DRAFT INTERNATIONAL STANDARD

ISO/DIS 81001-1

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2019-11-10

Voting terminates on:
2020-02-02

Health software and health IT systems safety, effectiveness and security —

Part 1:
Foundational principles, concepts, and terms

ICS: 35.240.80

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 81001-1:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

This document was prepared by a joint working group of ISO technical committee 215: *Health informatics* and subcommittee 62A: *Common aspects of electrical equipment used in medical practice*.

A list of all parts in the ISO 81001- series can be found on the ISO website.

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

Introduction

While the benefits of digital health are widely accepted, the potential for inadvertent and adverse impacts on *safety*, *effectiveness* and *security* caused by *health software* and *health IT systems* is also becoming more apparent. Today's sophisticated *health software* and *health IT systems* provide advanced levels of decision support and integrate patient data between *systems*, across organizational lines, and across the continuum of care. In addition to the patient and healthcare *system* benefits this creates, there is also increased likelihood of software-induced adverse *events*. Design flaws, coding errors, incorrect *implementation* or configuration, data integrity issues, faults in decision support tools, poor alignment with clinical workflows and improper maintenance and use of such *systems* are examples of *events* with the potential to cause *harm* to patients.

Managing *safety*, *effectiveness* and *security* for *health software* and *health IT systems* requires a comprehensive and coordinated approach to optimizing these three properties. Many *organizations* and *roles* are involved throughout the *life cycle* of *health software* and *health IT systems* (including *medical devices*), so a common understanding of the relevant concepts, principles and terminology is important in standardizing the *processes* and inter-organizational communications to support a coordinated approach to managing *safety*, *effectiveness* and *security*.

This document addresses these issues by providing a framework of fundamental concepts, principles and vocabulary for optimizing the *key properties* of *safety*, *effectiveness* and *security* of *health software* and *health IT systems*, including those that can be classified as a *medical device*. In doing so, it provides the foundation for other standards (e.g. the ISO/IEC 80001- series) addressing specific aspects of the software *life cycle* (see Figure 1) in greater detail.

This document is for use by *organizations* and people who build, acquire, operate, maintain, use or decommission *health software* and *health IT systems* (including *medical devices*), as well as by those creating standards that address *safety*, *security* and *effectiveness* for *health software*, *health IT systems* and *medical devices*. It is applicable to all *organizations* involved, regardless of size, complexity or business model.

Annex A provides further information on the rationale for this document, the terms and definitions being used and their relationship to other standards addressing various aspects of *health software* and *health IT systems safety*, *effectiveness* and *security*.

