regulations: the Saudi Ministry of Health (MoH) and other regulatory authorities expanded regulations governing telemedicine to accommodate a wider range of healthcare services delivered remotely. This included allowing healthcare providers to offer consultations, diagnoses, and prescriptions via telehealth platforms.
- Licensing and credentialing: the authorities streamlined the licensing and credentialing process for healthcare professionals providing telehealth services to enable them to quickly adapt to remote care delivery.
- Reimbursement policies: the government and health insurance providers adjusted reimbursement policies to cover telehealth consultations and services, making them more accessible and affordable for patients.
- Telehealth infrastructure: investments were made to enhance telecommunication infrastructure and digital health platforms to support the increased demand for telehealth services during the pandemic.
- Public awareness and education: the government and healthcare authorities conducted public awareness campaigns to educate the population about the availability and benefits of telehealth services, encouraging their use for non-emergency medical consultations and follow-ups.

These changes aimed to promote the widespread adoption of telehealth services as a safe and convenient alternative to in-person healthcare visits during the COVID-19 pandemic. By leveraging telemedicine, Saudi Arabia sought to ensure that patients could continue to receive timely medical care while minimizing the risk of virus transmission.

### **A.5 Oceania**

#### **A.5.1 Australia**

##### **A.5.1.1 Impact on medical devices**

Australia implemented several changes to its medical device regulations to address the urgent healthcare needs and ensure the availability of essential medical devices. Some of these changes include the following.

- Expedited approval processes: the Therapeutic Goods Administration (TGA), Australia's regulatory authority for therapeutic goods including medical devices, introduced expedited approval processes for certain medical devices essential for COVID-19 diagnosis, treatment, and prevention. These processes aimed to streamline regulatory review and clearance to facilitate timely access to critical medical devices.
- Relaxed regulatory requirements: the TGA temporarily relaxed certain regulatory requirements for the approval and supply of medical devices, particularly those related to COVID-19 response. This included flexibility in documentation requirements and expedited review timelines to accelerate the approval process while maintaining appropriate safety and quality standards.
- Emergency use authorization: similar to other regulatory agencies worldwide, the TGA issued guidance on emergency use authorization for medical devices, allowing certain products to be approved for use in emergencies without undergoing the full regulatory process. This enabled quicker access to essential medical devices during the pandemic while ensuring necessary safety measures were in place.
- Remote assessments: to facilitate regulatory processes while adhering to social distancing measures, the TGA implemented remote assessment procedures for medical device applications. This allowed for the continuation of regulatory activities despite restrictions on in-person interactions.

- Priority review pathways: the TGA established priority review pathways for medical devices related to COVID-19, prioritizing the assessment of these products to expedite their availability in the market.
- Monitoring and reporting: the TGA enhanced monitoring and reporting mechanisms for medical devices, particularly those used in the context of COVID-19, to ensure ongoing safety and efficacy surveillance.

These regulatory changes were implemented to address the unprecedented challenges posed by the COVID-19 pandemic and ensure that healthcare providers and patients had timely access to essential medical devices while maintaining appropriate regulatory oversight and standards.

#### **A.5.1.2 Impact on telehealth**

##### **A.5.1.2.1 General**

The Australian Health Practitioner Regulation Agency (AHPRA) works with 15 national boards to register and accredit health professionals. AHPRA provides guidance on telehealth services for practitioners. The Medical Board of Australia also provides guidance on telehealth consultations with patients. The Australian Medical Council develops standards for medical education and training at medical school, intern and specialist medical training stages and programs for endorsement of medical registration

Telehealth services are largely funded by the federal government and the eight state or territory governments that operate public hospitals. Australia has a mixed public and private health system, where patients admitted to a public facility are not charged for health services. However, patients consulting with a private health provider (general practitioner, medical or nursing specialist, allied health professional, pathologist or radiologist) can be asked to pay a portion of the fee which is set by each practitioner. Holders of private health insurance can also in some circumstances, be able to claim a subsidy for telehealth services from their insurer.

As of 2023 more than 40 organizations have developed their own guidelines for telehealth services. Guidelines concentrate on four areas perceived as barriers to practice medicine when care is physically separated. These are:

- a) privacy, confidentiality, and patient consent processes;
- b) defining responsibility for patients and relationships with patients;
- c) processes to minimize liability and risk;
- d) managing quality and risk.

Guidelines are available for the following specialties, services or professions: allied health, audiology, cancer, cardiology, dentistry, dermatology, diabetes, exercise physiology, gastroenterology, general practice, geriatric care, mental health, nutrition and dietetics, occupational therapy, optometry, pain management, palliative care, pharmacy, pathology, physiotherapy, podiatry, rehabilitation, social work, speech pathology and stroke.

Initially, in Australia, telehealth services provided for professional development followed by administrative meetings and clinical use. Subsequently, educational use has proportionately declined while clinical use has greatly increased. Until the COVID-19 pandemic, Australian clinical services focused on consultations between hospital-based specialists and patients in regional areas and emergency presentations. Telephone-based advice lines servicing the public directly are not usually considered telehealth services. Asynchronous text or web-based services for regional populations have been slow to develop.

With the advent of the pandemic, key regulatory changes to the Medicare Benefits Scheme (MBS) payment regulations legitimized and resourced the use of telehealth across a much greater range of healthcare activities than was previously permissible. Subsequently, there were huge increases in the volume of telephone and, to a lesser extent, video-based consultations between doctors and patients for services funded by the MBS. As of April 2023, on a quarterly-basis, remote consultations comprised 18 % of 35 million



consultations, 9,7 % of 6,8 million specialist consultations, 21 % of 2,6 million mental health consultations, 28,4 % of 1 million allied health consultations.<sup>10)</sup>

#### **A.5.1.2.2 Devices and software regulation**

General-purpose technology and software used to deliver telehealth services include computers, mobile devices, computer software, communications devices and applications. These are not subject to regulations and guidelines from the health sector but are subject to national or international regulations, standards and codes. An example would be the need for devices and software to protect users from cyber-attacks. In this example, national codes for cyber security defence (Australian Digital Health Agency, 2020) or international standards would apply. Additionally, manufacturers and suppliers should comply with standards and legislation for manufacturing in areas such as quality control or electrical safety.

Devices used by telehealth services can require approval by the Therapeutic Goods Administration (TGA), part of the Australian Government's Department of Health and Aged Care. The TGA is responsible for evaluating, assessing and monitoring therapeutic goods including medical devices incorporating a software element. The Therapeutic Goods Act 1989 outlines the legal requirements for the import, export, manufacture, and supply of therapeutic goods in Australia. The TGA has a rigorous approval process designed to ensure that only safe, effective, and high-quality therapeutic products supplied in Australia. It also monitors the performance of products once they are in use to ensure they continue to meet regulatory requirements.

Medical devices that include a software element are rated by the TGA in a four-tier classification system based on the risk posed to patients and users. Class I devices are considered low risk, Class IIa and IIb are medium risk, while Class III are high risk. The higher the risk, the greater the regulatory oversight to ensure safety and efficacy. The evaluation process typically involves pre-market assessment of clinical data and risk management documents followed by post-market monitoring. The TGA can take regulatory action if a product is found to pose a risk to the patient or user.

The TGA works with the International Medical Device Regulators Forum (IMDRF) to harmonize regulatory requirements for medical products internationally. The IMDRF promotes the use of relevant standards such as IEC 80001-1, ISO 31000 and the ISO/IEC 27000 series. IEC 80001-1 provides guidance on the use of medical devices in a networked environment, which by definition contain a software element for communications and can also use software for the measurement of medical parameters. The IMDRF defines software as a medical device as "software intended to be used for one or more medical purposes and that performs these purposes without being part of a hardware medical device". It encompasses clinical software to facilitate diagnosis, mitigation, treatment, and prevention of disease. Examples include remote surgery for medical providers or implantable interface software for patients.

The TGA has excluded many software products from being medical devices (e.g. self-assessment apps), exempted others (e.g. general-purpose computing and communications software and clinical decision support software), and provided examples of regulated and unregulated software on its website.

Self-assessment apps are an example of a class of software exempted from assessment by the TGA. There is a wider group of applications, commonly but not exclusively intended for use on mobile devices (smartphones etc) by healthcare providers, patients and consumers, often referred to as mHealth apps. The Australian Digital health Agency has published an Assessment Framework for mHealth apps. This framework provides

The framework is voluntary and assurance-focused rather than regulatory. Instead, apps can be nominated for assessment under the framework. The TGA can assess mHealth apps as a Software-Based Medical Device. The framework does not assess hardware, sensors or apps that provide a read-only view of a medical record such as the Australian My Health Record, or apps used to administer processes used within health facilities such as patient flow dashboards.

---

10) Medicare Benefits Schedule (MBS) activity in Australia. (2020, June 22), Centre for Online Health, University of Queensland. <https://coh.centre.uq.edu.au/telehealth-and-coronavirus-medicare-benefits-schedule-mbs-activity-australia>

## **A.6 South America**

### **A.6.1 Brazil**

#### **A.6.1.1 Impact on medical devices**

One notable change was the implementation of expedited processes for the registration and approval of medical devices related to COVID-19 diagnosis, treatment, and prevention.

Specifically, Brazil's regulatory agency for health surveillance, ANVISA (Agência Nacional de Vigilância Sanitária), introduced streamlined pathways for the registration and authorization of medical devices necessary for the pandemic response. These changes aimed to facilitate timely access to essential medical devices while maintaining safety and efficacy standards.

ANVISA implemented measures such as the following.

- Fast-track approval process: ANVISA established accelerated review processes for COVID-19 related medical devices, allowing for quicker clearance compared to standard regulatory pathways.
- Emergency Use Authorization (EUA): ANVISA introduced emergency use authorization mechanisms for certain medical devices, allowing them to be used in Brazil for COVID-19 response purposes without undergoing the full registration process.
- Flexible requirements: the regulatory requirements for documentation and clinical evidence were adjusted to expedite the approval of medical devices needed to address the pandemic.

These regulatory changes were part of Brazil's broader efforts to enhance its healthcare response to the COVID-19 crisis and ensure that necessary medical devices could reach healthcare providers and patients in a timely manner.

#### **A.6.1.2 Impact on telehealth**

The pandemic highlighted the importance of telehealth services in providing remote medical care, reducing the risk of virus transmission, and ensuring continued access to healthcare services for patients. To facilitate the expansion of telehealth during the pandemic, Brazil implemented the following regulatory changes.

- Expansion of telemedicine services: Brazil's Federal Council of Medicine (Conselho Federal de Medicina, CFM) issued Resolution 2222/2021, which temporarily expanded the scope of telemedicine services allowed by physicians during the pandemic. This resolution permitted the remote provision of medical care, including consultations, prescriptions, and follow-up appointments, through telehealth platforms.
- Relaxation of telemedicine regulations: the CFM relaxed certain regulatory requirements for telemedicine consultations, such as allowing remote prescribing of medications based on teleconsultations. This facilitated access to healthcare services while minimizing the need for in-person visits to healthcare facilities.
- Interoperability standards: Brazil also worked on establishing interoperability standards and guidelines for telehealth platforms to ensure the secure and efficient exchange of health information between healthcare providers and patients.
- Reimbursement policies: the Brazilian government and health insurers adjusted reimbursement policies to cover telehealth consultations, enabling healthcare providers to receive payment for remote services provided to patients.
- Public awareness and education: efforts were made to raise public awareness about the availability and benefits of telehealth services, encouraging patients to utilize remote consultations when appropriate.

These regulatory changes aimed to promote the use of telehealth as a safe and effective means of delivering healthcare services during the COVID-19 pandemic, while also laying the groundwork for its continued integration into the healthcare system beyond the crisis.

## **A.7 Africa**

### **A.7.1 General**

In Africa, at the continental level, the African Union Commission through its Center for Disease Control developed a continent-wide strategy with the two overarching goals of

- a) preventing severe illness and death from COVID-19 infection in member states, and
- b) minimizing social disruption and economic consequences of COVID-19 outbreaks.

Such actions envisage that the Africa CDC

- coordinates the efforts of Member States, African Union agencies, World Health Organization, and other partners to ensure synergy and minimize duplication, and
- promote evidence-based public health practice for surveillance, prevention, diagnosis, treatment, and control of COVID-19.<sup>11)</sup>

### **A.7.2 Impact on medical devices**

While this guidance did not specifically call out RCC or medical device regulation, several African countries modified their medical device regulations in response to the COVID-19 pandemic. The modifications aimed to expedite the approval and importation of medical devices, including diagnostic tests, ventilators, and personal protective equipment (PPE), to enhance their capacity to respond to the pandemic. These changes often involved streamlining regulatory processes, relaxing certain requirements, and implementing fast-track approval mechanisms to ensure timely access to essential medical devices. However, specific modifications varied from country to country, reflecting the diverse regulatory landscapes across the African continent.

### **A.7.3 Impact on telehealth**

Many African countries also modified regulations regarding telehealth in response to the COVID-19 pandemic. These modifications aimed to facilitate remote access to healthcare services while minimizing in-person contact to reduce the spread of the virus. Some common regulatory changes included the following.

- a) Expansion of telehealth services: many countries expanded the scope of telehealth services allowed, permitting healthcare providers to deliver a broader range of medical services remotely.
- b) Licensing and credentialing: some countries relaxed licensing and credentialing requirements for healthcare professionals providing telehealth services, allowing for easier and faster deployment of telemedicine platforms.
- c) Reimbursement policies: changes were made to reimbursement policies to ensure that telehealth consultations were covered by insurance and reimbursed at rates comparable to in-person visits.
- d) Data privacy and security: regulations were updated to address data privacy and security concerns related to telehealth platforms, ensuring that patient information was adequately protected during remote consultations.
- e) Cross-border telemedicine: some countries facilitated cross-border telemedicine services by temporarily waiving restrictions or implementing mutual recognition agreements for healthcare providers licensed in other jurisdictions.

These modifications aimed to promote the use of telehealth as a safe and effective means of delivering healthcare services during the pandemic while adhering to regulatory standards and protecting patient safety and privacy.

---

11) White Paper, "Covid-19 & Other Epidemics", AUDA-NEPAD, <https://nepad-aws.assyst-uc.com/publication/auda-nepad-response-covid-19-other-epidemics>

## **Annex B** **(informative)**

### **RCC-MH interoperability challenges**

#### **B.1 RCC-MH interoperability challenges**

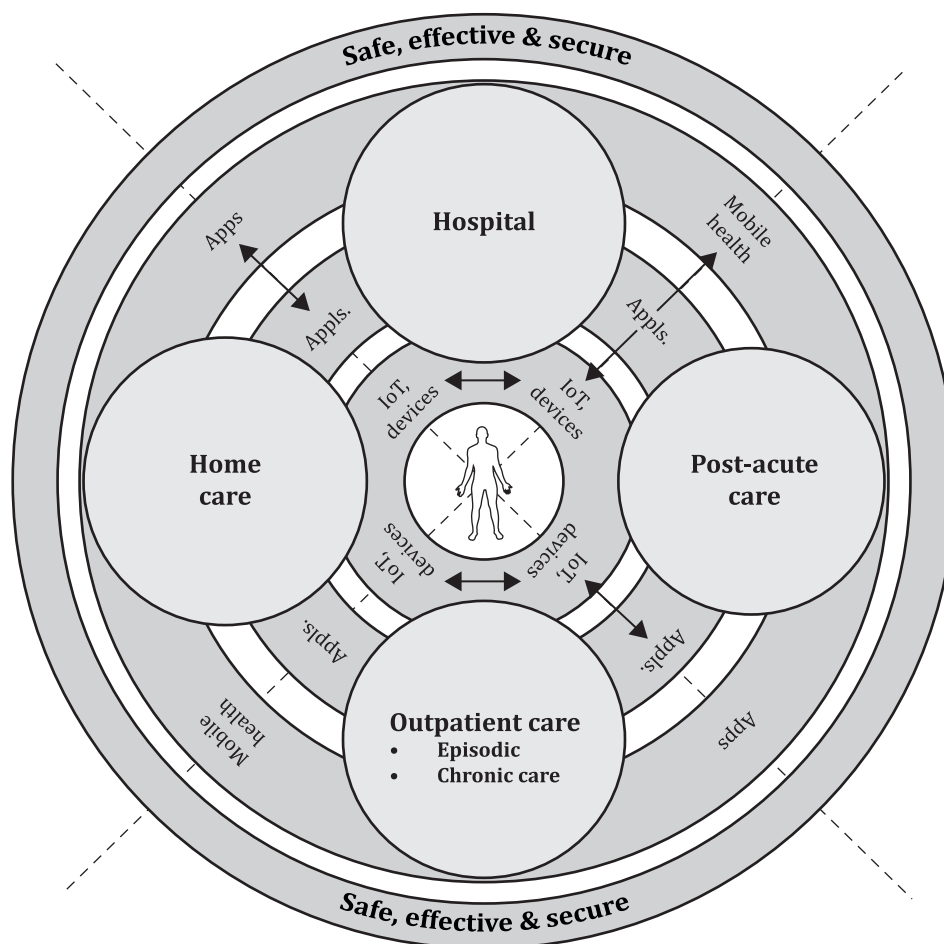
By its very nature, RCC-MH relies on communications between patients, caregivers, clinical specialists and related devices and IT systems. [Annex A](#) looks at these various paths and makes the case for mature, open standards-based interoperability.

