AS ISO 81001.1:2022
ISO 81001-1:2021

Australian STANDARD®

STANDARDS Australia

Health software and health IT systems safety, effectiveness and security

Part 1: Principles and concepts

AS ISO 81001.1:2022

This Australian Standard ® was prepared by IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 09 July 2022.

This Standard was published on 22 July 2022.

The following are represented on Committee IT-014:

Australasian Institute of Digital Health
Australasian Telehealth Society
Australian College of Nursing
Australian Commission on Safety and Quality in Health Care
Australian Digital Health Agency
Australian Healthcare and Hospitals Association
Australian Information Industry Association
Australian Institute of Health and Welfare
Australian Private Hospitals Association
Consumers Federation of Australia
CSIRO
Department of Health, TAS
Engineers Australia
Flinders University
GS1 Australia
Medical Software Industry Association
Monash University
NSW Ministry of Health
Queensland Health
Royal College of Pathologists of Australasia
SA Health
The Pharmacy Guild of Australia
Victorian Department of Health and Human Se[illegible]

This Standard was issued in draft form for comme[illegible] DR AS ISO 81001.1:2022.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76113 885 0

Health software and health IT systems safety, effectiveness and security

Part 1: Principles and concepts

First published as AS ISO 81001.1:2022.

Preface

This Standard was prepared by the Standards Australia Committee IT-014, Health Informatics.

The objective of this document is to provide the principles, concepts, terms and definitions for health software and health IT systems, key properties of safety, effectiveness and security, across the full life cycle, from concept to decommissioning, as represented in Figure 1. It also identifies the transition points in the life cycle where transfers of responsibility occur, and the types of multi-lateral communication that are necessary at these transition points.

This document also establishes a 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.

This document is applicable to all parties involved in the health software and health IT systems life cycle including the following:

(a) Organizations, health informatics professionals and clinical leaders designing, developing, integrating, implementing and operating health software and health IT 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 health software and health IT 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 software, 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) Providers of training, assessment or advice in safety, effectiveness and security risk management for health software and health IT systems.

(f) Developers of related safety, effectiveness and security standards.

This document is identical with, and has been reproduced from, ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts*.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms "normative" and "informative" are used in Standards to define the application of the appendices or annexes to which they apply. A "normative" appendix or annex is an integral part of a Standard, whereas an "informative" appendix or annex is only for information and guidance.

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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 jointly by Technical Committee ISO/TC 215, *Health informatics*, and Technical Committee IEC/TC 62, *Electrical equipment in medical practice*, Subcommittee SC 62A, *Common aspects of electrical equipment used in medical practice*.

A list of all parts in the ISO 81001 and IEC 81001 series can be found on the ISO and IEC websites.

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* causing harm to both patients and healthcare organizations. 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 *health software* and *health IT systems* are examples of *events* with the potential to cause *harm*.

Managing *safety*, *effectiveness* and *security* for *health software* and *health IT systems* (including *medical devices*), 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* (see Figure 1). Therefore, a common understanding of the 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 takes into account the evolving complex internal and external context in healthcare, including people, technology (hardware/software), *organizations*, *processes*, and external environment.

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*.

In addition to a common set of terms, definitions and concepts, this document describes eight foundational elements in Clause 5, which support the overarching themes articulated in Clause 4. For each foundational element, there is a "statement" describing each element; a "rationale" explaining why it is important; "key concepts and principles" pertinent for managing *safety*, *effectiveness* and *security*; and high-level guidance on the "approach" *organizations* can take to apply the concepts and principles.

Given the importance of communication between the various *organizations*, *roles* and responsibilities involved across the *life cycle* of *health software* and *health IT systems* for the four foundational cross-organizational elements, additional specific clauses on communication and information sharing at major transition points are also included for 5.3.2, 5.3.3, 5.3.4 and 5.3.5.