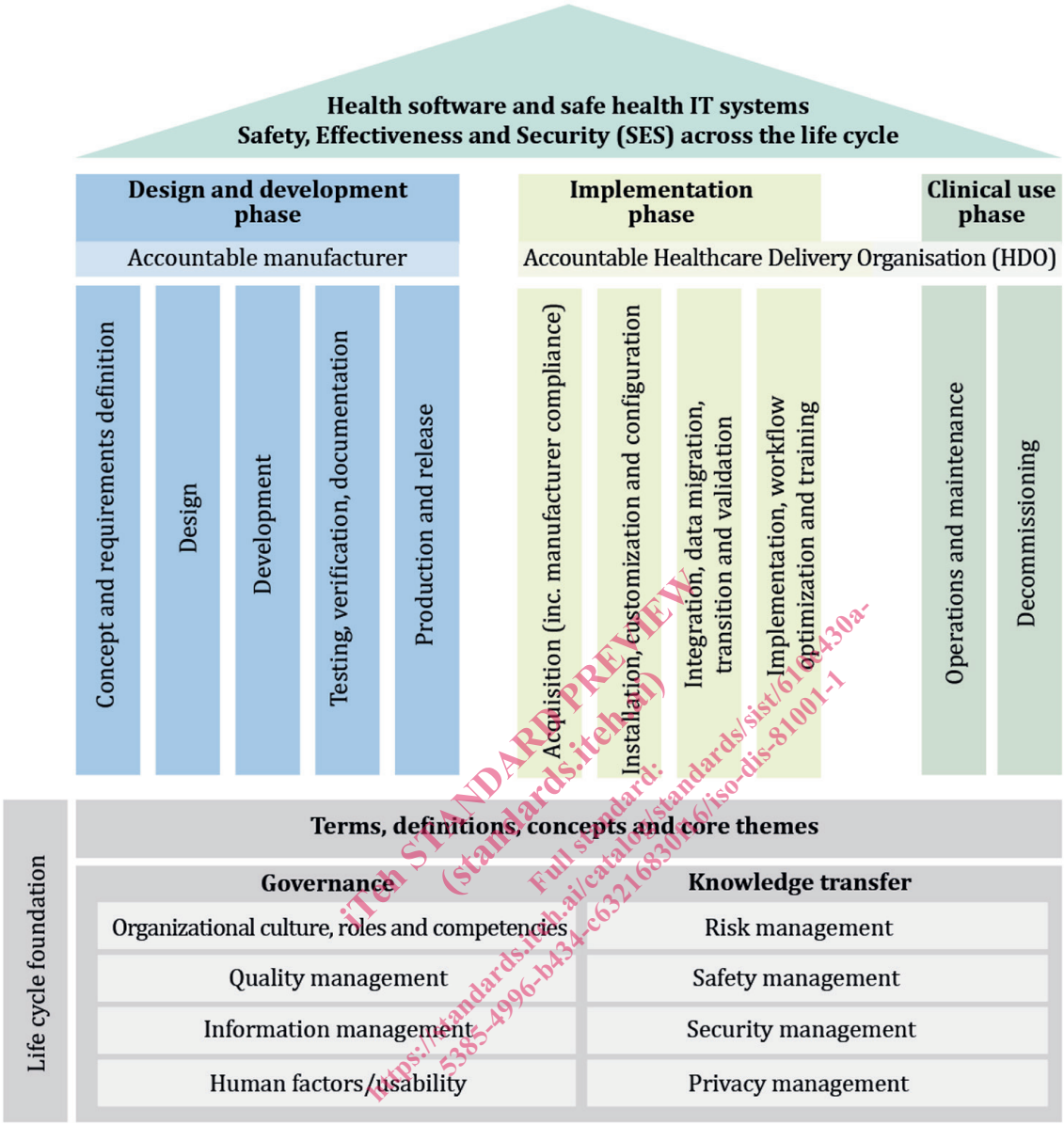

Figure 1 — Life cycle framework addressing safety, security and effectiveness of health software and health IT systems

Health software and health IT systems safety, effectiveness and security —

Part 1: Foundational principles, concepts, and terms

1 Scope

This document articulates the foundational principles, concepts, terms and definitions for *health software* and *health IT system safety*, *effectiveness* and *security* across the full *life cycle*, from concept to decommissioning, represented in Figure 1 (see Introduction). It takes into account the evolving complex internal and external context in healthcare, including people, technology (hardware/software), *organizations*, *processes*, and external environment. It also addresses the transition points in the *life cycle* where transfers of responsibility occur, and the types of multi-lateral communication that are necessary. This document provides a unifying foundation of coherent concepts and terminology for other standards that address specific aspects of the *safety*, *effectiveness*, and *security* (including *privacy*) of *health software* and *health IT systems*.

The fundamental concepts and principles of managing *safety*, *effectiveness* and *security* are applicable to all parties involved in the *health software* and *health IT systems life cycle* including:

a) *Organizations*, health informatics professionals and clinical leaders designing, developing, integrating, implementing and operating these *systems* – for example *health software developers* and *medical device manufacturers*, *system integrators*, *system administrators* (including cloud and other IT service providers);

b) Healthcare service delivery *organizations*, healthcare providers and others who use these *systems* in providing health services;

c) Governments, health system funders, monitoring agencies, professional *organizations* and *customers* seeking confidence in an *organization's* ability to consistently provide safe, effective and secure *health IT systems* and services;

d) *Organizations* and interested parties seeking to improve communication in managing *safety*, *effectiveness* and *security risks* through a common understanding of the concepts and terminology used in *safety*, *effectiveness* and *security* management;

e) *Organizations* performing conformity assessments against the requirements of ISO/IEC 80001- series;

f) Providers of training, assessment or advice in *safety*, *effectiveness* and *security risk management* for *health software* and *systems*; and

g) *Developers* of related *safety*, *effectiveness* and *security* standards.

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 terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

NOTE Annex B contains a diagrammatic representation of how the terms used in this document relate conceptually.

3.1
accompanying document
document accompanying a *health software* (3.23) and *health IT system* (3.22) or an accessory, containing information for the responsible *organization* (3.35) or operator, particularly regarding *safety* (3.55)

Note 1 to entry: Adapted from IEC 60601-1:2005 definition 3.4 by replacing medical electrical equipment and medical electrical system with *health software* and *health IT system* and replacing basic safety and essential performance with *safety* in order to expand the scope to *health software* and *health IT system*.

3.2
administrator
role (3.53) responsible for the ongoing operation of the implemented *health IT system* (3.22) and ensuring it is safeguarded and maintained on an ongoing basis

3.3
asset
physical or digital entity that has value to an individual, an *organization* (3.35) or a government

[SOURCE: ISO/IEC JTC 1/SC 41 N0317, 2017-11-12]

3.4
assurance case
reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

Note 1 to entry: An *assurance case* contains the following and their relationships:

— one or more claims about properties;

— arguments that logically link the evidence and any assumptions to the claim(s);

— a body of evidence and possibly assumptions supporting these arguments for the claim(s); and

— justification of the choice of top-level claim and the method of reasoning.