#### **B.2 Interoperability paths**

When analysing the various interoperability paths, there are 4 main paths:

- Device to/from device – this refers to the ability of devices to communicate with each other either in peer to peer or controller/agent architectures.
- Device to/from enterprise/cloud applications – typically communication of patient measurements and related metadata from devices to IT applications (such as EHRs, EMRs, etc.), as well as settings and other information from these applications back to the devices.
- Device to/from apps – typically communication of patient measurements and related metadata from devices to mobile health apps, as well as settings and other information from these apps back to the devices.
- Apps to/from applications – Mobile health apps can be intermediaries between the devices and the end applications. In addition, apps can add additional information to the device data stream such as patient demographics, location and patient entered data. Mobile health apps can also be used as portals to the health IT applications as well as end-points for certain applications such as distributed alerting systems.

[Figure B.1](#) illustrates these various paths denoted by the double arrows.



**Figure B.1 — RCC-MH data flows**

### B.3 Degrees of interoperability

Interoperability is generally defined as the ability of two or more systems to exchange information and use that information. This is the very minimum level of interoperability and not adequate for RCC-MH in the long term since it does not address the many issues currently faced in an era of proprietary interoperability solutions. (This is discussed in more detail in [Clause B.4](#)).

There are numerous interoperability models such as the model proposed by Tolk<sup>12)</sup> which has 7 levels, the model proposed by ISO 23903 which has 8 levels and is also 3 dimensional and the simpler model proposed by HIMSS which has only 4 levels<sup>13)</sup>. The HIMSS maturity model is a good starting point, proposing the following four levels:

- Foundational (Level 1): it establishes the inter-connectivity requirements needed for one system or application to securely communicate data to and receive data from another.
- Structural (Level 2): it defines the format, syntax and organization of data exchange including at the data field level for interpretation.
- Semantic (Level 3): it provides for common underlying models and codification of the data including the use of data elements with standardized definitions from publicly available value sets and coding vocabularies, providing shared understanding and meaning to the user.

12) <https://www.mscoe.org/content/uploads/2017/12/Tolk-Muguira-The-Levels-of-Conceptual-Interoperability-Models.pdf>

13) <https://www.himss.org/resources/interoperability-healthcare>

- Organizational (Level 4): it includes governance, policy, social, legal and organizational considerations to facilitate the secure, seamless and timely communication and use of data both within and between organizations, entities and individuals. These components enable shared consent, trust and integrated end-user processes and workflows.

HIMSS tends to view things from an institutional/enterprise point of view and not at the device level, but this model can be applied to devices, apps and applications. Generally, the goal is to achieve seamless, open-standards based, plug-and-play interoperability.

The reality today is that while many systems achieve the basic definition of interoperability, each implementation requires considerable development effort to achieve and to maintain. There is general interoperability at the physical (foundational) level such that standards such as ethernet, Wi-Fi, bluetooth, etc. are used allowing us to achieve connectivity but the structural, semantic and organizational mechanisms are for the most part proprietary, blocking the way to seamless interoperability.

## **B.4 Why standards-based interoperability?**

Much of this document deals with exchanging data with devices [including Software as a Medical Device (SaMD)]. The question arises as to whether this can be done using open standards-based protocols or to continue with the current generally accepted approach of data consumers such as EHRs, clinical decision support systems, AI based applications, etc. being responsible for conversion of proprietary protocols for their own needs. This is typically done through the use of protocol converters, gateways and integration engines.

It is recognized that the use of proprietary protocols is not as popular as it once was when talking about gateways from devices to EHRs or other IT applications. In these cases, it is relatively easy to find solutions that use IHE profiles (see [F.4.3.1](#)) to communicate results. However, the adoption of open standards-based approaches has been very limited in the other interoperability paths.

For example, even though solutions have been available such as IEEE 11073 Point-of-Care Device (PoCD) or IEEE 11073 Personal Health Device (PHD) protocols (see [F.4.2.1.4](#)), there has been very minimal uptake of these standards. At the same time, there are many reasons to adopt standards-based interoperability solutions, many of which could fulfil the gaps that have been previously identified. These solutions include:

- quick integration with EHRs and other IT systems even if using an integration gateway;
- opening the possibility for device-to-device communication;
- opening the possibility for certification of interoperable interfaces;
- considerable reduction in the overhead and cost of testing device interfaces;
- support for remote control of devices;
- remote maintenance of devices using common tools.

[Tables 1](#) to [7](#) also provides many gaps that could be addressed by using open interoperability standards especially if an ecosystem for open-source software, testing, certification and regulatory acceptance develops around those standards.



## **Annex C** **(informative)**

### **Nomenclature standards landscape for medical devices**

#### **C.1 General**

Semantic interoperability plays a critical role when exchanging medical device data and enabling systems to correctly interpret and use the information in a safe and effective manner. In deployments where devices and systems from multiple vendors are used, publicly available standard nomenclatures such as IEEE 11073, LOINC and SNOMED are essential.

#### **C.2 IEEE 11073 series**

##### **C.2.1 IEEE 11073-10101**

The nomenclature defined in IEEE 11073 is well-suited for medical device data exchange. Originally published in 2004, the IEEE 11073-10101 nomenclature focused on devices typically used in acute care settings such as the ICU, CCU, OR, ER and other areas in the hospital. Patient monitors, infusion pumps, ventilators and other PoCD devices served as the target for this early ambitious effort that laid the foundations for device data models and nomenclature that could support simple single-parameter devices (such as a thermometer) to complex multi-parameter monitors. This scalability provided the foundation for later work in the personal health devices (PHD) used in home health and telemedicine environments, such as weighing scales, non-invasive blood pressure meters, glucose meters and other devices.

The collaboration between the IEEE 11073 acute care and PHD domains ensures that the underlying IEEE 11073-10101 nomenclature supports a broad range of devices and sophistication and ensures the availability of advanced terminology that home and personal health care devices can use in the future.

**NOTE 1** The recent revision of ISO/IEEE 11073-10101-2020 covers both the acute care and roughly twenty PHD specializations. The nomenclature standard was extended by the IEEE 11073-10101b amendment published in 2023. Two additional nomenclatures, ISO/IEEE 11073-10102:2014 Annotated ECG (aECG) and ISO/IEEE 11073-10103:2023 Implanted Devices Cardiac (IDC) extend the base ISO/IEEE 11073-10101 nomenclature to support advanced diagnostic ECG and implanted cardiac devices.

Although the IEEE 11073-10101 nomenclature supports many of the blood gas and other analytes that traditionally can be measured by POCT devices, the COVID-19 pandemic emphasizes the continued need for standardized vocabularies for lab devices that can be used in central labs, hospitals, clinics and at home. To facilitate this, the IEEE 11073 Standards Committee has enjoyed a close collaboration with LOINC, including mapping of the more widely used 800+ IEEE 11073 terms to LOINC as well as supporting the use of LOINC for POCT devices. This collaboration is enabled by enterprise-capable communication protocols such as HL7 V2, HL7 V3, FHIR and DICOM that support the transmission of a 3-tuple { numeric identifier, readable string, vocabulary identifier } that allows the most appropriate nomenclature(s) to be used for a clinical application.

For the majority of medical devices, the IEEE 11073 nomenclature is unrivalled. It supports numeric observations, waveforms, (device) settings, annotations, events and alerts as well as simple and complex commands. It also defines device infrastructure vocabularies that identify the types of devices and their internal subsystems and additional information required for communication, battery and clock management and other essential functions.

[Table C.1](#) provides a summary of the term ‘partitions’ in the IEEE 11073 nomenclature, where each partition represents a 16-bit range of related numeric codes and, within each partition, individual terms are assigned a 16-bit integer code. The partition and code may be combined as a single 32-bit ‘context free’ numeric code, equal to the sum of the (Partition \* 2<sup>16</sup>) plus Code within that partition.

For example, ‘heart rate’ is represented by MDC\_ECG\_HEART\_RATE (2::16770), defined in Partition 2. In an HL7 V2 OBX-3 observation identifier, this term would be represented as |147842^MDC\_ECG\_HEART\_RATE^MDC|, where the first component 147842 is the ‘context free’ numeric identifier, the second component MDC\_ECG\_HEART\_RATE is a coded readable text string and the third component ‘MDC’ identifies the IEEE 11073 nomenclature.

**Table C.1 — Organization of IEEE 11073-10101**

Partition#	Partition
1	Object-Oriented: Classes, Attributes, Attributes, Actions, Notifications, Timekeeping Devices (MDS, VMD, CHAN) Top-level devices and subsystems
2	Vital signs parameters (ECG, SpO2, hemodynamic, infusion pumps; respiratory ventilator and anaesthesia; EEG, EOG, neuromonitoring, blood gas and fluid chemistry, fluid output, etc.)
3	Events and Alerts: Physiologic events, technical events, device and status events, ...
4	Units of Measurement (dimensions)
5	Virtual attributes
6	Parameter groups
7	Body Sites: EEG, EOG, neuromonitoring, cardiovascular, head, gas measurement other body sites
8	Communication Infrastructure: Device specialization, serial communication, time synchronization
128	PHD Disease Management: SABTE, Peak Flow, Glucose Monitoring, Insulin Pump, INR, etc.
129	PHD Health Fitness: Sensors, Activity, Exercise, ...
130	PHD Aging Independently: Home sensors, events, and location monitoring; medication dispenser
255	Return Codes
256	External Nomenclature: Identify IEEE 11073 and external nomenclatures and versions
258	Device Settings: Identifies SCADA terms that are numeric settings
514	Predicted Values: Identifies SCADA terms that are predicted values
NOTE The IEEE 11073-10101b nomenclature substantially extends IEEE 10101-2019 by adding over 630+ new event and alert identifiers plus new capabilities such as haemodialysis, neuromuscular transmission (NMT), regional cerebral oximetry (rSO2) and a significantly expanded infusion pump nomenclature based on the work of the IHE PCD domain over the past ten years.	

Partition 2 of IEEE 11073-10101-2019 covers the vast majority of numeric observations, waveforms and settings that can be measured or reported by acute care devices and PHDs. The Partition 2 device metrics and enumerations are listed in [Table C.2](#).

NOTE 2 Clauses to support Hemodialysis, NMT, rSO2 and IHE PCD infusion pump model and Medical Equipment Management (MEM) terms have been included in IEEE 11073-10101b:2023.



**Table C.2 — Partition 2 of IEEE 11073-10101**

Clause	Metrics and enumeration term groups
A.7.1	ECG measurements
A.7.2	ECG enumerations
A.7.3	hemodynamic monitoring measurements
A.7.4	respiratory, ventilator, and anaesthesia
A.7.5	common blood-gas, blood, urine, and other fluid chemistry measurements
A.7.6	fluid output measurements
A.7.7	infusion pumps
A.7.8	neurological monitoring measurements
A.7.9	neurophysiologic measurements and enumerations
A.7.10	stimulation modes
A.7.11	miscellaneous measurements
A.7.12	infant incubator and warmer microenvironments
A.7.13	spirometry
A.7.14	extensions for personal health devices

The IEEE 11073 Personal Health Devices (PHD) Working Group has defined the IEEE 11073-20601 base standard and the IEEE 11073-104xx series of Device Specializations that provide a complete specification of each device, including additional nomenclature required by the device not already in IEEE 11073-10101. (See [Annex B](#) for a list of PHD Specializations)

The IEEE 11073-104xx Device Specializations provide additional terminology required to support the device, including device status and other information. In a similar manner, acute-care PoCD devices use ‘containment trees’ to list the terms that are used and their relationship to the overall device and to each other, discussed in [C.2.2](#).

### **C.2.2 IEEE 11073 Device Containment Model (tabular format)**

An example of a ‘tabular’ containment tree for a simple PoCD vital signs monitor is shown in [Table C.3](#). The monitor has a top-level MDS (Medical Device System) representing the entire device, one or more VMDs (Virtual Medical Device) representing major subsystems and/or plug-in modules) and optional CHAN (channels) and METRIC-level observations.

**Table C.3 — Containment tree for simple PoCD vital signs monitor**

REFID	Description	CF_CODE10	UOM_MDC	UOM_UCUM	CF_UCODE10
MDC_DEV_SYS_VS_MDS	Vital Signs Monitor	70741	.	.	.
. MDC_DEV_ANALY_SAT_O2_VMD	Pulse Oximetry (VMD)	69642	.	.	.
.. MDC_DEV_ANALY_SAT_O2_CHAN	SpO2 (Channel)	69643	.	.	.
... MDC_PULS_OXIM_SAT_O2	SpO2	150456	MDC_DIM_PERCENT	%	262688
... MDC_PULS_OXIM_PULS_RATE	SpO2 Pulse Rate	149530	MDC_DIM_BEAT_PER_MIN	{beat}/min	264864
. MDC_DEV_ECG_VMD	ECG (VMD)	69798	.	.	.
.. MDC_DEV_CARD_RATE_CHAN	ECG Heart Rate (Channel)	70739	.	.	.
... MDC_ECG_CARD_BEAT_RATE	ECG Heart Rate	147842	MDC_DIM_BEAT_PER_MIN	{beat}/min	264864
. MDC_DEV_ANALY_RESP_RATE_VMD	Resp (VMD)	69722	.	.	.
.. MDC_DEV_ANALY_RESP_RATE_CHAN	Resp Rate (Channel)	69723	.	.	.
... MDC_RESP_RATE	Resp Rate	151562	MDC_DIM_RESP_PER_MIN	{resp}/min	264928
. MDC_DEV_PRESS_BLD_NONINV_VMD	NIBP (VMD)	70686	.	.	.
.. MDC_DEV_PRESS_BLD_NONINV_CHAN	Systolic/Diastolic/MAP/Rate	70687	.	.	.
... MDC_PRESS_BLD_NONINV_SYS	Systolic	150021	MDC_DIM_MMHG MDC_DIM_KILO_PASCAL	mm[Hg] kPa	266016 265987
... MDC_PRESS_BLD_NONINV_DIA	Diastolic	150022	MDC_DIM_MMHG MDC_DIM_KILO_PASCAL	mm[Hg] kPa	266016 265987
... MDC_PRESS_BLD_NONINV_MEAN	Mean Arterial Pressure	150023	MDC_DIM_MMHG MDC_DIM_KILO_PASCAL	mm[Hg] kPa	266016 265987
... MDC_PULS_RATE_NON_INV	Pulse Rate	149546	MDC_DIM_BEAT_PER_MIN MDC_DIM_PER_MIN MDC_DIM_PULS_PER_MIN	{beat}/min {count}/min {pulse}/min	264864 264672 264896
. MDC_DEV_METER_TEMP_VMD	Temperature (VMD)	69902	.	.	.
.. MDC_DEV_METER_TEMP_CHAN	Body Temp (Channel)	69903	.	.	.
... MDC_TEMP_BODY	Body temperature	150364	MDC_DIM_DEGC MDC_DIM_FAHR	Cel [degF]	268192 266560

The containment model defines a hierarchical structure for conveying this information, and it can precisely specify the device observations for a patient on a multi-parameter monitor, ventilator and infusion pumps in an ICU. It provides a rigorous framework for device modelling and semantic validation, including co-constraints such as units-of-measure and enumerated values, measurement sites and observation cardinality.

**NOTE 1** In the tabular containment representation, the hierarchical level is indicated by zero, one, two or three dots preceding the \_MDS, \_VMD, \_CHAN and METRIC REFIDs; additional FACET and SUBFACET levels can be used to report detailed aspects of an observation, such as measurement variance. Containment can also be encoded using XML, the preferred encoding for round-trip model exchange between vendors and the NIST RTMMSv2 system.

The containment model is largely independent of how the information is encoded, whether IEEE 11073 ASN.1-modeled binary, IHE PCD HL7 V2.6, FHIR or other message formats. It can be used to ensure semantic

correctness along the entire data path, from device through gateway and enterprise receiving systems and applications, using different message protocols.

### **C.2.3 IEEE 11073 and relationship to other standards**

The IEEE Standards Association (IEEE-SA) is a voluntary open consensus SDO that considers multiple viewpoints in a balanced and fair manner. The IEEE 11073 standards, in particular, are also written to facilitate their approval as International ISO/IEEE Standards, an important aspect for medical device manufacturers that manufacture and market their products internationally.

Another important aspect of this work is that multiple standards and profiling organizations are involved, such as HL7 and the Integrating the Healthcare Enterprise (IHE). The IHE provides opportunities for vendors to test their prototype implementations, such as the annual IHE North America Connectathon where vendors meet to test their interfaces. Devices and systems that pass Connectathon testing can demonstrate their products at the HIMSS/IHE Interoperability Showcase later in the year.

Working with organizations that span the entire medical device informatics data chain, from device to enterprise, ensures that IEEE 11073 and other nomenclatures are sufficiently complete and rigorous to support day-to-day clinical care as well as advanced clinical research in an open manner.