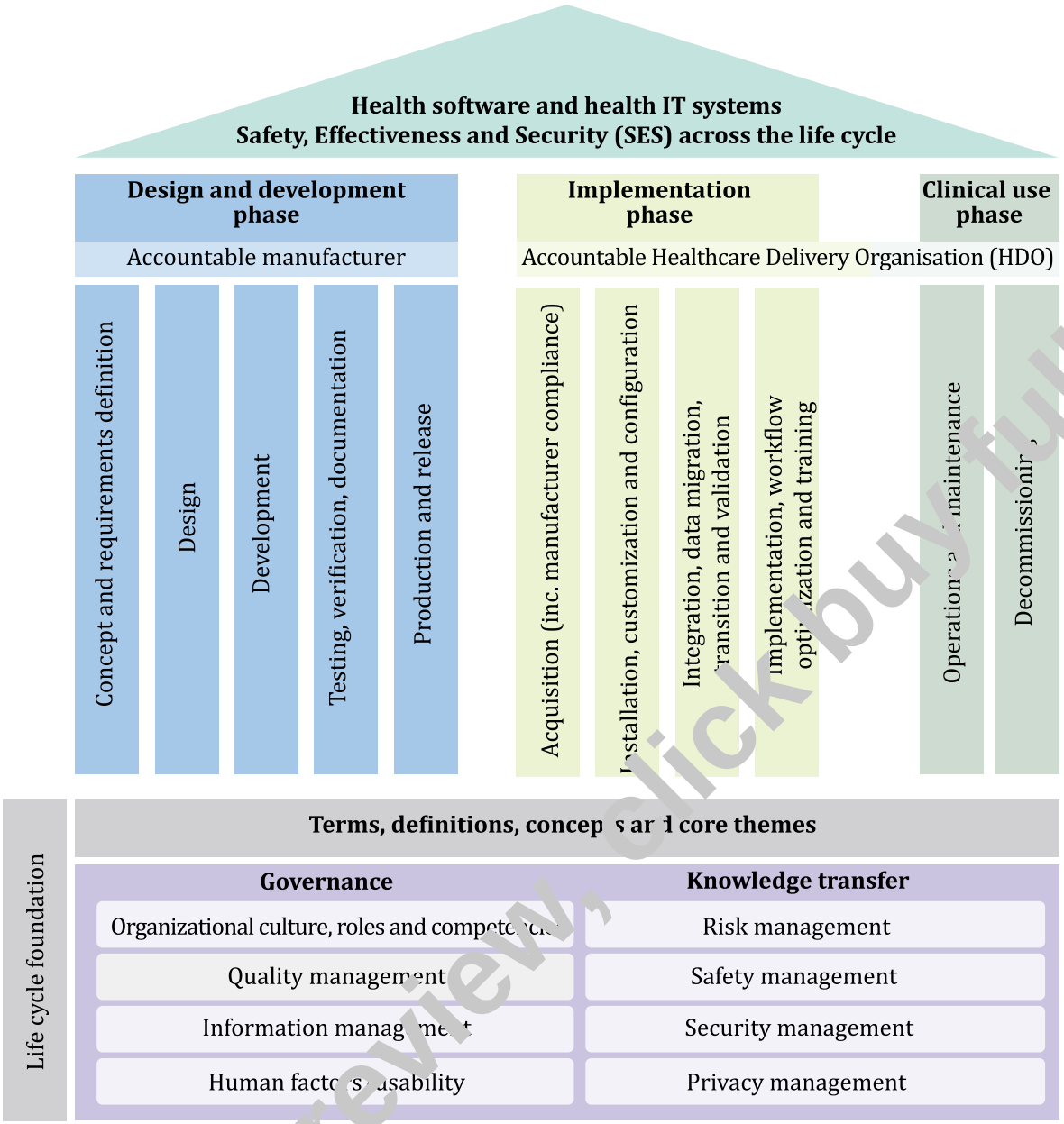

Figure 1 — *Life cycle* framework addressing *safety, effectiveness* and *security* of *health software* and *health IT systems*

Australian Standard®

Health software and health IT systems safety, effectiveness and security

Part 1: Principles and concepts

1 Scope

This document provides the principles, concepts, terms and definitions for *health software* and *health IT systems, key properties* of *safety*, *effectiveness* and *security,* across the full *life cycle*, from concept to decommissioning, as represented in Figure 1. It also identifies the transition points in the *life cycle* where transfers of responsibility occur, and the types of multi-lateral communication that are necessary at these transition points. This document also establishes a 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*.

This document is applicable to all parties involved in the *health software* and *health IT systems life cycle* including the following:

a) *Organizations*, health informatics professionals and clinical leaders designing, developing, integrating, implementing and operating *health software* and *health IT 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 *health software* and *health IT 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 software*, *health IT systems* and services;

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

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

f) *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 https://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.