FINAL DRAFT

INTERNATIONAL STANDARD

# IEC/FDIS 80001-1

ISO/TC **215**

Secretariat: ANSI

Voting begins on:
**2021-02-12**

Voting terminates on:
**2021-04-09**

## Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software —

## Part 1: Application of risk management

Member bodies are requested to consult relevant national interests in IEC/SC 62A before casting their ballot to the e-Balloting application.

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.

Reference number
IEC/FDIS 80001-1:2021(E)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

___________

# SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE –

## Part 1: Application of risk management

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard IEC 80001-1 has been prepared by a Joint Working Group of Subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC Technical Committee 62: Electrical equipment in medical practice, and of ISO Technical Committee 215: Health informatics.

It is published as a double logo standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) structure changed to better align with ISO 31000;

b) establishment of requirements for an ORGANIZATION in the application of RISK MANAGEMENT;

c) communication of the value, intention and purpose of RISK MANAGEMENT through principles that support preservation of the KEY PROPERTIES during the implementation and use of connected HEALTH SOFTWARE and/or HEALTH IT SYSTEMS.

The text of this document is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 62A/XX/FDIS | 62A/XX/RVD |

Full information on the voting for the approval of this document can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

In this document, the following print types are used:

- requirements and definitions: roman type;
- *test specifications: italic type*;
- informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type;
- TERMS DEFINED IN CLAUSE 3 OF THIS DOCUMENT OR AS NOTED ARE PRINTED IN SMALL CAPITALS.

In referring to the structure of this document, the term

- “clause” means one of the five numbered divisions within the table of contents, inclusive of all subdivisions (e.g. Clause 5 includes subclauses 5.1, 5.2, etc.);
- “subclause” means a numbered subdivision of a clause (e.g. 5.1, 5.2 and 5.3 are all subclauses of Clause 5).

References to clauses within this document are preceded by the term “Clause” followed by the clause number. References to subclauses within this particular standard are by number only.

In this document, the conjunctive “or” is used as an “inclusive or” so a statement is true if any combination of the conditions is true.

The verbal forms used in this document conform to usage described in Clause 7 of the ISO/IEC Directives, Part 2. For the purposes of this document, the auxiliary verb:

- “shall” means that compliance with a requirement or a test is mandatory for compliance with this document;
- “should” means that compliance with a requirement or a test is recommended but is not mandatory for compliance with this document;
- “may” is used to describe a permissible way to achieve compliance with a requirement or test.

A list of all parts of the IEC 80001 series, published under the general title *Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software,* can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this standard will remain unchanged until the stability date indicated on the IEC website under "https://webstore.iec.ch" in the data related to the specific standard. At this date, the standard will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

**IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

# INTRODUCTION

HEALTHCARE DELIVERY ORGANIZATIONS rely on safe, effective and secure systems as business-critical factors. However, ineffective management of the implementation and use of connected systems can threaten the ability to deliver health services.

Connected systems that deliver health services, generally involve multiple software applications, various medical devices and complex HEALTH IT SYSTEMS that rely upon shared infrastructure including wired or wireless networks, point to point connections, application servers and data storage, interface engines, security and performance management software, etc. These HEALTH IT INFRASTRUCTURES are often used for both clinical (e.g. patient monitoring systems) and non-clinical organizational functions (e.g. accounting, scheduling, social networking, multimedia, file sharing). These connected systems can involve small departmental networks to large integrated infrastructures spanning multiple locations as well as cloud-based services operated by third parties. The requirements in this document are intended for multiple stakeholders involved in the application of RISK MANAGEMENT to systems that include HEALTH IT SYSTEMS and / or HEALTH IT INFRASTRUCTURE.

Within the context of ISO 81001-1, this document covers the generic lifecycle phase “implementation and clinical use” (see the lifecycle diagram in Figure 1).