One example is the collaboration between IEEE 11073 and ISO 19223 working groups regarding ventilator terminology and the largely verbatim adoption of the ISO 19223 ventilator mode syntax in IEEE P11073-10101b. This simplifies adoption by the vendor and user communities since the mapping effort from proprietary to standardized mode names should only be done once.

**NOTE** The HL7 Domain Analysis Model: Intra-Procedure Anesthesia, Release 1 (Feb 2020) and SNOMED CT have also adopted major concepts from ISO 19223 ventilator vocabulary and mode syntax.

## **C.3 LOINC**

One of the most widely used vocabularies for identifying health observations and measurements is LOINC (Logical Observation Identifiers Names and Codes)<sup>14)</sup>. Led by Dr. Clem McDonald, LOINC development started in 1994 and has now grown to over 95,000 terms. The Regenstrief Institute serves as the organizational home for the effort.

One of the primary areas of focus for LOINC are clinical lab measurements. Although IEEE 11073 has identifiers for common bedside lab measurements and devices, future IEEE 11073 work involving lab measurements will disclose mappings to LOINC if the LOINC terms are not supported directly by the protocol (IEEE and LOINC initiated mapping in 2017-2018 and more agreements/collaboration started in 2025). For example, LOINC has already published terms related to SARS coronavirus 2 (SARS-CoV-2) and COVID-19 and it makes little sense for the IEEE 11073 to duplicate this work.

**NOTE** The implication here is that the protocol used by POCT test devices used at home, retail locations or in clinics are able to support { numeric identifier, readable string, vocabulary identifier } 3-tuples, such as |147842^MDC\_ECG\_HEART\_RATE^MDC| for IEEE 11073 or |8867-4^Heart rate^LN| for LOINC using HL7 V2.

One area of close collaboration has been mapping of the 800+ most frequently used IEEE 11073 terms from the NIST 'Harmonized Rosetta' (hRTM) to their LOINC equivalents. The mapping also includes pre- and post-coordination of each term with their units-of-measure and measurement site since the two nomenclatures handle this differently.

Another resource developed and maintained by Regenstrief is The Unified Code for Units of Measure (UCUM) that supports electronic communication of units-of-measure using coded yet computable and composable human-readable text strings. UCUM has been widely adopted by the medical informatics community for electronic data interchange and is now required by HL7, DICOM and other standards development and profiling organizations such as IHE.

To support and promote the use of UCUM for the exchange of medical device data, a normative mapping between IEEE 11073 MDC and UCUM units-of-measure has been defined. This mapping is available both as a

---

14) <https://loinc.org/>

general unit mapping as well as parameter-by-parameter, e.g. heart rate can be reported as ‘beat-per-minute’ using MDC\_DIM\_BEATS\_PER\_MIN (with a fixed-width 16- or 32-bit numeric code) or any of the equivalent UCUM expressions {beat}/min, {beats}/min, 1/min or /min.

## C.4 SNOMED

SNOMED CT (SNOMED Clinical Terms)<sup>15)</sup> is a systematically organized computer processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting. SNOMED development was started in 1965 and SNOMED CT (SCT) was created in 1990 as the merger of several organizations. As of January 2020, the International version of SNOMED CT supports over 350 000 semantic concepts.

SNOMED-CT is hierarchically organized and tends to focus on the “answers” (e.g. a clinical finding, procedure, observable entity, body structures and sites, etc.) whereas LOINC tends to focus on observation identifiers, aka “questions” (e.g. ‘what is the glucose concentration’).

**NOTE** As informally summarized by Daniel J. Vreeman, former Director for LOINC and Health Data Standards at Regenstrief: “LOINC provides codes that represent the names of information items (e.g. questions) and SNOMED CT provides codes that can represent nominal and ordinal values (e.g. answers) for these named information items.”

In contrast, IEEE 11073 covers both observation identifiers and enumerated values but with a narrower focus on medical devices used in the ICU, CCU, OR and ER. These devices often have strict data transfer rate and latency requirements that make it difficult to use the SNOMED CT numeric code identifiers ‘as is’. As a consequence, IEEE 11073 has borrowed sparingly from SNOMED CT for terminology related to body site and anatomical locations and several other enumerated value sets.

## C.5 NIST Test Tools and RTMMS

This clause discusses the mechanisms that are available to verify that devices can send and receive the data and correctly interpret what was sent.

The first and essential step is to capture the terminology in open standards such as IEEE 11073, LOINC and SNOMED CT. The next step is to rigorously capture the relationships between observation identifiers and the data types and values that they could report (such as co-constraints such as units-of-measure and enumerated values) and finally higher-level issues of the measurements and observations that a device is able to acquire and to receive and correctly interpret. The higher-level aspects often can involve significant discussion and negotiation between the communicating parties, but fortunately tools and documentation such as containment trees can provide a sufficiently rigorous ‘contract’ to ensure correctness and completeness according to the use cases and clinical scenarios that the devices and systems are intended to serve.

This is by no means a simple task, but fortunately the IHE PCD domain and IEEE 11073 have been working with the National Institute of Standards and Technology (NIST) for nearly 15 years on the development of a publicly available database, the Rosetta Terminology Mapping Management System (RTMMS) and a suite of message conformance test tools called the NIST Test Tools.

The NIST RTMMS and Test Tools are used together to test messages. The NIST Test Tools evaluate messages for basic conformity to HL7 V2 messaging (a capability used by numerous ‘domains’, and not just medical devices) and then layered above that there are additional requirements stipulated by the IHE PCD Technical Framework and above that the IEEE 11073 nomenclature and co-constraints captured in the RTMMS system.

The NIST RTMMS and Test Tools have played a critical role in the success of the IHE PCD domain and expectations are quite high for the second-generation RTMMSv2 that is currently under development. In addition to continuing to provide royalty-free access to the IEEE 11073 nomenclature, the RTMMSv2 will be support the definition of containment tree models that will enable the next level of rigorous message conformance and interoperability testing.

---

15) <https://www.snomed.org/>

## **Annex D** **(informative)**

### **Accelerating safe effective & secure (SES) RCC-MH**

#### **D.1 What does SES mean?**

Items that medical device manufacturers could consider to provide a reasonable assurance of safety and effectiveness of their interoperability include:

- designing systems with interoperability as an objective;
- conducting appropriate verification, validation and risk management activities;
- specifying the relevant functional, performance, and interface characteristics in a user available manner such as labelling.

#### **D.2 Safety**

In the world of healthcare devices, safety drives everything. Safety does not only refer to the clinical accuracy of the device, but also to other aspects such as mechanical safety, electrical safety and physical safety. In the context of RCC-MH solutions the safety of the communications link becomes a very important factor. Issues include:

- What happens if the link is broken?
- What happens if the link is unreliable?
- What happens if the data is corrupted?
- What happens if the device is compromised?
- What happens if the data is inadequately secured?
- What happen in a rural area where connectivity is a challenge?
- What happens if the link gets overwhelmed with other devices and users?
  - What happens in an apartment building with 50 other Wi-Fi users?
- What happens if the device is sent incorrect commands or improperly formatted data?

In addition, there are safety issues that are very use case specific. The safety issues related to remotely monitoring a patient in an ICU are very different from those related to monitoring a patient in their home or community. Issues include:

- How often in the data acquired and reviewed?
- How quickly can someone respond to a clinical event?
- How are caregivers notified of clinical events?
- How are device settings adjusted if the caregiver is miles away?

These topics and others are typically addressed as part of the risk analysis of the device, which is usually done as directed by ISO 14971. Since devices cannot be absolutely safe, the analysis looks at the potential harms versus the potential rewards and tries to balance the two after the application of any risk mitigations.

ISO 14971 should be used for any work related to medical device risk management as well as ISO/TR 24971 which provides guidance for the implementation of ISO 14971. The FDA in its “Design Consideration and Pre-Market Submission Recommendations for Interoperable Medical Devices”<sup>16)</sup> also provides guidance on risk management (see Sections V.C and VI.B which can also be useful references outside of the United States).

### **D.3 Effectiveness**

In the context of RCC-MH solutions, effectiveness is the ability to produce the intended results. In other words, it is the ability of the solution to do what it was intended to do, by all stakeholders, safely and securely.

In order to achieve effectiveness, the solution is decomposed into a set of requirements which typically include specifications related to (not exhaustive):

- a) usability;
- b) quality;
- c) reliability;
- d) interoperability.

### **D.4 Security**

Cybersecurity by itself has no purpose. Security is a secondary objective that derives its purpose (and consequently the security requirements that need to be met) from a set of primary objectives such as:

- a) safety;
- b) effectiveness;
- c) privacy and confidentiality;
- d) information integrity;
- e) authenticity, trust, non-repudiation;
- f) availability, i.e. operational and functional reliability;
- g) user and operator needs;
- h) financial and business needs;
- i) legal and regulatory frameworks;
- j) soft objectives such as reputation and trust.

That is not to say that security is only of secondary importance, but rather that it has no self-defined objectives and requirements as these are derived through analysis of the primary objectives listed above. Further, there is no perfect security and defining the right level of security requirements and the resulting implementation of security measures is always a balance of what is possible (e.g. available budgets) and feasible (e.g. required functionality) resulting in a residual level of risk that is deemed acceptable. Different types of health devices have different levels of risk to the patient and therefore require different security approaches.

Therefore, any security program that stands on its own without being defined by these primary objectives will fail and be counterproductive to the primary objective by either underdelivering, by being too restrictive, or by overinvesting in the wrong priorities.

For example, security is a prerequisite for privacy, without security one cannot assure privacy. However, the level of security required is defined by privacy considerations and within the scope of what is possible,

---

16) <https://www.fda.gov/media/95636/download>



practical, and feasible. For example, it can be reasonable to expect that a remote user would log on to a critical system using multi-factor authentication, thus ensuring the desired level of confidentiality. Yet, the same approach could be counterproductive when applied to a life-saving medical device in the ER.

This document primarily focuses on how to define, realize, and maintain the appropriate security posture to be met in order to assure safety and effectiveness in the RCC-MH environment.

The four main tenets of cybersecurity are:

- protect the device – security built in the design;
- manage the device – maintain security posture through the device lifecycle;
- protect the ecosystem – ensure security between device and ecosystem and vice versa;
- detect and respond to incidents – enable technical and clinical response.

In the context of RCC-MH and compared to the traditional hospital environment, there are additional challenges that make the implementation of security even more challenging: some of the traditional security controls, such as oversight and management of the devices, are not under the purview of trained staff, the device is not operated on a secure network, and data is being transmitted via a public network and most likely via an intermediary cloud service.

This makes proper implementation of security on the level of the device (tenet 1 above) an even more important aspect. Security management (tenet 2) is also critical so that management can be done mostly remotely or by untrained users (i.e. the patient or caregiver), minimizing the need for on-site intervention by trained staff. Relying on security measures provided by the ecosystem (e.g. the network) as well as relying on devices to detect security incidents to initiate the appropriate response is far less practical and desirable. In other words, in the remote care environment, emphasis should be on security by design and security by default, whereas secondary approaches such as security management, security posture of the ecosystem, and reliance on incident response can be reduced to a minimum.

## **Annex E** **(informative)**

### **RCC-MH socio-technical challenges**

#### **E.1 Social determinants of health**

The social determinants of health (SDH or SDoH) can be grouped into five domains: economic stability, education access and quality, healthcare access and quality, neighborhood and built environment, and social and community context. The impact of SDH on an individual's health, well-being, and quality of life has become widely accepted in recent years.

Recent reports and efforts continue to call attention to the need for innovative strategies to reduce and eliminate inequities caused by SDH, including Healthy People 2030<sup>17)</sup>. Challenges in the RCC-MH require strategies to reach and engage patients as well as novel tools and approaches to address challenges with data collection, harmonization, fusion, analysis and visualization of diverse SDH data from electronic health records (EHRs), administrative databases, sensor technologies, biomedical and non-traditional research platforms, self-report and medical and consumer devices.

The quality and validity of SDH information collected in RCC-MH settings continues to be hampered by a variety of issues, including differences in time scales, use of heterogeneous and sparse data, lack of metadata and paradata, poor interoperability, uncertain data provenance, lack of interpretability, uneven bias mitigation, gaps in data privacy and security, implicit biases built into measures and/or data algorithms, and the lack of diverse knowledge representations including taxonomies and ontologies that capture definitional differences in constructs from marginalized population groups, and their interrelationships.

---

17) <https://health.gov/healthypeople>



## **Annex F** **(informative)**

### **RCC-MH communications standards landscape**

#### **F.1 Overview**

Numerous standards address aspects of the RCC-MH solution space. This annex reviews the various applicable aspects, organized in accordance with the following categories:

- a) safety;
- b) effectiveness;
- c) interoperability;
- d) security.

#### **F.2 Safety-related standards landscape**

##### **F.2.1 Overview**

From a regulatory viewpoint device safety is achieved by a combination of a formal risk management and mitigation analysis with a formal development process. A number of standards are typically used to guide these efforts.

##### **F.2.2 ISO 14971**

ISO 14971 specifies terminology, principles and a process for risk management of medical devices, including software as a medical device and in vitro diagnostic medical devices. The process described intends to assist manufacturers of medical devices to identify the hazards associated with the medical device, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.

The requirements of ISO 14971 are applicable to all phases of the life cycle of a medical device. The process described in ISO 14971 applies to risks associated with a medical device, such as risks related to biocompatibility, data and systems security, electricity, moving parts, radiation, and usability.

ISO 14971 requires manufacturers to establish objective criteria for risk acceptability but does not specify acceptable risk levels.

Note The guidance document ISO/TR 24971 provides guidance on the application of ISO 14971.

The US Food and Drug Administration has granted Recognized Consensus Standard status to the third edition of the ISO 14971 risk management standard for medical devices and IVD products.

The process outlined in ISO 14971 can be summarized as follows:

- a) risk management planning;
- b) risk analysis;
- c) risk evaluation;
- d) risk controls;
- e) overall residual risk acceptability;

- f) risk management review;
- g) production and post-production information.

### **F.2.3 ISO 13485**

ISO 13485 is a quality management system standard for medical device/component manufacturers. This includes any organization that designs, produces, installs, or services medical devices and components. It requires a risk management process and points back to ISO 14971 for that aspect of the process.

### **F.2.4 IEC 62304**

IEC 62304 is a standard that specifies life cycle requirements for the development of medical software and software within medical devices.

It is harmonized by the European Union (EU) and the United States (US), and therefore can be used as a benchmark to comply with regulatory requirements from both these markets.

### **F.2.5 IEC 82304-1**

IEC 82304-1 applies to the safety and security of health software products designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware. Its primary focus is on the requirements for manufacturers.

It covers the entire lifecycle including design, development, validation, installation, maintenance and disposal of health software products.

Health software products are intended by their manufacturer for managing, maintaining or improving health of individual persons, or the delivery of care. Some health software can contribute to a hazardous situation and risk control is therefore required to prevent harm or reduce the likelihood of harm occurring. Testing of the finished product is not, by itself, adequate to address the safety of health software. Therefore, requirements for the processes by which the health software is developed are necessary. IEC 82304-1 relies heavily on IEC 62304:2006 and IEC 62304:2006/AMD1:2015 for the software development process which can be applied to health software products.

### **F.2.6 ANSI/AAMI/UL 2800 series**

The ANSI/AAMI/UL 2800 series addresses the safety, security and effectiveness of the interoperable elements of medical systems throughout their development, deployment, assembly, and operation. The standard applies both the IEC 62304 and ISO 14971 standards to the problem space of interoperable devices.

The ANSI/AAMI/UL 2800 series employs a life cycle process approach to organizing requirements, providing a set of interoperability planning, realization, deployment, and monitoring activities that incorporate cross-cutting requirements for security and risk management. ANSI/AAMI/UL 2800 also provides supplementary guidance on key clinical and engineering properties essential for ensuring effective interoperability.

### **F.2.7 ISO/IEC 80001 series**

The ISO/IEC 80001 series deals with the general challenge of maintaining the safety, effectiveness and security of medical devices when they are sharing a network with IT devices such as printers, phones, general purpose computers, etc. The development of this standard was triggered by the increasing use of wired and wireless LANs which could not be dedicated to the sole use of medical device networks and had to be shared with other users, which created a number of risk management issues.

Most of the recommendations and requirements in the ISO/IEC 80001 series are on the responsible organization (RO), which is typically the IT organization responsible for managing the network. Manufacturers are responsible for providing adequate documentation and support to the RO to allow them to safely deploy the medical devices on the IT network.

Given that most RCC-MH solutions use an intranet or internet, the ISO/IEC 80001 series is quite relevant and provides substantial food for thought concerning potential risks that might need to be mitigated. One of

the most challenging aspects is configuration management, as IT networks are continuously changing and therefore risk mitigation strategies probably should be updated often.

The core standard, IEC 80001-1, defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security (the key properties). It does not specify acceptable risk levels and applies after a medical device has been acquired by a responsible organization and is a candidate for incorporation into an IT-network. It applies throughout the life cycle of IT-networks incorporating medical devices. IEC 80001-1 applies where there is no single medical device manufacturer assuming responsibility for addressing the key properties of the IT-network incorporating a medical device.