[SOURCE: ISO/IEC 15026-1:2019, 3.1.2]

3.5
change management
process (3.38) for recording, coordination, approval and monitoring of all changes

[SOURCE: ISO/IEC/TS 22237-7:2018, 3.1.3]

3.6
change-release management
process (3.38) that ensures that all changes to the *health IT infrastructure* (and its *component* (3.9) parts) are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with *configuration management* (3.10)

Note 1 to entry: Adapted from ISO/IEC 20000-1:2005.

3.7
clinical change management
strategic and systematic approach that supports people and their *organizations* (3.35) in the successful transition and adoption of electronic health solutions, with a focus on outcomes including solution adoption by *users* (3.65) and the realization of benefits

Note 1 to entry: Adapted from *A Framework and Toolkit for Managing eHealth Change: People and Processes, Canada Health Infoway Change Management Framework* – 2011.

3.8
cloud service
one or more capabilities offered via cloud computing invoked using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.9
component
collection of *system* (3.60) resources that (a) forms a physical or logical part of the *system*, (b) has specified functions and interfaces, and (c) is treated (e.g., by policies or specifications) as existing independently of other parts of the *system*

[SOURCE: RFC 4949, modified — Note1 deleted.]

3.10
configuration management
process (3.38) that ensures that configuration information of *components* (3.9) within the *health IT infrastructure* (3.21) are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the *health IT infrastructure*

Note 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclause 9.1.

3.11
customer
person or *organization* (3.35) that could or does receive a *product* (3.39) or a service that is intended for or required by this person or *organization*

Note 1 to entry: A *customer* can be internal or external to the *organization*.

[SOURCE: ISO 9000:2015, 3.2.4, modified — Example deleted.]

3.12
developer
role (3.53) responsible for execution of the design and development phase (from concept to release and maintenance) of a *health software* (3.23) or *health IT system* (3.22)

Note 1 to entry: A *developer* could, for example, be part of a manufacturing *organization* (3.35), a supplier of services, or an *HDO* (3.24).

3.13
effectiveness
ability to produce the intended result

3.14
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An *event* can be one or more occurrences and can have several causes.

Note 2 to entry: An *event* can consist of something not happening.

Note 3 to entry: An *event* can sometimes be referred to as an "incident" or "accident".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry deleted.]

3.15
exploit
defined way to breach the *security* (3.56) of information *systems* (3.60) through *vulnerability* (3.67)

[SOURCE: ISO/IEC 27039:2015, 2.9]

3.16
exposure
extent to which an *organization* (3.35) and/or stakeholder is subject to an *event* (3.14)

[SOURCE: ISO Guide 73:2009, 3.6.1.2]

3.17
harm
injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 63:2019, 3.1]

3.18
hazard
potential source of *harm* (3.17)

[SOURCE: ISO/IEC Guide 63:2019, 3.2]

3.19
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more *hazards* (3.18)

[SOURCE: ISO/IEC Guide 63:2019, 3.3]

3.20
health information technology
health IT
the documented and intended application of information technology to the collection, storage, processing, retrieval, and communication of information relevant to health, patient care, and well-being

3.21
health IT infrastructure
combined set of IT *assets* (3.3) available to the individual or *organization* (3.35) for developing, configuring, integrating, maintaining, and using IT services and supporting health, patient care and other organizational objectives

Note 1 to entry: As per the definition for *asset* this can include the following:

a) data and information;

b) *health software* (3.23) a (including *medical devices* (3.34), health applications, middleware, and operating *system* (3.60) software)

c) hardware *components* such as computers, mobile devices, servers, databases, and networks;

d) services, including *security* (3.56), software development, IT operations and externally provided services such as data centres, internet and software-as-a-service and cloud solutions;

e) people, and their qualifications, skills and experience:

f) technical procedures and documentation to manage and support the *health IT infrastructure*

g) HIT *systems* that are configured and implemented to address organizational objectives by leveraging the above *assets*

h) intangibles, such as reputation and image

3.22
health IT system
a combination of interacting health information elements (including *health software* (3.23), *medical devices* (3.34), IT hardware, interfaces, data, procedures and documentation) that is configured and implemented to support and enable an individual or *organization's* (3.35) specific health objectives

3.23
health software
software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a *medical device* (3.34)

Note 1 to entry: *Health software* fully includes what is considered software as a *medical device*.

3.24
healthcare delivery organization
HDO
facility or enterprise such as a clinic or hospital that provides healthcare services

3.25
***implementation* (of a *system*)**
life cycle (3.32) phase at the end of which the hardware, software and procedures of the *system* (3.60) considered become operational

[SOURCE: ISO/IEC 2382:2015, 2122692, modified — Change "system development" to "*life cycle*" and delete notes to entry.]