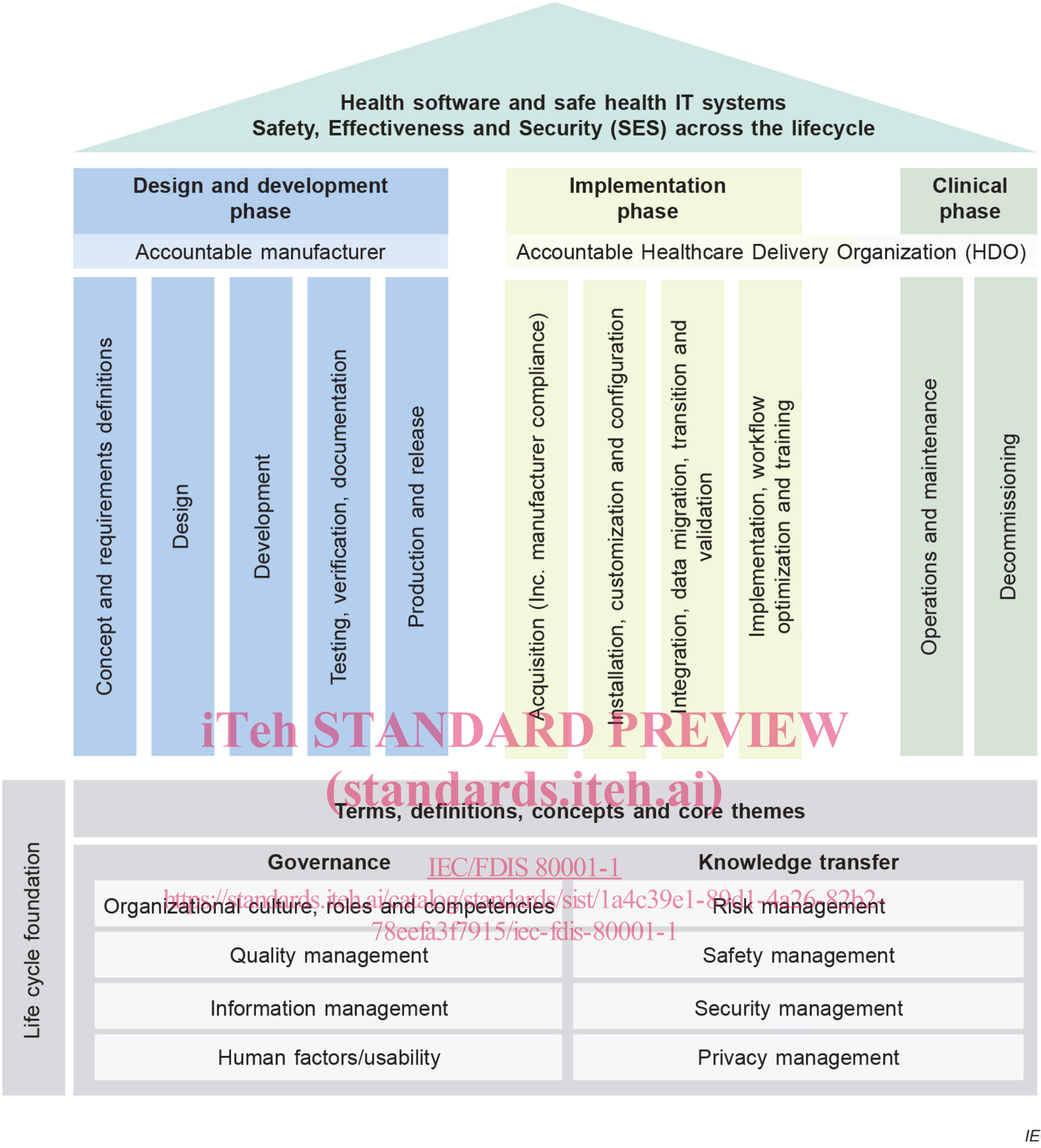
Health software and safe health IT systems
Safety, Effectiveness and Security (SES) across the lifecycle
Design and development phase
Implementation phase
Clinical phase
Accountable manufacturer
Accountable Healthcare Delivery Organization (HDO)
Concept and requirements definitions
Design
Development
Testing, verification, documentation
Production and release
Acquisition (Inc. manufacturer compliance)
Installation, customization and configuration
Integration, data migration, transition and validation
Implementation, workflow optimization and training
Operations and maintenance
Decommissioning
Life cycle foundation
Terms, definitions, concepts and core themes
Governance
Knowledge transfer
Organizational culture, roles and competencies
Risk management
Quality management
Safety management
Information management
Security management
Human factors/usability
Privacy management
IEC

**Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health IT software and health IT systems**

This document facilitates ORGANIZATIONS in using or adapting existing work practices and processes, personnel and tools wherever practicable to address the requirements of this document. For example, if an organization has an existing RISK MANAGEMENT PROCESS, this can be used or adapted to support the three KEY PROPERTIES of SAFETY, EFFECTIVENESS, and SECURITY. Requirements are defined such that they can be evaluated and as such support an ORGANIZATION in verifying and demonstrating the degree of compliance with this document.

The RISK MANAGEMENT requirements of this document are based upon existing concepts adapted and extended for use by all stakeholders supporting implementation and clinical use of connected HEALTH SOFTWARE and HEALTH IT SYSTEMS (including medical devices). This document aligns with ISO 81001-1, ISO Guide 63, IEC Guide 120.

# SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE –

# Part 1: Application of risk management

## 1 Scope

This document specifies general requirements for ORGANIZATIONS in the application of RISK MANAGEMENT before, during and after the connection of a HEALTH IT SYSTEM within a HEALTH IT INFRASTRUCTURE, by addressing the KEY PROPERTIES of SAFETY, EFFECTIVENESS and SECURITY whilst engaging appropriate stakeholders.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

## 3 Terms and definitions

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

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

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

NOTE With the exception of the terms and definitions listed in this clause, all terms and definitions used in this standard are taken from ISO 81001-1:20—.

### 3.1
**CONSEQUENCE**
outcome of an event affecting objectives

Note 1 to entry: A CONSEQUENCE can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: CONSEQUENCES can be expressed qualitatively or quantitatively.

Note 3 to entry: Any CONSEQUENCE can escalate through cascading and cumulative effects.

[SOURCE:ISO 31000:2018, 3.6]

**3.2**
**HEALTHCARE**
care activities, services, management or supplies related to the health of an individual or population

Note 1 to entry: This includes more than performing procedures for subjects of care. It includes, for example, the management of information about patients, health status and relations within the HEALTHCARE delivery framework and may also include the management of clinical knowledge.

[SOURCE: ISO 13940:2015, 3.1.1, modified – The definition was reworded to include population.]

**3.3**
**INCIDENT**
unplanned interruption to a service a reduction in the quality of a service or an event that has not yet impacted the service to the customer or user

[SOURCE: ISO/IEC 20000-1:2018, 3.2.5]

**3.4**
**INITIAL RISK**
RISK derived during risk estimation taking into consideration any retained RISK control measures

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.3, modified – The definition was reworded.]

**3.5**
**LIKELIHOOD**
chance of something happening

Note 1 to entry: In risk management terminology, the word “LIKELIHOOD” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “LIKELIHOOD” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “LIKELIHOOD” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7]

**3.6**
**PROCESS**
set of interrelated or interacting activities which transforms inputs into outputs

Note 1 to entry: The term “activities” covers use of resources.

[SOURCE: IEC 80001-1:2010, 2.19]

**3.7**
**HEALTH IT RISK MANAGER**
person accountable for risk management of a health IT system

[SOURCE: IEC 80001-1:2010, 2.17, modified – Replacement of the term "medical IT-network risk manager" with "health risk manager", and replacement in the definition "medical IT-network" with "health IT system".]

**3.8**
**RISK MANAGEMENT PLAN**
description of how the elements and resources of the risk management PROCESS will be implemented within an organization or project

[SOURCE: ISO/IEC 16085:2006, 3.11]

## 4 Principles

The following principles provide the basis for RISK MANAGEMENT. They communicate the value, intention and purpose of RISK MANAGEMENT and their application supports the preservation of the KEY PROPERTIES during the implementation and use of HEALTH IT SYSTEMS within a HEALTH IT INFRASTRUCTURE:

- RISK MANAGEMENT is an integral part of an ORGANIZATION'S activities at all stages of the HEALTH IT SYSTEM lifecycle;
- accountability for the RISK MANAGEMENT PROCESS remains with the HEALTHCARE DELIVERY ORGANIZATION;
- a HEALTHCARE DELIVERY ORGANIZATION may assign responsibility for RISK MANAGEMENT of the HEALTH IT SYSTEM and/or HEALTH IT INFRASTRUCTURE to a different ORGANIZATION such as providers of HEALTH IT SYSTEMS, HEALTH IT INFRASTRUCTURE or a collaboration of HEALTHCARE DELIVERY ORGANIZATIONS.

RISK MANAGEMENT creates and protects value. It contributes to the demonstrable maintenance or/and improvement of SAFETY, EFFECTIVENESS and SECURITY in the implementation and use of connected HEALTH IT SYSTEMS.

- A structured and comprehensive approach to RISK MANAGEMENT contributes to consistent and comparable clinical outcomes;
- The RISK MANAGEMENT PROCESS is scalable and can be customised and made proportionate to the ORGANIZATION'S objectives;
- Appropriate and timely involvement of stakeholders leads to improved awareness and alignment across the ORGANIZATION and enables informed RISK MANAGEMENT;
- RISKS can emerge, change or disappear as new HEALTHCARE tools and methodologies are developed. Proactive RISK MANAGEMENT anticipates, detects, acknowledges and responds to changes and events in a timely manner;
- The inputs to RISK MANAGEMENT are based on historical and current information, as well as future expectations. RISK MANAGEMENT explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders;
- The SOCIOTECHNICAL ECOSYSTEM significantly influences all aspects of RISK MANAGEMENT at each level within the HEALTHCARE DELIVERY ORGANIZATION and at each lifecycle stage; and
- RISK MANAGEMENT is a continuous activity, improved through learning and experience. RISK MANAGEMENT strengthens the ORGANIZATION resilience and supports the ORGANIZATION'S business needs and objectives.

NOTE RISK is balanced across the KEY PROPERTIES wherever practical.