The ISO/IEC 80001 series includes a number of other guidance documents. It is also undergoing a transformation with some of the documents being withdrawn or replaced with documents in the IEC 81001 series.

- IEC/TR 80001-2-1: Step by step risk management of medical IT-networks; practical applications and examples
- IEC/TR 80001-2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC/TR 80001-2-3: Guidance for wireless networks
- IEC/TR 80001-2-4: General implementation guidance for healthcare delivery organizations
- IEC/TR 80001-2-5: Application guidance — Guidance for distributed alarm systems
- IEC/TR 80001-2-6: Application guidance — Guidance for responsibility agreements
- IEC/TR 80001-2-7: Guidance for HDOs on how to self-assess their conformance with IEC 80001-1
- IEC/TR 80001-2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC/TR 80001-2-2
- IEC/TR 80001-2-9: Application guidance — Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

## **F.2.8 IEC 62366-1**

This standard specifies a process for a manufacturer to analyse, specify, develop and evaluate the usability of medical devices. It focuses on the usability engineering (human factors engineering) process which permits the manufacturer to assess and mitigate risks associated with medical devices to provide safety for the patient, user, and others. The standard can be used to identify, but not to assess or mitigate, risks associated with abnormal use.

International regulatory bodies are placing an increasing emphasis on usability evaluations of medical devices with the aim of reducing user errors and improving the safety of the devices.

## **F.3 Effectiveness standards landscape**

### **F.3.1 General**

As previously discussed, effectiveness is the ability of a solution to do what it is supposed to do. In the medical device world, there are numerous standards that specify a minimum level of clinical performance such as the IEC 60601 and ISO/IEC 80601 series described in [F.3.2](#).

### **F.3.2 IEC 60601 and ISO/IEC 80601 standards**

These series establish a core set of requirements for the development of medical devices in the IEC 60601-1-x series. This includes topics such as electrical safety, EMC, EMI, alarm handling, etc.

The IEC 60601-2-x and ISO/IEC 80601-2-x series expand on the core standards and provide particular safety related requirements for specific medical device types such as ventilators, anaesthesia machines, pacemakers, thermometers, etc.

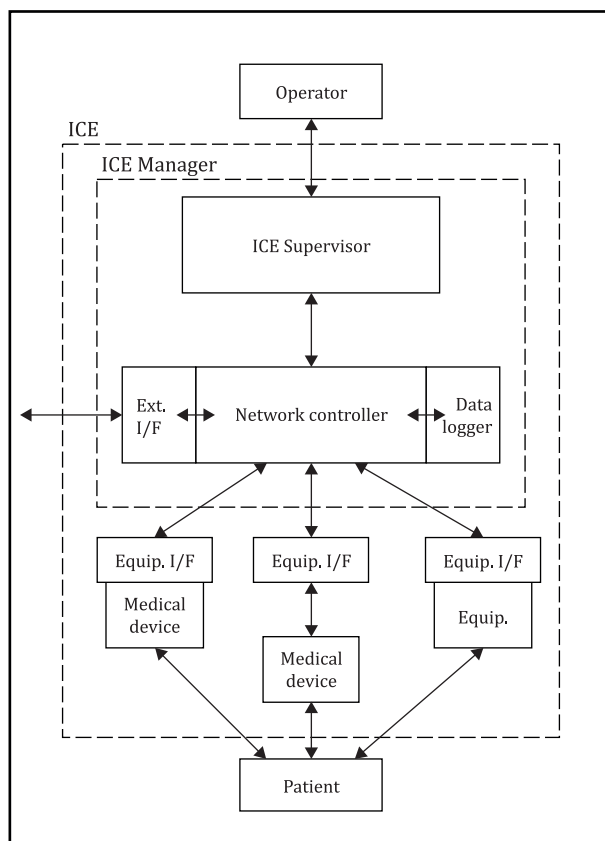
## F.4 Device-to-device interoperability standards landscape

### F.4.1 Device interoperability architectures

#### F.4.1.1 AAMI 2700 (ICE) series

The AAMI 2700 series is focused on defining “Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE)”. Currently there are 2 standards in the series: ANSI/AAMI 2700-1 “General requirements and conceptual model” which defines the reference architecture and AAMI 2700-2-1 which defines “Particular requirements for forensic data logging”.

The AAMI 2700-1 ICE conceptual model (see [Figure F.1](#)) is built around a hub-and-spoke architecture where all communication is routed by a network controller which is in turn managed by an ICE supervisor. [Figure F.1](#) shows the conceptual model from the standard.



**Figure F.1 — AAMI 2700-1 ICE conceptual model**

AAMI 2700-2-1 defines requirements for a forensic data logger which is used to capture data that can be used to analyse technical events after they occurred. The data store will contain a log of the messages that traversed the network in order to analyse any network related failures or issues post occurrence.

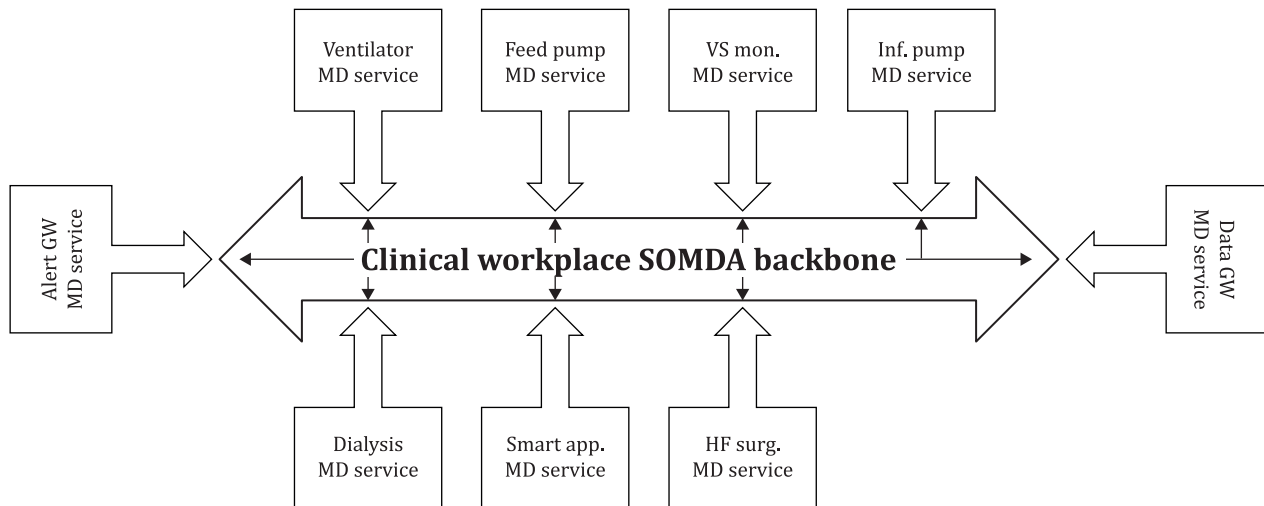
It is also anticipated that a number of other supporting standards will be released, though at this time there is no active work on them. They include:

- AAMI 2700-2-2: Requirements for network control and equipment interfaces
- AAMI 2700-2-3: Requirements for device models

- AAMI 2700-2-4: Requirements for the supervisor
- AAMI 2700-2-5: Requirements for safe and reliable integration

#### F4.1.2 IEEE 11073 SDC

The IEEE 11073 Service Oriented Device Communication (SDC) series not only covers architecture but also protocol, semantics, etc. and is covered in more detail in 4.2. As is implied by the name, SDC implies a service-oriented architecture (depicted in [Figure F.2](#)) with peer-to-peer discovery and communication, though it is possible to use it in a more ‘supervised’ ICE compatible fashion.



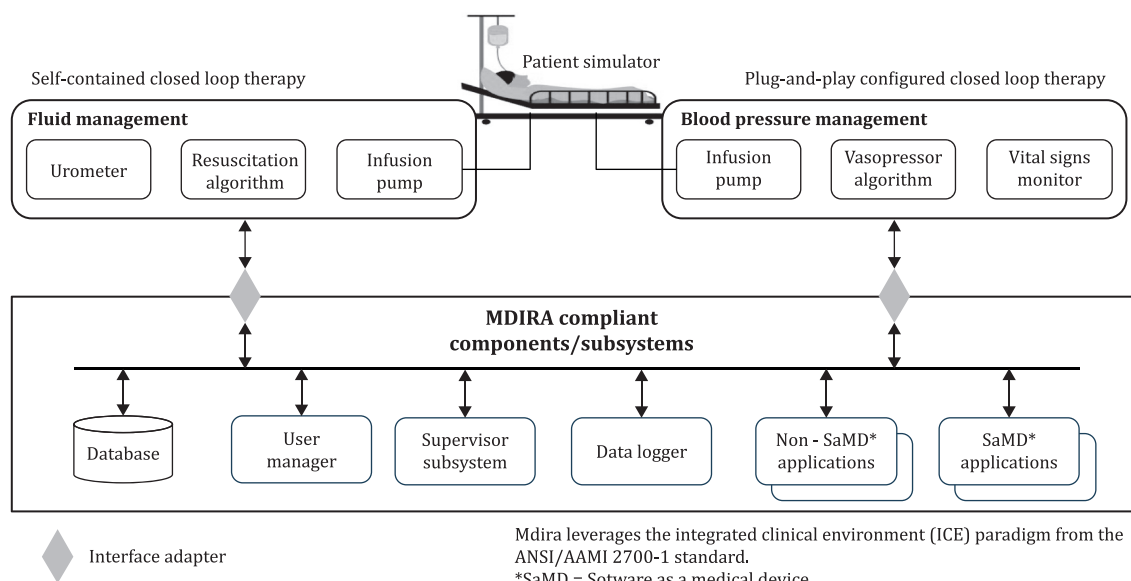
**Figure F.2 — Peer-to-peer SDC architecture overview**

#### F4.1.3 DoD MDIRA project

The Defense Health Agency funded the U.S. Army Medical Research and Development Command to research technical architectures to support autonomous medical systems for prolonged care in austere environments and hospitals of the future. The result is MDIRA (Medical Device Interoperability Reference Architecture), a technical framework intended to guide stakeholder organizations and industry in developing interoperable, safe, and secure medical device systems that will deliver advanced and autonomous medical care. The MDIRA research team is engaging stakeholders from government, industry, academia, and civilian healthcare who are on the cutting edge of integrated clinical environments, closed-loop care systems, medical device and cybersecurity standards, and regulatory clearance and approvals for patient safety.

From an architecture standpoint, MDIRA borrows heavily from both the ICE and SDC architectures. There is no ICE network controller and the role of the supervisor is somewhat different than defined in the standard. [Figure F.3](#) provides a high-level view.

## Mdira reference implementation concept



SOURCE Created by Johns Hopkins University Applied Physics Laboratory, reproduced with permission of the authors.

**Figure F.3 — MDIRA system concept**

The project publishes regular updates to its architecture document which can be found on their website<sup>18)</sup>.

## F.4.2 Standards: service interoperability communication

### F.4.2.1 IEEE 11073 standards

#### F.4.2.1.1 General

In addition to the IEEE 11073 SDC architecture that was described in [F.4.1.2](#), the IEEE 11073 series specifies the full interoperability stack including nomenclature, syntax and information models. Work on these standards started back to the 1990s, and these documents were originally intended for plug-and-play interoperability for point-of-care devices in professional healthcare provider environments such as ICUs, ORs, ERs, etc. With the advent of consumer-oriented devices, the IEEE 11073 Standards Committee was partitioned into the point-of-care device (PoCD) and the personal health device (PHD) working groups. The PHD WG tends to focus on devices with constrained compute and memory resources typically using Bluetooth and/or USB as a physical layer. The PoCD WG tends to focus on devices with more compute, memory and power resources typically using Wi-Fi and/or Ethernet as a physical layer.

Most of the IEEE 11073 standards have also been adopted by ISO and are labelled as such.

#### F.4.2.1.2 IEEE 11073 – Foundational standards

Despite the 2 separate WGs, there are a number of key concepts that are shared between the working groups. These include the nomenclature, the domain information model (DIM), and cybersecurity. The nomenclature is discussed in considerable depth further on in this document (see [Annex A](#)). The domain information model (ISO/IEEE 11073-10201) has been profiled (typically simplified) for applicability to the PHD oriented use cases (see ISO/IEEE 11073-10206 and IEEE 11073-20601). The nomenclature and DIM are also used in the HL7 DoF (Device on FHIR) and IHE DEV PCD program profiles (see [F.4.3.2](#)). Cybersecurity (IEEE 11073-40101 and IEEE 11073-40102) is described in more detail in this document (see [G.2.5](#)).

18) <https://secwww.jhuapl.edu/mdira>

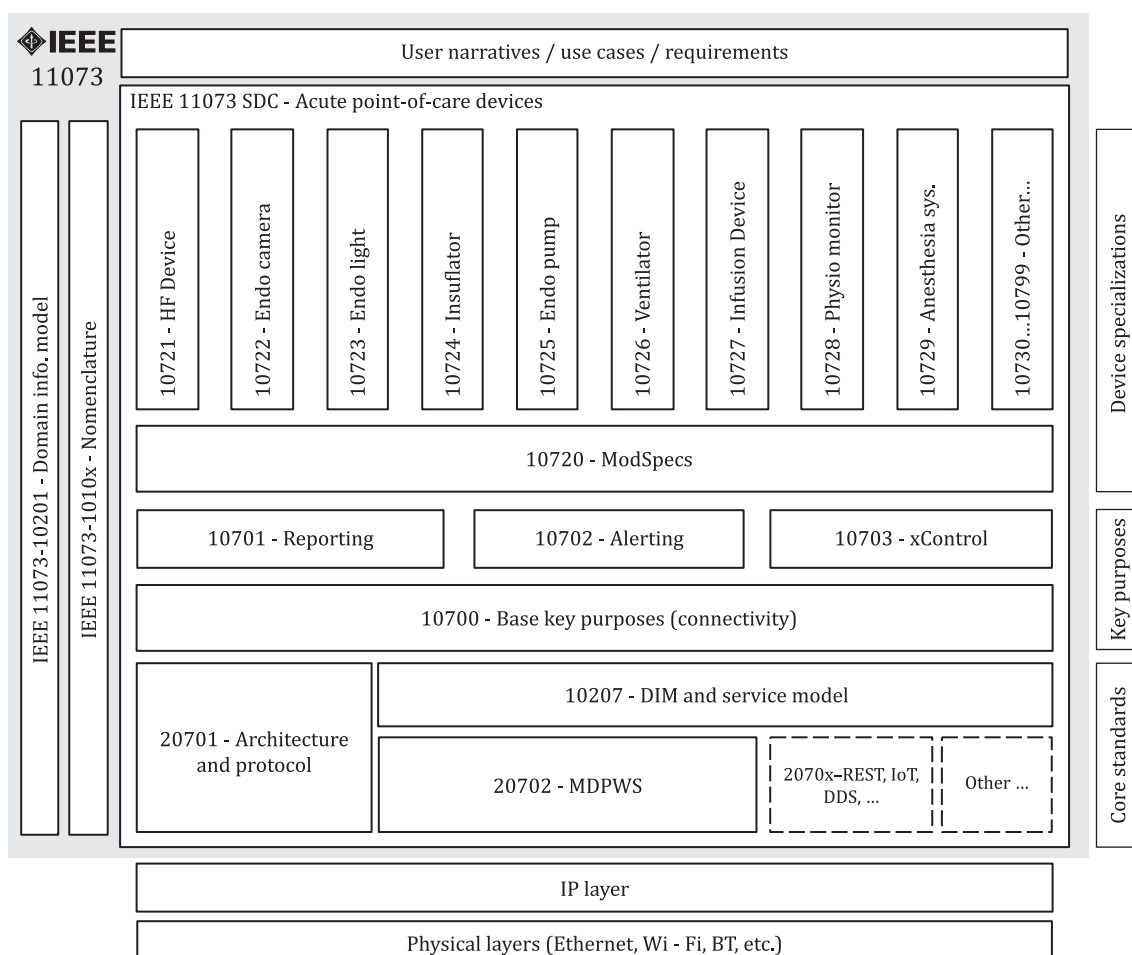
### F.4.2.1.3 IEEE 11073 – Point-of-care devices working group

IEEE 11073 PoCD-related standards support real-time plug-and-play interoperability for person connected medical acute care devices such as patient monitors, ventilators, infusion devices, etc. In this case:

- “real-time” means that data from multiple devices can be retrieved, time correlated, and displayed or processed in fractions of a second;
- “plug-and-play” means that all a user has to do is make the connection – the systems automatically detect, configure, and communicate without any other human interaction;
- “efficient exchange of care device data” means that information that is captured at the point-of-care (e.g. personal vital signs data) can be archived, retrieved, and processed by many different types of applications without extensive software and equipment support, and without needless loss of information.

Within the last few years, the WG has been focusing on a service-oriented architecture for high performance medical device interoperability under the SDC (Service-oriented Device Connectivity) moniker. This approach was originally developed in a multi-partner project funded by the German government. This project has evolved into the OR.NET<sup>19)</sup> consortium which has prototyped and publicly demonstrated device implementations based on SDC.