3.26
implementer
role (3.53) responsible for the clinical installation, workflow optimization, and training of *health software* (3.23) and *health IT systems* (3.22) in the clinical setting

Note 1 to entry: An *implementer* can be the *manufacturer* (3.33), the *HDO* (3.24), or a third party.

3.27
integrator
role (3.53) responsible for the integration of *health software* (3.23) and *health IT systems* (3.22) with the existing *health IT systems*, *medical devices* (3.34), and technology being used by the *healthcare delivery organization* (3.24), including technical installation, configuration, and data migration

3.28
intended use
intended purpose
use for which a *product* (3.39), *process* (3.38) or service is intended according to the specifications, instructions and information provided by the *manufacturer* (3.33)

Note 1 to entry: The intended medical indication, patient population, part of the body or type of tissue interacted with, *user* (3.65) profile, use environment, and operating principle are typical elements of the *intended use*.

[SOURCE: ISO/IEC Guide 63, 2019, 3.4, modified — Add admitted term *intended purpose*.]

3.29
interoperability
ability of two or more *systems* (3.60) or *components* (3.9) to exchange information and to use the information that has been exchanged

[SOURCE: IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries. New York: Institute of Electrical and Electronics Engineers; 1990]

3.30
IT-network
system (3.60) or *systems* composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

Note 1 to entry: Adapted from IEC 61907:2009, definition 3.1.1.

3.31
key properties
three *risk* (3.44) managed characteristics (*safety* (3.55), *effectiveness* (3.13), and *security* (3.56)) of *health software* (3.23), *health IT systems* (3.22), and *health IT infrastructures* (3.21)

3.32
life cycle
series of all phases in the life of a *product* (3.39) or *system* (3.60), from the initial conception to final decommissioning and disposal

[SOURCE: ISO/IEC Guide 63:2019, 3.5, modified — The words "medical device" have been replaced with "*product* or *system*".]

3.33
manufacturer
natural or legal person with responsibility for design and/or manufacture of a *medical device* (3.34) with the intention of making the *medical device* available for use, under his name; whether or not such a medical device is designed and/or manufactured by that person himself or on his behalf by another person(s)

Note 1 to entry: This "natural or legal person" has ultimate legal responsibility for ensuring compliance with all applicable regulatory requirements for the *medical devices* in the countries or jurisdictions where it is intended to be made available or sold, unless this responsibility is specifically imposed on another person by the Regulatory Authority within that jurisdiction.

Note 2 to entry: The *manufacturer's* responsibilities are described in other GHTF guidance documents. These responsibilities include meeting both pre-market requirements and post-market requirements, such as adverse *event* (3.14) reporting and notification of corrective actions.

Note 3 to entry: "Design and/or manufacture" can include specification development, production, fabrication, assembly, processing, packaging, repackaging, labelling, relabelling, sterilization, installation, or remanufacturing of a *medical device*; or putting a collection of devices, and possibly other *products* (3.39), together for a medical purpose.

Note 4 to entry: Any person who assembles or adapts a *medical device* that has already been supplied by another person for an individual patient, in accordance with the instructions for use, is not the *manufacturer*, provided the assembly or adaptation does not change the *intended use* (3.28) of the *medical device*.

Note 5 to entry: Any person who changes the *intended use* of, or modifies, a *medical device* without acting on behalf of the original *manufacturer* and who makes it available for use under his own name, should be considered the *manufacturer* of the modified *medical device*.

Note 6 to entry: An authorized representative, distributor or importer who only adds its own address and contact details to the *medical device* or the packaging, without covering or changing the existing labelling, is not considered a *manufacturer*.

Note 7 to entry: To the extent that an accessory is subject to the regulatory requirements of a *medical device*, the person responsible for the design and/or manufacture of that accessory is considered to be a *manufacturer*.

[SOURCE: ISO/IEC Guide 63:2019, 3.6]

3.34
medical device
instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the *manufacturer* (3.33) to be used, alone or in combination, for human beings, for one of more of the specific medical 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 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 function by such means

Note 1 to entry: *Products* (3.39) which can 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 reproductive technologies.

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

3.35
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of *organization* includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, association, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by modifying Note 1 to entry.

3.36
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: To provision of health services to the individual and that may include:

a) information about the registration of the individual for the provision of health services;

b) information about payments or eligibility for health care in respect to the individual;

c) a number, symbol, or particular assigned to an individual to uniquely identify the individual for health purposes;

d) any information about the individual that is collected in the course of the provision of health services to the individual;

e) information derived from the testing or examination of a body part or bodily substance; and

f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

Note 2 to entry: *Personal health information* (3.36) does not include information that, either by itself or when combined with other information available to the holder, is anonymized, the identity of the individual who is the subject of the information cannot be ascertained from the information.