[Figure F.4](#) illustrates the building blocks and architecture of an SDC based implementation. Note that the ISO/IEEE 107xx standards are still in development, however products can still be developed and released based on the existing ISO/IEEE 11073-10207, ISO/IEEE 11073-20701 and ISO/IEEE 11073-20702.



**Figure F.4 — IEEE 11073 PoCD architecture layers**

19) [www.ornet.org](http://www.ornet.org)

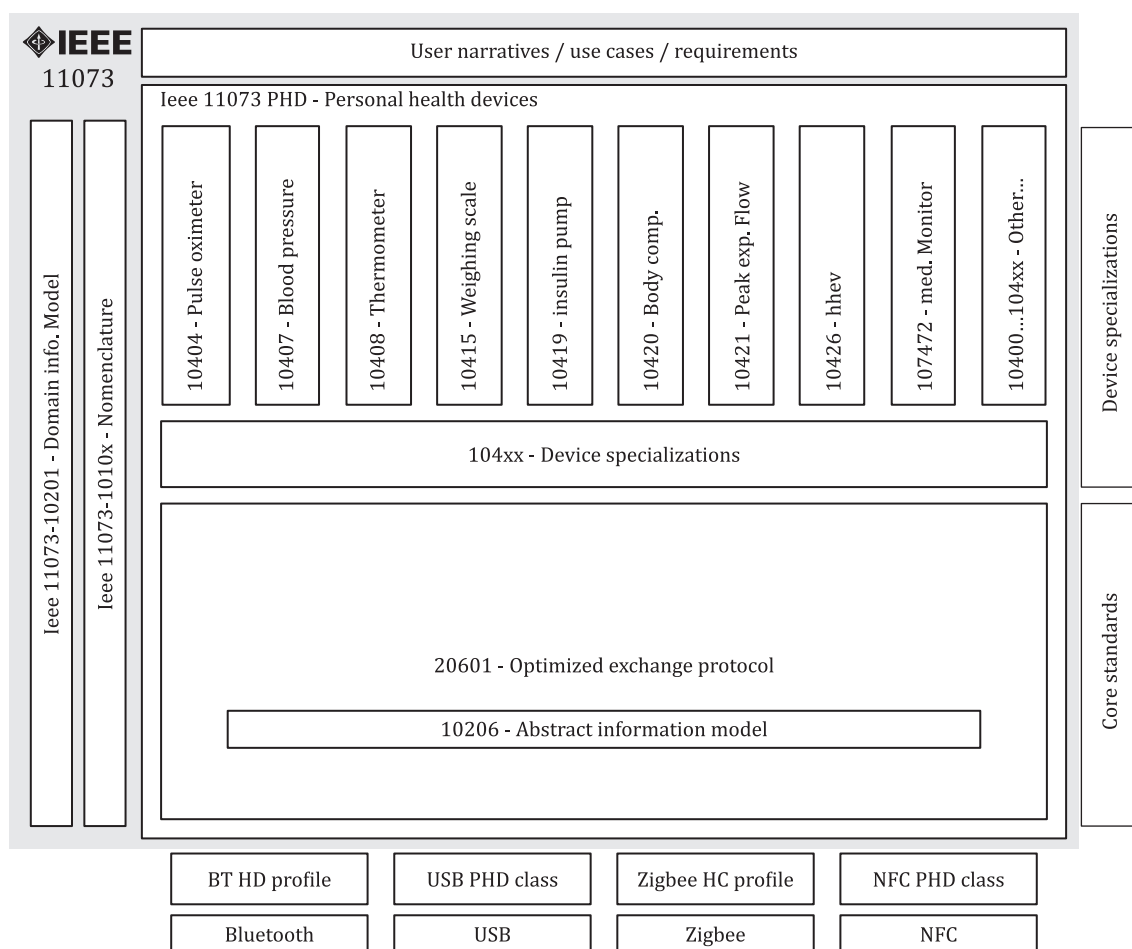


#### F.4.2.1.4 IEEE 11073 – Personal health devices working group

As fitness and health devices entered the market, the IEEE 11073 Standards Committee saw the need to address interoperability for these types of devices which are not generally used directly by clinicians, but that can provide data with clinical significance. The term PHD evolved for medical devices, as well as for health and fitness devices, used outside of professional healthcare organizations, by users directly. Today, PHDs are commonly sold together with consumer electronics products. They are used in home and mobile environments. Most devices provide digital displays and local storage of readings. Because of their small size and limited power supply, many devices have low computational limits and limited functionality. Users increasingly find it cumbersome to read data from displays and wish to use the data generated by these PHDs beyond the limited capabilities of the device. Communicating the recorded data is therefore gaining in importance, with the additional advantage of avoiding data breaches. Over time, as the functionality of PHDs increase, their usage in clinical use cases is only expected to increase.

The IEEE PHD series takes the approach of providing a base standard containing a “toolkit” of capabilities (ISO/IEEE 11073-20601) along with “device specializations” (see [Annex B](#)) tailoring the broad toolkit to specific usages to meet the needs of the device being specialized. As previously mentioned, a standard nomenclature (ISO/IEEE 11073-10101) is used across the base standard and all specializations, with relevant nomenclature terms included in device specializations for ease of implementation. The goal is for the device specialization together with the base standard to be self-contained and complete.

[Figure F.5](#) provides an overview of the PHD standards architecture.



**Figure F.5 — IEEE 11073 PHD architecture layers**



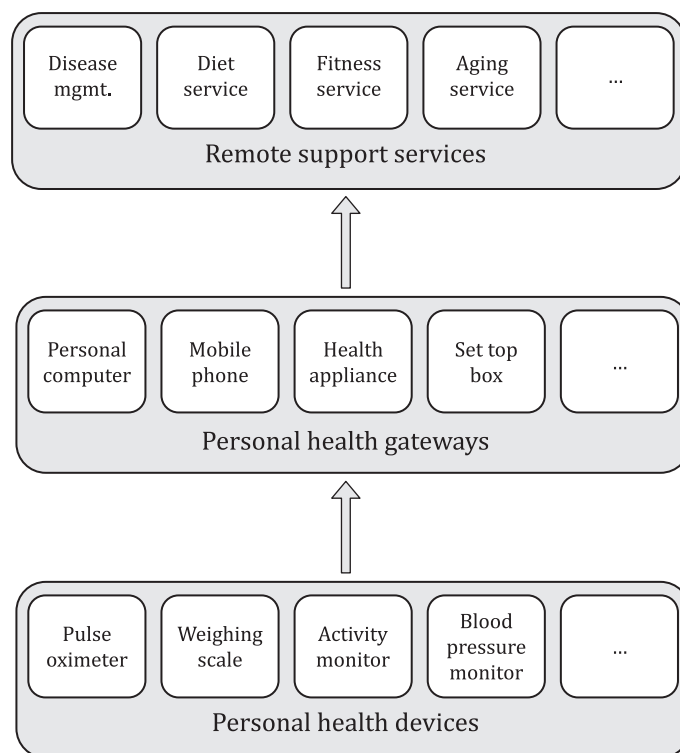
#### F4.2.1.5 IEEE 11073-10206 abstract content model

The IEEE 11073 PHD abstract information content model (ACOM) describes a PHD through a class containing manufacturer-provided information about the device, observations generated from the device and optional classes that describe the power and clock capabilities of the device. ACOM can be used to represent both the device and the measurement data generated by the device. This standard uses IEEE 11073-10101 nomenclature to express the underlying meaning, or semantic content in the information model. The model does not prescribe a security framework, nor a method for encoding or exchanging information.

Measurement data generated by the device, in conjunction with the supporting information about the measurement, is called an observation. ACOM provides a structured way to compose information about a range of different observation types including observations that are scalars, lists, discrete observations (states and events), a sequence of periodic scalars, and strings. Commonly used PHDs generate observations that can be expressed using these types. ACOM can therefore be used to document the information content in a wide range of PHDs.

ACOM descriptions for common PHDs are provided. These descriptions provide the same type of information that is found in the Domain Information Model of the IEEE 11073-104XX series of specifications.

Categories and typical types of devices in the personal health space are shown in [Figure F.6](#). PHDs (e.g. blood pressure monitors, weighing scales, and pedometers) collect information about a person (or persons) and transfer the information to a Personal Health Gateway (PHG) (e.g. cell phone, health appliance, or personal computer) for collection, display, and possible later transmission. The PHG can also forward the data to remote support services for further analysis or to support disease management. The information is available independently from a range of domains including disease management, health and fitness, and aging.



**Figure F.6 — Personal health device deployment architecture**

The IEEE 11073™ PHD working group focuses on the information content and the data exchange between the PHDs and PHG. Within the overall IEEE 11073 context, ACOM concentrates on the information content of PHDs, with the objective of allowing the information to be used seamlessly across the healthcare ecosystem.

#### **F.4.2.1.6 Personal Connected Health Alliance (PCHAlliance)**

The Personal Connected Health Alliance (PCHAlliance or PCHA) has a mission to support a patient/consumer-centred approach to improving health and wellness. This is achieved through personal technology that supports secure clinical-grade data transformed into actionable information based on evidence to change health behaviours and enable management of chronic conditions. Continua is a major initiative within the PCHAlliance that publishes and promotes the global adoption of standards and implementation guidelines that unleash the massive amounts of medical-grade data, enabling a more holistic perspective. Continua enables remote care service companies to draw upon the Continua Design Guidelines to integrate information & communication technology (ICT) systems.

The IHE Personal Connected Health Program was created in 2019 as part of an effort to broaden the scope of the IHE Patient Care Device Domain [now the IHE Devices (DEV) Domain] to include personal connected health outside the clinical environment. In 2019, IHE entered into a cooperative agreement with the PCHAlliance to leverage their experiences and expertise in personal connected health and remote patient monitoring. More specifically, the early Personal Connected Health profiles are based on PCHA's Continua Design Guidelines that provide the only secure end-to-end ICT solution for personal connected health and care using open standards.

#### **F.4.2.2 IEEE/UL 2933 – TIPPSS for clinical IoT**

The IEEE/UL 2933 standards project was formed in 2020 (published in 2024) with the objective of creating a standard for the Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security. The standard establishes requirements for Clinical IoT sensors/actuators/devices and connected apps and applications.

The purpose of this standard is to help enable secured data sharing in connected healthcare solutions for improved healthcare outcomes, help protect patient and data privacy and security, and assist in protecting the subjects and humans who are the ultimate users of these solutions.

### **F.4.3 Device to healthcare enterprise/cloud apps interoperability standards landscape**

#### **F.4.3.1 IHE DEV domain overview**

The Integrating the Healthcare Enterprise IHE Devices (DEV) Domain promotes the integration of clinical and personal health devices into the healthcare enterprise, from the point-of-care to the EHR, potentially resulting in significant improvements in patient safety and quality of care. IHE's process is based on adapting existing standards and creating profiles for specific use cases, improving interoperability by restricting optionality, specifying field usage, and clarifying how to apply standards based on the use case. In addition, IHE conducts Connectathons which promote cross-vendor testing of implementations.

The DEV domain is currently organized in the following three programs.

- a) PCD (patient care device) focuses on exchanging information from acute care devices such as vital signs, physiological monitors, ventilators, infusion pumps, and anaesthesia workstations with enterprise applications such as clinical information systems.
- b) PCH (Personal Connected Health) promotes the development of IHE profiles for remote health and fitness monitoring in support of consumer-centred approach to improving their health and wellness. PCH profiles provide guidance for implementing globally recognized standards that enable collection and sharing of massive amounts of medical-grade personal health data.
- c) DPI (device point-of-care interoperability) develops profiles for point-of-care devices leveraging the IEEE 11073 SDC series.

#### **F.4.3.2 IHE DEV – PCD program**

The IHE DEV Patient Care Device (PCD) program is concerned with use cases in which at least one actor is a regulated patient-centric point-of-care medical device that communicates with at least one other actor such

as a medical device or information system. The PCD program has been active since 2005 and has defined and publicly tested a number of profiles:

- ACM (Alert Communication Management);
- DEC (Device Enterprise Communication);
- MEM (Medical Equipment Management);
- MEMDMC (Device Management Communication);
- MEMLS (Location Services);
- IPEC (Infusion Pump Event Communication);
- PCIM (Point of Care Identity Management);
- PIV (Point of Care Infusion Verification);
- RDQ (Retrospective Data Query);
- RTM (Rosetta Terminology Mapping);
- WCM (Waveform Communication Module).

These profiles are typically based on a combination of HL7 v2 syntax as well as IEEE 11073 based semantics (nomenclature and information model). Many of the IHE PCD profiles have achieved wide manufacturer and provider acceptance, most notably the DEC profile which communicates results from devices to IT systems, the PIV profile which supports bar-code-based infusion safety and the ACM profile which is used to report and distribute alerts to clinician devices.

#### **F4.3.3 IHE DEV – PCH program**

The IHE Personal Connected Health (PCH) program supports those device-related harmonization activities that are required for seamless integration between the clinical and consumer environments. The PCH program also coordinates with other programs of the DEV domain and promotes the development of IHE profiles for remote health and fitness monitoring in support of consumer-centred approaches to improving their health and wellness. PCH profiles provide guidance for implementing globally recognized standards that enable collection and sharing of massive amounts of medical-grade personal health data.

The PCH program currently has several activities that address the following points.

- Abstract information content Model (ACOM) – the collaboration with the IEEE 11073 PHD WG to create the IEEE 11073-10206 standard: a stand-alone simplified information model independent of transport that directly maps to HL7 FHIR.
- Direct-to-Cloud (D2C) constrained devices – the development of implementation guidance, in form of a new IHE Devices profile, for uploading ACOM-based health-related observations from a compute-constrained health sensor device directly to a health & fitness server. The upload is done via cellular IoT and zero-touch configuration (no Bluetooth or Wi-Fi pairing).
- Generic Health Sensor (GHS) – the collaboration with the Bluetooth SIG Medical Devices WG to create a service and profile specifications to provide a means of communicating a wide range of ACOM-based health-related observations from a health sensor device to a collector (that can act as a personal health gateway).
- Mobile health apps – the development of profiles that foster a singular domain in which to coordinate the development of implementation guidelines to help patient and consumer facing application developers employ IHE profiles. These profiles apply HL7 FHIR, IEEE 11073 and other standards for the purpose of moving data between personal mobile devices and applications, and health information systems and exchanges.

- Test and tools – the development of test and verification tools and processes to foster compliance with the relevant IHE Profiles.
- CDG evolution and maintenance – evolving and maintaining PCHA's Continua Design Guidelines.
- Backlog projects – current activities on HOLD include updating the Remote Patient Monitoring (RPM) Profile and finalizing the work on questionnaires.

The PCH program has defined the Personal Health Device Observation Upload (POU) IHE Profile which describes a standardized means of representing personal healthcare device (PHD) data as FHIR resources. Health care is increasingly being delivered outside of a clinical setting. PHDs are often used in non-clinical settings. This profile prescribes a framework for moving the health information generated by PHDs into the enterprise in an interoperable manner. The profile addresses concerns associated with representation and translation of PHD information fostering usability and trust of the PHD data.

The profile makes normative references to a range of PCHAlliance, Bluetooth Special Interest Group, and HL7 documents that address different issues associated with collecting and communicating health data in a home setting. In particular, it requires the use of IEEE 11073 nomenclature to describe the medical observation. It then outlines how the medical observations are to be communicated from the health device through a gateway, which can be internal to the health device itself, and then translated into FHIR and delivered to a FHIR server. The profile addresses the movement of the data over a number of commonly used communication systems, including Bluetooth Low Energy and Universal Serial Bus providing the basis for interoperability between the health device and the gateway. The profile uses the HL7 PHD implementation guide (PHD IG) to describe how to map the IEEE based information into the FHIR resources that are presented to the FHIR server.

#### **F.4.3.4 IHE DEV – DPI program**

The IHE DEV DPI Program is focused on profiling point-of-care device-to-device connectivity based on the IEEE 11073 SDC series. The program was created at the end of 2020 and is currently working on the SDPi (service-oriented device point-of-care interoperability) profiles. They leverage the ISO/IEEE 11073 SDC standards that provide for SOA-based device-to-device plug-and-play interoperability at high acuity points of care (e.g. surgery, ICU or emergency). The four IHE SDPi profiles in development map to four ISO/IEEE 11073 SDC Participant Key interoperability Purposes (PKP) standards tailored for medical technology: Plug-and-play Connectivity (SDPi-P), Reporting (SDPi-R), Alerting (SDPi-A) and external Control (SDPi-xC).

The IHE SDPi profiles include defined “gateway” actors for integrating an SDC-based environment with both HL7 V2 and FHIR connected environments. This aspect of the work is done as a joint HL7/IHE project called Project Gemini. More information follows in [F.4.4.3](#).

### **F.4.4 HL7 FHIR and devices**

#### **F.4.4.1 General**

While the efforts of the IHE DEV domain have so far focused on HL7 v2 for device to enterprise/cloud connectivity, HL7 FHIR oriented efforts are also ongoing for the same applications.

#### **F.4.4.2 HL7 devices on FHIR**

The HL7 Devices on FHIR (DoF) work began in the summer of 2016, building on work that had been pursued during the preceding years, and has been a very active collaboration with HIMSS/PCHAlliance Continua and IHE Devices, resulting in the development of two implementation guides (one for PoCD and one for PHD).

The goal of this work is to push forward FHIR Implementation Guides for both personal health and point-of-care (acute care) devices for use cases beginning with straightforward device observation reporting for numerics, enumerations and waveforms providing for full traceability from observations to identity and characteristics of the device and subsystem that sourced them.

The next phase will be to provide for representing both physiological events and alerts of clinical significance, and technical alerts to technology managers for surveillance for error states or upcoming maintenance needs.

The DoF team is actively working to expand the IGs to support both device alerting, as well as device SDC inter-connection. There is also consideration of a 3rd IG focused not on helping device technologists send granular device data using FHIR – which can quickly get very complicated even with PHDs – but on the applications community that wants to integrate device-sourced information. All of this work is included in the initial set of projects identified in [F.4.4.3](#).

#### **F.4.4.3 HL7/IHE Gemini Project – SDPi and FHIR**

This joint HL7-IHE Gemini program pulls together established and emerging work in the HL7 DEVICES and IHE DEVICES working groups to achieve a greater degree of collaboration efficiency as well as coordination and cohesion between the activities and work products of the two groups. The program objectives include:

- One simple device interoperability story – from Surgery to Surfing!
- One coordinated and cohesive set of specifications and implementation/test tools
- One centralized collaboration place-and-tool set flying under the “SDPi+FHIR” banner

The Gemini program focus on “SDPi+FHIR” brings together two core specification areas, IHE's SDPi and HL7's FHIR, that can cover the three main use contexts: high-acuity point-of-care, healthcare enterprise, and home/mobile. There can be other alternative standards and technical approaches, but much of this work is being actively pursued in the various organizations, by many of the same people but with ad hoc coordination and collaboration, a sub-optimal mix of tools, and with work artefacts spread across various locations using different formats.

#### **F.4.5 DICOM**

Digital Imaging and Communications in Medicine (DICOM) is the standard for the communication and management of medical imaging information and related data. The DICOM standard addresses the exchange of digital information between medical imaging equipment and other systems. Because such equipment could interoperate with other medical devices and information systems, the scope of this standard overlaps with other areas of medical informatics. DICOM has been developed with an emphasis on diagnostic medical imaging as practiced in radiology, cardiology, pathology, dentistry, ophthalmology and related disciplines, and image-based therapies such as interventional radiology, radiotherapy and surgery. However, it is also applicable to a wide range of image and non-image related information exchanged in clinical, research, veterinary, and other medical environments.

DICOM facilitates interoperability of medical imaging equipment by specifying:

- for network communications, a set of protocols to be followed by devices claiming conformance to the standard;
- the syntax and semantics of commands and associated information that can be exchanged using these protocols;
- for media communication, a set of media storage services to be followed by devices claiming conformance to the standard, as well as a file format and a medical directory structure to facilitate access to the images and related information stored on interchange media;
- information to supply with an implementation for which conformance to the standard is claimed.

DICOM is a service-oriented protocol, specifying the semantics of commands and associated data, and how devices claiming conformance to the standard react to commands and data being exchanged. Specified services include support for management of the workflow of an imaging department. Many DICOM services involve the exchange of persistent information objects, such as images. An instance of such an information object could be exchanged across many systems and many organizational contexts, and over time. While minor changes can be made to the attributes of an instance to facilitate its handling within a particular organization (e.g. by coercing a Patient ID to the value used in a local context), the semantic content of an instance does not change.



Conformance to the DICOM standard is stated in terms of service-object pair (SOP) classes, which represent services (such as storage using network, media, or web) operating on types of information objects (such as CT or MR images).

A large number of information objects defined in the DICOM standard follow a common composite information model with information entities representing patient, study, series, equipment, frame of reference, and the specific instance data type. This information model is a simplification of the real world concepts and activities of medical imaging; for acquisition modalities, a study is approximately equivalent to an ordered procedure, and a series is approximately equivalent to a performed data acquisition protocol element. In other domains, such as radiotherapy, the study and series are less clearly related to real world entities or activities, but they are still required for consistency. This simplified model is sufficient for the pragmatic needs of managing imaging and related data collected in routine practice.

#### **F.4.6 IEEE 1752 open mobile health data**

Mobile health (mHealth) data encompasses all varieties of personal health data that can be collected from equipment-specific sensors (on the body, in the body, around the body) and mobile applications (within any mobile computing device). Standardizing mHealth data and metadata aims to facilitate data aggregation and exchange across different platforms (e.g. between wearable devices, mobile app and backend) with greater ease (partly due to less conflicting specification) and accuracy (partly due to a wider support of use cases and definitions).

The primary goal of IEEE 1752 is to provide standard semantics to enable meaningful description, exchange, sharing, and use of mHealth data in its scope. IEEE 1752.1 defines specifications for standardized representations in JSON Schema for mHealth minimum metadata and provides common data schemas for digital biomarkers related to sleep and physical activity and mobility and for subjective measures. P1752.2 started in early June 2021 with the goal of providing common data schemas for digital biomarkers related to cardiovascular, respiratory and metabolic measures.

Data and associated metadata complying to this standard are intended to be sufficiently clear and complete to support use of mHealth data for a broad set of consumer health, biomedical research, and patient-centred clinical care needs. The standard does not address the manner in which these schemas are transmitted, negotiated, encapsulated or any of the security or privacy approaches that could be required in order to create such transactions. The scope of IEEE 1752 is entirely delineated by the data elements as modelled by the given schemas.

Data schemas specify the format and payload of data. Systems often receive data from many different devices or platforms, with each source modelling and describing the data differently. It is much easier to process and make sense of data if all data points for a specific measure (e.g. total sleep time, kcal burned during physical activity) are expressed in a shared, common (standard) schema regardless of the source. In healthcare, common data schemas are particularly important because of the semantic importance and complexity of health data. Common schemas define the meaningful distinctions for each clinical measure and ensure consistency in how mHealth data is recorded, providing sufficient information to enable correct clinical interpretation of the data and thereby increasing the overall clinical utility of mHealth data and improving the ability of developers to quickly build clinically usable products.

#### **F.4.7 Mobile health standards**

HL7 has the Mobile Health Working Group which is focused on mobile health applications. This WG is working on a number of projects:

- HL7 Consumer Mobile Health Application Functional Framework (cMHAFF) – Guidance to health app developers (STU)<sup>20)</sup>
- HL7 Mobile Health Application Data Exchange (MHADE) – FHIR-based Exchange of data from devices to applications (FHIR IG)<sup>21)</sup>

---

20) <https://confluence.hl7.org/display/MH/cMHAFF+Project>

21) <https://confluence.hl7.org/display/MH/Mobile+Health+App+Data+Exchange+Project>

- HL7 PPS – Unique MH App Identifier – similar to device UDI [Also submitted to the ONC USCDI (Core Data for Interoperability)]. As part of this effort, IEEE is being considered as a registry for mobile health apps, creating an industry collaboration for certification of MH apps.<sup>22)</sup>

---

22) <https://confluence.hl7.org/display/MH/Mobile+Health+App+Data+Exchange+Project> ; <https://www.healthit.gov/isa/uscdi-data/unique-mobile-health-application-identifier-umhai> ; <https://confluence.hl7.org/display/MH/Unique+Mobile+Health+Application+Identifier+%28UMHAI%29+Project>



## **Annex G** **(informative)**

### **RCC-MH cybersecurity standards landscape**

#### **G.1 Cybersecurity related regulations and regulatory guidance**

The following regulations can be considered regarding health device cybersecurity from a regulatory perspective. This is not a complete list:

- US FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance
- US FDA: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions; Guidance for Industry and Food and Drug Administration Staff
- US FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
- US FDA: Design Considerations for Devices Intended for Home Use
- US FDA: Postmarket Management of Cybersecurity in Medical Devices
- US FDA: Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act - Draft Guidance for Industry and Food and Drug Administration Staff
- European Commission: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
- European Commission: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU
- Germany: Cyber Security Requirements for Network-Connected Medical Devices
- MDCG 2019-16 – Guidance on Cybersecurity for medical devices
- Germany (BSI) – Security requirements for eHealth applications Technical Guideline (BSI TR 03161)
- France – ANSM: Cybersecurity of medical devices integrating software during their life cycle
- Health Canada: Pre-market Requirements for Medical Device Cybersecurity
- Australia / TGA: Medical device cybersecurity guidance for industry
- Australia / TGA: Medical device cybersecurity information for users
- Singapore Standards Council Technical Reference 67: Medical device cybersecurity
- Japan: Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1
- Japan: Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1
- China: Medical Device Network Security Registration on Technical Review Guidance Principle
- IMDRF: Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL)
- IMDRF: Principles and Practices for the Cybersecurity of Legacy Medical Devices (IMDRF/CYBER WG/N70 FINAL)

- IMDRF: Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12
- IMDRF: Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices IMDRF/GRRP WG/N47 FINAL

## **G.2 Cybersecurity related standards**

### **G.2.1 General**

The following standards can be considered regarding health device cybersecurity. Additional standards to be considered can be found in [Annex C](#). This is not a complete list:

- IEC 62443-3-2, Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design
- IEC 62443-4-1, Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements
- IEC 81001-5-1, Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle
- IEC 80001-1, Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
- IEC/TR 80001-2-2, Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- IEC TR 80001-2-8, Application of risk management for IT-networks incorporating medical devices — Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
- ISO/TR 80001-2-7, Application of risk management for IT-networks incorporating medical devices — Application guidance — Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
- ISO/IEC 27000 series, Information technology — Security techniques — Information security management systems
- ISO/IEC 27035-1, Information technology — Information security incident management — Part 1: Principles and processes
- ISO/IEC 27035-2, Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure
- ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes
- ISO/TS 11633-1, Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis
- ISO/TR 11633-2, Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 2: Implementation of an information security management system (ISMS)

## **G.2.2 UL 2900 series**

### **G.2.2.1 Overview**

The UL 2900 series applies to a method of evaluating software for cybersecurity related issues and an organization's capability maturity to test a product's security controls against the stated requirements. It is written with the objective of supporting conformity assessment of products and organizations.

It consists of a base standard (UL 2900-1) and a number of vertical standards such as UL 2900-2-1 for healthcare.

#### **G.2.2.2 UL 2900-1**

UL 2900-1 applies to "network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware".

UL 2900-1 describes:

- a) requirements regarding the software developer (vendor or other supply chain member) risk management process for their product;
- b) methods to be used for evaluating and testing of products for the presence of vulnerabilities, software weaknesses and malware;
- c) requirements regarding the presence of security risk controls in the architecture and design of a product.

UL 2900-1 does not contain requirements regarding functional testing of a product. This means this standard contains no requirements to verify that the product functions as designed.

UL 2900-1 does not contain requirements regarding the hardware contained in a product.

#### **G.2.2.3 UL 2900-2-1**

The security evaluation standard applies to the testing of network connectable components of healthcare systems. It applies to, but is not limited to, the following key components:

- a) medical devices;
- b) accessories to medical devices;
- c) medical device data systems;
- d) in vitro diagnostic devices;
- e) health information technology;
- f) wellness devices;
- g) all software components used for the secure operation of the device, wherever they reside, including remote assets.

Note Combinations of the technologies listed here can be applied to such solutions as "telemedicine," where a single solution can contain both regulated and unregulated components.

## **G.2.3 AAMI TIR 57**

AAMI TIR 57 provides guidance on methods to perform information security risk management for a medical device in the context of the safety risk management process required by ISO 14971.

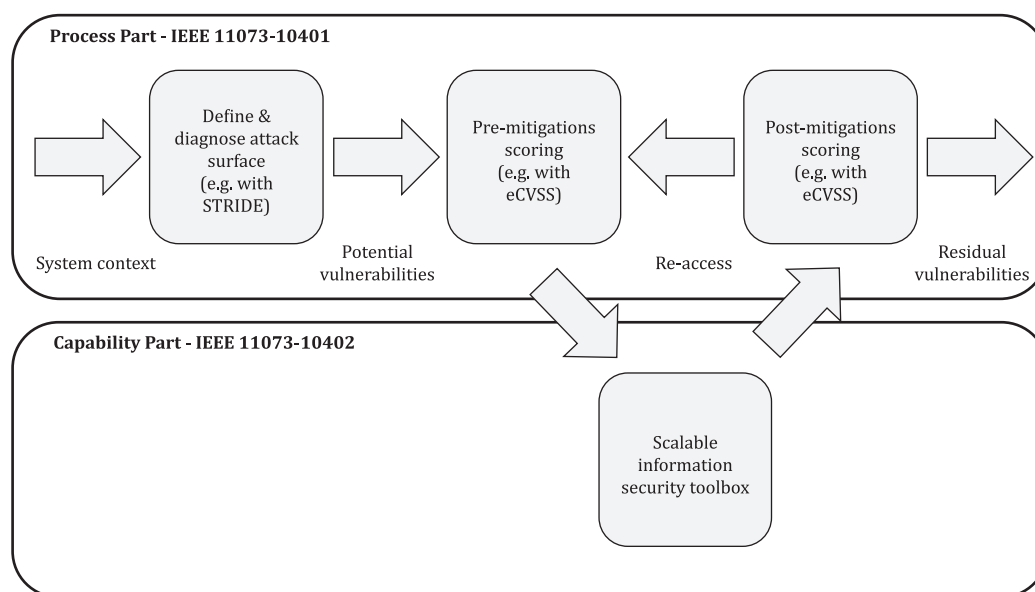
AAMI TIR 57 incorporates the expanded view of risk management from IEC 80001-1 by incorporating the same key properties of safety, effectiveness and data and systems security with annexes that provide process details and illustrative examples.

#### G.2.4 AAMI TIR 97

AAMI TIR 97 provides guidance on methods to perform postmarket security risk management for a medical device in the context of the safety risk management process required by ISO 14971. This TIR is intended to be used with AAMI TIR 57.

#### G.2.5 IEEE 11073 – Foundational cybersecurity standards

The ISO/IEEE 11073 PHDs/PoCDs family of standards, Bluetooth SIG profiles and services specifications, and the Continua Design Guidelines were developed to specifically address interoperability of PHDs/PoCDs. Within the context of secure interoperability, cybersecurity is the process and capability of preventing unauthorized access or modification, misuse, denial of use, or the unauthorized use of information that is stored on, accessed from, or transferred to and from a PHD/PoCD. The process part of cybersecurity is risk analysis of use cases specific to a PHD/PoCD. This is covered by the foundational IEEE 11073-40101 and depicted in the top row in [Figure G.1](#). The capability part of cybersecurity is information security controls related to both digital data and the relationships to safety and usability. This is covered by the foundational IEEE 11073-40102 and depicted in the bottom row in [Figure G.1](#).



**Figure G.1 — Scopes of IEEE 11073-10401 and IEEE 11073-10402**

The IEEE 11073-40101 defines an iterative, systematic, scalable, and auditable approach to identification of cybersecurity vulnerabilities and estimation of risk. This iterative vulnerability assessment uses the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme and the embedded Common Vulnerability Scoring System (eCVSS). The assessment includes system context, system decomposition, pre-mitigation scoring, mitigation, and post-mitigation scoring and iterates until the remaining vulnerabilities are reduced to an acceptable level of risk. The standard enables a common approach to vulnerability assessment based on threat modelling capable of analysing PHDs/PoCDs across domains. With that, the results of different manufacturers and different devices can be compared. It is the foundation to align the cybersecurity mitigation techniques for a multi-vendor system.

The IEEE 11073-40102 defines a security baseline of application layer cybersecurity mitigation techniques for certain use cases or for times when certain criteria are met. This standard provides a scalable information security toolbox appropriate for PHD/PoCD interfaces, which fulfils the intersection of requirements and recommendations from National Institute of Standards and Technology (NIST) and the European Network

and Information Security Agency (ENISA). This standard maps to the NIST cybersecurity framework, IEC TR 80001-2-2, and the STRIDE classification scheme. The mitigation techniques are based on the extended CIA triad and are described generally to allow to determine the most appropriate algorithms and implementations. Thus, this standard is transport-independent and can be directly used for manufacturer-specific implementations or translated into transport-dependent SDO or industry standards (e.g. Bluetooth SIG profile and service).

### **G.2.6 NIST/NCCOE**

The National Cybersecurity Center of Excellence (NCCoE) is a part of the Applied Cybersecurity Division of NIST's Information Technology Laboratory. It brings together members of private industry, government agencies, and academia to create practical, standards-based solutions that organizations of all types and sizes can use to protect their assets, people, and data.

Of particular interest to this document, the NCCoE has worked on a project called "Securing the Telehealth Remote Patient Monitoring Ecosystem". The project team created a representative RPM (Remote Patient Monitoring) ecosystem in the laboratory environment, performed a risk assessment and then applied the NIST Cybersecurity Framework and guidance based on medical device standards, collaborating with industry and public partners. This project demonstrated how an organization can implement a solution to enhance privacy and secure their telehealth RPM ecosystem.

As part of this project NIST released a set of supporting documents.<sup>23)</sup>

## **G.3 Addressing cybersecurity gaps**

### **G.3.1 Secure the device**

A systematic and scientifically sound approach to determining the required level of security for a given device is missing today. Methodologies should be established that device manufacturers can use to determine and implement the level of security required for a given device and based on:

- device risk class (safety, privacy, business risks);
- device use case;
- device use environment;
- device user capabilities;
- device lifecycle.

Device security capabilities suggested for inclusion are: desired security controls, fail safe mode, security event detection and logging, backup and restore capabilities, and updateability, as well as including a methodology to determine security requirements, implementation, and confirmation (through testing) that requirements are met.

### **G.3.2 Secure device communication**

A device shall be able to communicate securely, including technical, administrative, and clinical communication channels. As today's device integration environments are complex, secure communication cannot always rely on transport layer security features provided by subsegments of what is typically a complex data flow across multiple hops and network types. Ideally, device communication provides end-to-end cryptographic protection to assure confidentiality, integrity, and authenticity.

Types of communication paths to be considered include wireless or wired IP networks that can include, depending on device type and use case, home, public, or enterprise networks. Security measures that protect data in transit should consider the presence of 3<sup>rd</sup> party service providers (e.g. network operators, cloud service).

---

23) <https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem>

Supported communication streams include:

- clinical (e.g. HL7 or DICOM);
- administrative (e.g. service or billing related);
- technical (e.g. remote support, OTA software update).

As these data streams have different risk levels and characteristics, they should support their cryptographic protection through separate certificates so as to minimize the exposure of those certificates that support high-risk functions.

### **G.3.3 Secure manufacturing and distribution**

The development of standards and best practices is desired to prevent cyber compromise during the manufacturing and distribution process. This includes:

- secure manufacturing transfer;
- protection of software and firmware in the production environment;
- protection of the production IT ecosystem;
- provision and protection of security-specific ecosystem (e.g. PKI);
- protection and prevention of exposure of secret materials (certificates) during provisioning during production or at go-live;
- processes for transfer of software updates and phase-in into production and management of inventory;
- special considerations for 3<sup>rd</sup> party manufacturing (contract or off-the-shelf components containing software or firmware);
- protection of finished devices from cyber compromise.

### **G.3.4 Secure integration**

The development of standards and best practices is desirable to address protection of the device during go-live, assure integration of security features and functions (e.g. PKI), and assure environmental security features have been provided (e.g. firewalls).

Preferably, the go-live/deployment process provides positive feedback of success or clearly articulates failures.

### **G.3.5 Maintaining security**

Maintaining a device's security baseline is desirable during the useful life of a device. Ideally, this would include mitigation of newly discovered vulnerabilities or the implementation of new security control measures in response to new threats. Good security design minimizes the burden on the device operator, e.g. it minimizes the need for updates or patches. Preferably, if updates or patches need to be deployed, it is a remote process and providing for background installation.

### **G.3.6 Secure maintenance**

Any local or remote service should utilize roll-based-access control and, if needed, multi-factor authentication to protect high-privilege access. Preferably, remote access requires a secure channel (e.g. VPN) and all service activities to be logged.

### **G.3.7 Secure decommissioning**

Device decommissioning is typically a device operator function. This includes removal or all sensitive data (clinical, identifying information, user and network credentials). The device design should be such that easy

and reliable data removal can be performed by the device operator or user and that confirmation of data removal success or failure is provided.

### **G.3.8 Communication about security**

A device should communicate its security status and integrate with local or remote security management systems. This includes security documentation provided to the operator during procurement, but also ongoing updates of documentation and device security status information provided by interface query or on an event-by-event basis. This documentation includes:

- device-external security documentation;
- device version (incl. patch level);
- other relevant security properties;
- vulnerability communication and mitigation;
- version and update history (logs);
- security event detection and logging;
- security system integration and communication;
- device response to management queries (e.g. discovery or vulnerability scans);
- device support of external management systems (CMMS, risk or standards managers).



## **Annex H** **(informative)**

### **RCC-MH telehealth standards landscape**

#### **H.1 Standards**

##### **H.1.1 General**

There are a number of telehealth related standards that do not specifically deal with the communication issues related to telehealth but are more focused on quality and processes.

##### **H.1.2 ISO 13940**

ISO 13940 defines a system of concepts for different aspects of the provision of healthcare. To be able to represent both clinical content and clinical context, ISO 13940 is related to a generic healthcare/clinical process model as well as comprehensive concept definitions and concept models for the clinical, management and resource aspects of healthcare services.

In practice ISO 13940 covers the concept definitions needed whenever structured information in healthcare is specified as a requirement. The definitions are intended to refer to the conceptual level only and not to details of implementation. ISO 13940 covers all levels of specifications in the development of:

- logical reference models within the information viewpoint as a common basis for semantic interoperability on international, national or local levels;
- information systems;
- information for specified types of clinical processes.

##### **H.1.3 ISO 13131**

ISO 13131 provides processes that can be used to analyse the risks to the quality and safety of healthcare and continuity of care when telehealth services are used to support healthcare activities. Using risk management processes, quality objectives and procedures are derived which provide guidelines for the operations of telehealth services which include but are not limited to the following domains:

- management of telehealth quality processes by the healthcare organization;
- strategic and operational process management relating to regulations, knowledge management (best practice) and guidelines;
- healthcare processes relating to people such as healthcare activities, planning, and responsibilities;
- management of financial resources to support telehealth services;
- management of information management and security used in telehealth services;
- processes related to the planning and provision of human resources, infrastructure, facilities and technology resources for use by telehealth services.

ISO 13131 provides a set of example guidelines containing quality objectives and procedures for each domain. Organizations can apply the quality and risk management processes described to develop quality objectives and procedures appropriate to the telehealth services they provide.

ISO 13131 does not provide guidance for the manufacture, assembly, configuration, interoperability or management of devices, products or technical systems.

## **H.1.4 ISO/IEC 20001-1**

ISO/IEC 20001-1 specifies requirements for an organization to establish, implement, maintain and continually improve a service management system (SMS). The requirements specified in ISO/IEC 20001-1 include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value. ISO/IEC 20001-1 can be used by:

- a customer seeking services and requiring assurance regarding the quality of those services;
- a customer requiring a consistent approach to the service lifecycle by all its service providers, including those in a supply chain;
- an organization to demonstrate its capability for the planning, design, transition, delivery and improvement of services;
- an organization to monitor, measure and review its SMS and the services;
- an organization to improve the planning, design, transition, delivery and improvement of services through effective implementation and operation of an SMS;
- an organization or other party performing conformity assessments against the requirements specified in ISO/IEC 20001-1;
- a provider of training or advice in service management.

## **H.1.5 ISO 5477**

ISO 5477 provides business rules for public health emergency preparedness and response (PH EPR) information systems. It includes a description of the EPR information systems domain. It also includes an informative framework for mapping existing semantic interoperability standards for emergency preparedness and response to PH EPR information systems.

## **H.1.6 The international patient summary (IPS)**

While not specifically a telehealth standard, the IPS is a key tool for exchanging a basic set of clinical data of a patient which is specialty-agnostic, condition-independent but readily usable by all clinicians for unscheduled (cross-border) patient care.

A patient summary is a standardized set of basic clinical data that includes the most important health and care related facts required to ensure safe and secure healthcare. This summarized version of the patient's clinical data gives health professionals the essential information they need to provide care in the case of an unexpected or unscheduled medical situation (e.g. emergency or accident). While this data is mainly intended to aid health professionals in providing unscheduled care, it can also be used to provide planned medical care, e.g. in the case of citizen movements or cross-organizational care paths, or even as a crystallization point for health records.<sup>24)</sup>

In order to improve the interoperability and implementation consistency of the IPS, IHE (Integrating the Healthcare Enterprise) has developed a profile of the IPS and has also promoted implementation testing at international Connectathons.

---

24) <https://international-patient-summary.net/>

## Annex I (informative)

### Device specializations

In addition to general requirements that apply to all devices, the IEEE has developed, or is in the process of developing, specific guidelines for specific types of devices (see [Tables I.1](#) and [I.2](#)). These standards provide further guidance for specific types of devices in order to reduce the amount of interpretation of the standards and to increase interoperability.

**Table I.1 — IEEE 11073 personal health device (PHD) published device specializations**

Document	Device type
IEEE 11073-10404	Pulse Oximeter
IEEE 11073-10406	Basic Electrocardiograph (1- to 3-lead ECG)
IEEE 11073-10407	Blood Pressure Monitor
IEEE 11073-10408	Thermometer
IEEE 11073-10415	Weighing scale
IEEE 11073-10417	Glucose Meter
IEEE 11073-10418	International Normalized Ratio (INR) monitor
IEEE 11073-10419	Insulin Pump
IEEE 11073-10420	Body Composition Analyzer
IEEE 11073-10421	Peak expiratory flow monitor (peak flow)
IEEE 11073-10422	Urine Analyzer
IEEE 11073-10424	Sleep Apnoea Breathing Therapy Equipment (SABTE)
IEEE 11073-10425	Continuous Glucose Monitor (CGM)
IEEE 11073-10426	Home Healthcare Environment Ventilator
IEEE 11073-10427	Power Status Monitor of Personal Health Devices
IEEE 11073-10428	Electronic Stethoscope
IEEE 11073-10429	Spirometry
IEEE 11073-10441	Cardiovascular fitness and activity monitor
IEEE 11073-10442	Strength Fitness Equipment
IEEE 11073-10471	Independent Living Activity Hub
IEEE 11073-10472	Medication monitor

**Table I.2 — IEEE 11073 point-of-care device (PoCD) planned device specializations**

Document	Device type
IEEE 11073-10721	HF Device
IEEE 11073-10722	Endo Camera
IEEE 11073-10723	Endo Light
IEEE 11073-10724	Insufflator
IEEE 11073-10725	Endo Pump
IEEE 11073-10726	Ventilator
IEEE 11073-10727	Infusion Device
IEEE 11073-10728	Physio Monitor
IEEE 11073-10729	Anesthesia System

## Annex J (informative)

### Summary of applicable standards

[Table J.1](#) lists many of the most important standards and technical guidance relevant to the field of RCC-MH.

NOTE [Table J.1](#) list is not exhaustive.

**Table J.1 — Documents applicable to RCC-MH**

Classification	Standard	Description
Risk management	ISO 14971	Medical Devices — Application of Risk Management to Medical Devices
	ISO/TR 24971	Medical devices — Guidance on the application of ISO 14971
Development process	IEC 62304:2006+A1:2015	Medical Device Software — Software Life Cycle Processes
	IEC 82304-1 ISO/TS 82304-2	Health Software — Part 1: General Requirements for Product Safety Health Software — Part 2: Health and wellness apps — Quality and Reliability
	ISO 13485	Medical devices — Quality management systems — Requirements for regulatory purposes
	IEC 62366-1	Medical devices — Part 1: Application of usability engineering to medical devices
Device-to-device interoperability	ISO/IEEE 11073 series	1010x series: Nomenclature 1020x series: Information Models 104xx series: Personal Health Device Specializations 107xx series: Requirements for Participants in SDC Systems 4010x series: Cybersecurity
	IEEE/UL 2933	Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS - Trust, Identity, Privacy, Protection, Safety, Security
	AAMI 2700 Series ANSI/AAMI 2700-1 ANSI/AAMI 2700-2-1	Medical Devices and Medical Systems – Essential Safety and Performance Requirements for Equipment Comprising the Patient-Centric Integrated Clinical Environment (ICE) – Part 1: General Requirements and Conceptual Model Part 2-1: Particular requirements for Forensic Data logging
	ANSI/AAMI/UL 2800-1	Standard For Safety for Medical Device Interoperability

**Table J.1 (continued)**

Classification	Standard	Description
Device to healthcare enterprise interoperability	IHE DEV Domain PCD Profiles PCH Profiles DPI Profile	Related to Point of Care Device to Enterprise Communication Related to Personal Connected Health to Ent. Communication Related to Device-to-Device PoC Integration
	HL7 v2	Specific areas of interest in the HL7 standard are related to: Patient Demographics Observations and Results
	HL7 Mobile Health	Specific working group within HL7 that focuses on Mobile Health related User Guides.
	HL7 FHIR	Specific resources of interest in the HL7 FHIR standard include: Patient Resource Device Resource
	DICOM Series	Digital Imaging and Communications in Medicine <a href="https://www.dicomstandard.org/current/">https://www.dicomstandard.org/current/</a>
	ISO 5477	Health informatics – Interoperability of public health emergency preparedness and response information systems
Device cybersecurity	ANSI/CAN/UL 2900 Series UL 2900-1 UL 2900-2-1	Standard for Software Cybersecurity for Network Connectable Products Part 1: General Requirements Part 2-2: Particular Requirements for Network Connectable Healthcare and Wellness Systems
	ISO/IEEE 11073-40101 ISO/IEEE 11073-40102	Foundational--Cybersecurity--Processes for vulnerability assessment Foundational--Cybersecurity--Capabilities for mitigation
	AAMI SW96	Standard for Medical Device Security - Security risk management for device manufacturers
	AAMI TIR57 AAMI TIR75 AAMI TIR 97	Principle for medical device security – Risk management Factors to consider when multi-vendor devices interact via an electronic interface: Practical applications and examples Principles for medical device security – Postmarket risk management for device manufacturers

**Table J.1** *(continued)*

Classification	Standard	Description
Healthcare enterprise deployment	ISO/IEC 80001 series (Guidance)	<p>Application of risk management for IT-networks incorporating medical devices —</p> <ul style="list-style-type: none"> <li>a) Part 1: Roles, responsibilities and activities</li> <li>b) Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples</li> <li>c) Part 2-2: Guidance for the communication of medical device security needs, risks and controls</li> <li>d) Part 2-3: Guidance for wireless networks</li> <li>e) Part 2-4: General implementation guidance for healthcare delivery organizations</li> <li>f) Part 2-5: Application guidance — Guidance for distributed alarm systems</li> <li>g) Part 2-6: Application guidance — Guidance for responsibility agreements</li> <li>h) Part 2-7: Guidance for HDOs on how to self-assess their conformance with IEC 80001-1</li> <li>i) Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2</li> <li>j) Part 2-9: Application guidance — Guidance for use of security assurance cases to demonstrate confidence in 80001-2-2 security capabilities</li> </ul>
	ISO/IEC 81001 series	<p>Health software and health IT systems safety, effectiveness and security</p> <p>Part 1: Principles and concepts (FDIS)</p> <p>Part 5-1: Security — Activities in the product life cycle (DIS)</p>

## Annex K (informative)

### Care delivery locations

[Table K.1](#) provides a non-exhaustive list of care delivery locations aligned with the locations of care described in this document. It can be useful when looking at [Figures 1, 2](#) and [B.1](#), as well as [5.2](#).

**Table K.1 — Care delivery locations for different types of care**

Type of care	Care delivery locations
Home and community care	Homeless Shelter Facility
	Home
	Accredited Social Health Activist (ASHA) Home Care
	Group Home
	Temporary Lodging
	Residential Substance Abuse Facility
	Psychiatric Residential Treatment Centre
Outpatient care	Pharmacy
	Telehealth Facility
	School
	Prison/Correctional Facility
	Provider Office
	Assisted Living Facility
	Mobile Unit
	Walk-in Retail Health Clinic
	Place of Employment
	Urgent Care Facility
	Independent Clinic
	Health Centre
	Mental Health Centre
	Substance Abuse Treatment Facility
	Mass Immunization Centre
	Outpatient Rehabilitation Facility
	Public Health Clinic
	Outpatient Hospital
	Ambulatory Surgical Centre
	Birthing Centre
	Military Treatment Facility



**Table K.1** *(continued)*

Type of care	Care delivery locations
Post-acute care	Nursing Facility
	Anganwadi Centre
	Custodial Care Facility
	Ambulance
	Inpatient Psychiatric Facility
	Intermediate Care Facility
	Hospice
	Skilled Nursing Facility (SNF)
	Psychiatric Facility - Partial Hospitalization
	End-Stage Renal Disease Treatment Facility
	Long-Term Acute Care Facility (LTAC)
Hospital care	Inpatient Rehabilitation Facility
	Inpatient Hospital
	ER – Hospital

## **Annex L** **(informative)**

### **Conformance landscape**

#### **L.1 Verification**

Verification is the process of assuring that what was specified was actually implemented. In most cases this means creating traceability between the product requirements and the product tests. Verification is typically an in-vitro task with the testing being done by the manufacturer in a controlled environment against a set of test scripts.

#### **L.2 Validation**

Validation is the process of assuring that the product will actually work under real-life situations. Validation is typically done in the real environment or in a simulated real environment by typical users of the device. Real-world, in-vivo experience with the device is critical to evaluate human factors and usability issues that would not necessarily be discovered in the manufacturer's test lab.

A good analogue is the testing of vaccines. The vaccines are developed in a lab environment where they can be verified to be effective when tested in this lab environment against test viruses or in human proxies such as mice or monkeys. However, they should also be tested against human subjects to make sure that they are safe and effective, that is, that there are no undiscovered side effects and that they also protect real humans from infection.

#### **L.3 Conformity assessment**

Conformity assessment can be defined as a demonstration, whether directly or indirectly, that specified requirements relating to a product, process, system, person, or body are fulfilled. It includes sampling and testing, inspection, supplier's declaration of conformity, certification, and management system assessment and registration.<sup>25)</sup>

There are many types of testing including testing for performance, robustness, behaviour, functions and interoperability. Although conformity assessment can include some of these kinds of tests, it has one fundamental difference — the requirements or criteria for conformance are specified in the standard or specification. Ideally, this is usually in a conformance clause or conformance statement, but sometimes some of the criteria can be found in the body of the specification typically in the form of a 'should' or 'shall' statement. Some standards have subsequent documentation for the test methodology and assertions to be tested. If the criteria or requirements for conformance are not specified, there can be no conformance testing.<sup>26)</sup>

The US based National Institute of Standards and Test (NIST) has had a large role in developing test tools for a number of health IT organizations including the CDC and many of the IHE DEV domain profiles. In the latter case, NIST has developed testing for the IHE DEC, ACM and other profiles that are used as both pre-Connectathon and Connectathon test suites.

#### **L.4 Accredited test labs**

These are 3<sup>rd</sup> party testing organizations which will test a product and provide a conformity test report. These labs usually need to certify that they meet the requirements in ISO/IEC 17025. Accredited test labs for

25) <https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf>

26) Adapted from: <https://www.nist.gov/itl/ssd/information-systems-group/conformance-testing>

medical devices usually focus on electrical safety, EMC/RFI testing, bio-compatibility testing, etc. However, in the context of RCC-MH it is possible to envision accredited test labs providing interoperability testing to verify that a device or system has properly implemented a specific interoperability protocol.

The use of accredited test labs for interoperability testing could be a key to accelerating regulatory clearance and acceptance of devices by stakeholders especially if there is an accompanying certificate of compliance. This has been critical to the acceptance of various technologies such as Bluetooth and Wi-Fi.

In the US the voluntary FDA ASCA Program<sup>27)</sup>, based on NIST/NTTAA, is an accreditation scheme that capitalizes upon the increasingly prominent role that standards play in regulatory science and practice. ASCA's goals are to:

- streamline conformity assessment in device submissions;
- enhance the FDA's confidence in test methods and results;
- decrease the need for additional information related to conformance with a standard;
- promote consistency, predictability, and efficiency in medical device review;
- serve as a least burdensome approach to conformity assessment.

ASCA includes participation from accreditation bodies, testing laboratories, device manufacturers and FDA staff. Under the ASCA program, the FDA grants ASCA Recognition to qualified accreditation bodies to accredit testing laboratories to perform premarket testing for medical device companies. The FDA grants ASCA Accreditation to qualified testing laboratories, relying on international conformity assessment standards and a set of FDA-identified ASCA program specifications. A device manufacturer can choose to use an ASCA-accredited testing laboratory to conduct testing for premarket submissions to the FDA.

---

<sup>27)</sup> <https://www.fda.gov/medical-devices/standards-and-conformity-assessment-program/accreditation-scheme-conformity-assessment-asca>

## Bibliography

- [1] ISO 5477:2023, *Health informatics — Interoperability of public health emergency preparedness and response information systems*
- [2] ISO/TS 13131:2021, *Health informatics — Telehealth services — Quality planning guidelines*
- [3] ISO 13485, *Medical devices — Quality management systems — Requirements for regulatory purposes*
- [4] ISO 13940, *Health informatics — System of concepts to support continuity of care*
- [5] ISO 14971, *Medical devices — Application of risk management to medical devices*
- [6] ISO/TR 16056-2:2004, *Health informatics — Interoperability of telehealth systems and networks — Part 2: Real-time systems*
- [7] ISO 19223, *Lung ventilators and related equipment — Vocabulary and semantics*
- [8] ISO 23903, *Health informatics — Interoperability and integration reference architecture — Model and framework*
- [9] ISO/DTR 24306, *Guidance on the security requirements for gateways used in personal health care system*<sup>28)</sup>
- [10] ISO/TR 24971, *Medical devices — Guidance on the application of ISO 14971*
- [11] ISO 31000, *Risk management — Guidelines*
- [12] ISO/TS 82304-2:2021, *Health software — Part 2: Health and wellness apps — Quality and reliability*
- [13] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*
- [14] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*
- [15] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*
- [16] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*
- [17] ISO/IEC 20001-1, *Information technology — Service management — Part 1: Service management system requirements*
- [18] ISO/IEC 27000, *Information security management*
- [19] ISO/IEC 80001 (all parts), *Application of risk management for IT-networks incorporating medical devices*
- [20] ISO/IEC 80601 (all parts), *Medical electrical equipment*
- [21] IEC 60601 (all parts), *Medical electrical equipment*
- [22] IEC 62304:2006+AMD1:2015, *Medical device software — Software life cycle processes*
- [23] IEC 62366-1, *Medical devices — Part 1: Application of usability engineering to medical devices*
- [24] IEC 82304-1, *Health software — Part 1: General requirements for product safety*
- [25] ISO/IEEE 11073 (all parts), *Health informatics*
- [26] IEEE Std 610.7-1995, *IEEE Standard Glossary of Computer Networking Terminology*
- [27] IEEE Std 610-1990, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*

---

<sup>28)</sup> Under development.

- [28] IEEE 1752, *IEEE Standard for Open Mobile Health Data*
- [29] IEEE/UL 2933, *IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security*
- [30] AAMI TIR 67:2016, *Principles for Medical Devices Security - Risk Management*
- [31] AAMI TIR 97:2019, *Principles for Medical Devices Security - Postmarket Risk Management for Device Manufacturers*
- [32] AAMI 2700 (all parts), *Medical Devices and Medical Systems*
- [33] ANSI/AAMI/UL 2800 (all parts), *Standard for Safety for Medical Device Interoperability*
- [34] BSI TR 03161, *Security requirements for eHealth applications*
- [35] UL 2900, *Standard for Software Cybersecurity for Network Connectable Products*
- [36] IMDRF SaMD Working Group, *Software as a Medical Device (SaMD): Key Definitions*, 2013
- [37] Centers for Disease Control and Prevention, *Using Telehealth to Expand Access to Essential Health Services during the COVID-19 Pandemic*, June 10, 2020
- [38] De Georgia M. A., Kaffashi F., Jacono F. J. & Loparo K. A. *Information Technology in Critical Care: Review of Monitoring and Data Acquisition Systems for Patient Care and Research*, NIH National Library of Medicine, February 4, 2015. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4334936/>
- [39] RATHS D. CMS Expands Hospital-at-Home Program, Nov. 25, 2020 <https://www.hcinnovationgroup.com/population-health-management/remote-patient-monitoring-rpm/news/21164286/cms-expands-hospitalathome-program>
- [40] Coravos, A., Doerr, M., Goldsack, J. et al. Modernizing and designing evaluation frameworks for connected sensor technologies in medicine. *npj Digit. Med.* 3, 37 (2020). <https://www.nature.com/articles/s41746-020-0237-3>
- [41] Hale C. Philips sees medtech sales drop, connected care demand rise in the face of COVID-19, *Fierce Biotech*, 20 July, 2020. [https://www.fiercebiotech.com/medtech/philips-sees-medtech-sales-drop-connected-care-demand-rise-face-covid-19?mkt\\_tok=eyJpIjoiWW1NeE1EVTVOalF4TldKayIsInQiOiJaKzd2b2ZJRGVKR0tSRmxCeWZHUUNEVFVhXC9pY2tWUnVCWWtqTjU1MXNhVmpQOE0rNVp2Vm1mNFBLTDg1bXRIMjFGM1Y1R21HTnVzVGorcm9iNzJYSVRJMMmRuYXRyTTMxeEdubzNHZHRKRGIaA0aGxnWjh4VHJIREJVTmNyQ0cifQ%3D%3D&mrkid=4515100](https://www.fiercebiotech.com/medtech/philips-sees-medtech-sales-drop-connected-care-demand-rise-face-covid-19?mkt_tok=eyJpIjoiWW1NeE1EVTVOalF4TldKayIsInQiOiJaKzd2b2ZJRGVKR0tSRmxCeWZHUUNEVFVhXC9pY2tWUnVCWWtqTjU1MXNhVmpQOE0rNVp2Vm1mNFBLTDg1bXRIMjFGM1Y1R21HTnVzVGorcm9iNzJYSVRJMMmRuYXRyTTMxeEdubzNHZHRKRGIaA0aGxnWjh4VHJIREJVTmNyQ0cifQ%3D%3D&mrkid=4515100)
- [42] Wicklund E., VA, DoD Launch National Telehealth Projects for Critical Care, *mHealth Intelligence*, 09 July 2020 <https://mhealthintelligence.com.cdn.ampproject.org/c/s/mhealthintelligence.com/news/amp/va-dod-launch-national-telehealth-projects-for-critical-care>
- [43] Wicklind E., *The Promise and Potential for Telehealth in Home Health*, *mHealth Intelligence*, 10 July, 2020 <https://mhealthintelligence.com/features/the-promise-and-potential-for-telehealth-in-home-health>
- [44] US Government, Office of the National Coordinator for Health IT US Government Interoperability Standards Advisory, <https://www.healthit.gov/isa/sites/isa/files/inline-files/2020-ISA-Reference-Edition.pdf>
- [45] US Government, Office of the National Coordinator for Health IT US Government Interoperability Standards Advisory, *United State Core Data for Interoperability (USCDI)* <https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi>
- [46] US Government, Office of the National Coordinator for Health IT US Government Interoperability Standards Advisory, *US Government, Vocabulary/Code Set for COVID-19 Novel Coronavirus Pandemic* <https://www.healthit.gov/isa/covid-19>

- [47] Watson A., Wah R. & Thamman R. The Value of Remote Monitoring for the COVID-19 Pandemic, Telemedicine and e-Health, Vol. 26, No. 9, 10 September, 2020 <https://www.liebertpub.com/doi/10.1089/TMJ.2020.0134>
- [48] Siwicki B. EPIC and Kids Telehealth, Healthcare IT News, July 14, 2020 <https://www.healthcareitnews.com/news/using-zoom-epic-bring-telehealth-kids-during-covid-19>
- [49] Government of Australia, Department of Health Therapeutic Goods Administration, Actual and potential harm caused by medical software, July 2020 <https://www.tga.gov.au/sites/default/files/actual-and-potential-harm-caused-medical-software.pdf>
- [50] Brazelton, T. Telemedicine and COVID-19, Fierce Healthcare, July 8, 2020 <https://www.fiercehealthcare.com/tech/industry-voices-telemedicine-and-connection-time-covid-19>
- [51] Monitoring at Home (HumanFirst) <https://www.gohumanfirst.com/>
- [52] Digital Medicine Society (DiMe) <https://www.dimesociety.org/index.php/about-us-main/defining-digital-medicine>
- [53] HIMSS Interoperability in Healthcare, HIMSS <https://www.himss.org/what-interoperability>
- [54] FDA Enforcement Policy for Digital Health Devices for Treating Psychiatric Disorders During the Coronavirus Disease (COVID-19) Public Health Emergency, April 2020 Digital Health Devices For Treating Psychiatric Disorders
- [55] FDA Enforcement Policy for Remote Ophthalmic Assessment and Monitoring Devices During the Coronavirus Disease (COVID-19) Public Health Emergency, April 2020 Remote Ophthalmic Assessment and Monitoring Devices
- [56] FDA Enforcement Policy for Non-Invasive Fetal and Maternal Monitoring Devices During the Coronavirus Disease (COVID-19) Public Health Emergency, April 2020 Non-Invasive Fetal and Maternal Monitoring Devices
- [57] HL7, Overview of the HL7 FHIR interoperability standard <https://www.hl7.org/fhir/overview.html>
- [58] Wikipedia Overview of the IEEE/11073 interoperability standards [https://en.wikipedia.org/wiki/ISO/IEEE\\_11073](https://en.wikipedia.org/wiki/ISO/IEEE_11073)
- [59] OrNET E.V. IEEE 11073 Service-oriented device connectivity (SDC) standards <https://ornet.org/en/>
- [60] AAMI MEDICAL DEVICE INTEROPERABILITY. A Safer Path Forward, 2012 [https://www.aami.org/docs/default-source/reports/2012\\_interoperability\\_summit\\_report.pdf](https://www.aami.org/docs/default-source/reports/2012_interoperability_summit_report.pdf)
- [61] SHIELD – Standardization of lab Data to Enhance Patient-Centered Outcomes Research and Value-Based Care, US Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (ASPE) <https://aspe.hhs.gov/shield-standardization-lab-data-enhance-patient-centered-outcomes-research-and-value-based-care>
- [62] Gopalan Y. The Future of Telemedicine Devices Is Cloud & IoMT-Driven, Entrepreneur India, July 1, 2020 [www.entrepreneur.com/article/352668](http://www.entrepreneur.com/article/352668)
- [63] Koh D. MOH deploys Biofourmis' remote monitoring platform for COVID-19 patients in Singapore, Healthcare IT News, July 30, 2020 <https://www.healthcareitnews.com/news/asia-pacific/moh-deploys-biofourmis-remote-monitoring-platform-covid-19-patients-singapore>
- [64] Siwicki B. United Methodist Communities has early successes with telehealth and RPM, Healthcare IT News, October 28, 2020 <https://www.healthcareitnews.com/news/united-methodist-communities-has-early-successes-telehealth-and-rpm>
- [65] Wolfberg A., Bogdanovics E. Role of Continuous Glucose Data in Remote Patient Monitoring, Dexcom, [www.ModernHealthcare.com/ContinuousGlucoseDataSlides](http://www.ModernHealthcare.com/ContinuousGlucoseDataSlides).



- [66] CROTTI N. Abbott launches real-time remote neuromodulation tech, Medical Design and Outsourcing, March 8, 2021 <https://www.medicaldesignandoutsourcing.com/abbott-launches-real-time-remote-neuromodulation-tech/>
- [67] Miliard M. How health systems should be preparing now for the future of hospital at home, Healthcare IT News, March 23, 2021 <https://www.healthcareitnews.com/news/how-health-systems-should-be-preparing-now-future-hospital-home>
- [68] Schwartz BN, Klein JH, Barbosa MB, Hamersley SL, Hickey KW, Ahmadzia HK, Broth RE, Pinckert TL, Sable CA, Donofrio MT & Krishnan A. Expanding Access to Fetal Telecardiology During the COVID-19 Pandemic, Telemed J E Health. 2021 Nov;27(11):1235-1240. doi: 10.1089/tmj.2020.0508. Epub 2021 Jan 29. PMID: 33513044. <https://pubmed.ncbi.nlm.nih.gov/33513044/>
- [69] SCHENCKER L. Hospitalization at Home? Some Illinois hospitals are giving it a try. Medical Xpress, June 9, 2022 <https://medicalxpress-com.cdn.ampproject.org/c/s/medicalxpress.com/news/2022-06-hospitalization-home-illinois-hospitals.amp>
- [70] RATHS D. Scaling Up the Home Hospital Program at Brigham and Women's, Healthcare Innovation, de. 21, 2020 [https://www.hcinnovationgroup.com/population-health-management/remote-patient-monitoring-rpm/article/21203470/scaling-up-the-home-hospital-program-at-brigham-and-womens?utm\\_source=HI+Daily+NL&utm\\_medium=email&utm\\_campaign=CPS201221061&o\\_eid=9875H9243956D8S&rdx.ident\[pull\]=omeda|9875H9243956D8S&oly\\_enc\\_id=9875H9243956D8S](https://www.hcinnovationgroup.com/population-health-management/remote-patient-monitoring-rpm/article/21203470/scaling-up-the-home-hospital-program-at-brigham-and-womens?utm_source=HI+Daily+NL&utm_medium=email&utm_campaign=CPS201221061&o_eid=9875H9243956D8S&rdx.ident[pull]=omeda|9875H9243956D8S&oly_enc_id=9875H9243956D8S)
- [71] Kadakia K., Patel B. & Shah A. Advancing digital health: FDA innovation during COVID-19 npj Digital Medicine, 17 December, 2020 <https://www.nature.com/articles/s41746-020-00371-7>
- [72] U.S. Food & Drug Administration Digital Health Policies and Public Health Solutions for COVID-19, April 28, 2022 <https://content.govdelivery.com/accounts/USFDA/bulletins/31550af>
- [73] U.S. FOOD & DRUG ADMINISTRATION. Design Consideration and Pre-Market Submission Recommendations for Interoperable Medical Devices, September 6, 2017 <https://www.fda.gov/media/95636/download>
- [74] US General Accounting Office - Telehealth and Remote Patient Monitoring Use in Medicare and Selected Federal Programs <https://www.gao.gov/assets/gao-17-365.pdf>
- [75] <https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/standards-and-conformity-assessment-program>
- [76] <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-181105-optimizing-standards-n51.pdf>
- [77] <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/appropriate-use-voluntary-consensus-standards-premarket-submissions-medical-devices>







**ICS 35.240.80**

Price based on 92 pages