FINAL DRAFT
Technical
Specification

IEC/DTS 81001-2-2

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2025-**06**-**13**

Voting terminates on:
2025-**08**-**08**

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

Part 2-2:
Guidance for the implementation, disclosure and communication of security needs, risks and controls

Sécurité, efficacité et sûreté des logiciels de santé et des systèmes TI de santé —

Partie 2-2: Recommandations pour la mise en œuvre, la divulgation et la communication des besoins, des risques et des contrôles en matière de sécurité

This draft is submitted to a parallel vote in ISO and in IEC.

Reference number
IEC/DTS 81001-2-2:2025(en)

© IEC 2025

iTeh Standards
(https://standards.iteh.ai)
Document Preview

IEC/DTS 81001-2-2

https://standards.iteh.ai/catalog/standards/iso/25a40142-54e0-436b-9b3b-0553c5bc73d7/iec-dts-81001-2-2

CONTENTS

1

89

90

_____

HEALTH SOFTWARE AND HEALTH IT SYSTEMS SAFETY, EFFECTIVENESS AND SECURITY –

Part 2-2: Coordination – Guidance for the implementation, disclosure and communication of security needs, risks and controls

FOREWORD

IEC TS 81001-2-2 has been prepared by subcommittee 62A: Common aspects of electrical equipment, software, and systems, of IEC technical committee 62: Medical equipment, software, and systems and ISO technical committee 215: Health informatics. It is a Technical Specification.

This document withdraws and replaces:

– IEC TR 80001-2-2, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the 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 TR 80001-2-2*

148 This document includes the following significant changes:

149 a) Combines and updates the contents of IEC TR 80001-2-2 and IEC TR 80001-2-8;

150 b) Extends the scope to *health software* instead to only *medical device* software;

151 c) Aligns contents and definitions to ISO 81001-1:2021 and the updated IEC 80001-1;

152 d) Removed the Configuration of Security Features (CNFS) capability, as any configurable
153 *security capability* shall be clearly communicated.

154 e) Provide *security control* mappings to several new standards, e.g. IEC TR 60601-4-5,
155 IEC 62443-4-2, ISO/IEEE 11073-40102 and the recent versions of previous standards, e.g.
156 ISO/IEC 27002 and NIST 800-53 version 5.

157 The text of this Technical Specification is based on the following documents:

Draft	Report on voting
62A/XX/DTS	62A/XX/RVDTS

158

159 Full information on the voting for its approval can be found in the report on voting indicated in
160 the above table.

161 The language used for the development of this Technical Specification is English.

162 This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in
163 accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available
164 at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are
165 described in greater detail at www.iec.ch/publications.

166 A list of all parts in the IEC 81001 series, published under the general title *Health software and*
167 *health IT systems safety, effectiveness and security*, can be found on the IEC website.

168 Terms used throughout this document that have been defined in Clause 3 and the terms
169 referenced in the alphabetical index at the end of the document appear in *italics.*

170 The committee has decided that the contents of this document will remain unchanged until the
171 stability date indicated on the IEC website under webstore.iec.ch in the data related to the
172 specific document. At this date, the document will be

173 • reconfirmed,

174 • withdrawn, or

175 • revised.

176

177

INTRODUCTION

179 ISO 81001-1 provides the principles, concepts, terms and definitions for *health software* and
180 *health IT system*s, *key properties* of *safety*, *effectiveness* and *security* across the life cycle.
181 ISO 81001-1 and all parts of the ISO 81001 and IEC 81001 series are applicable to all relevant
182 stakeholders including *health software manufacturer*s (including *medical device manufacturer*s)
183 and *healthcare delivery organization*s (*HDOs*). This document provides guidance on the
184 implementation, disclosure and communication of *health software security* needs, *risks* and
185 controls for both *health software manufacturers* (including *medical device manufacturer*) and
186 *HDOs*.

187 For this document, the term "*manufacturer*" refers to the *health software manufacturer* which
188 includes the *medical device manufacturer*. The term "user" typically refers to the *HDOs* for
189 whom the information exchange resulting from using this document can be applied for their *risk*
190 *assessments* and to establish a common understanding of the products *security* capabilities,
191 and to further support the shared responsibility between *HDOs* and *manufacturers*.

192 The informative set of *security capabilities* presented are intended to be the baseline for a
193 *security*-centric discussion between all stakeholders, including *manufacturers*, vendors, *HDOs*,
194 procurements, etc. The level of effort is scalable across organizations of all sizes and it is
195 crucial that it is adapted to the *risk* tolerance and the organizational goals. This document can
196 be used across the life cycle of the *health IT system* and *health IT Infrastructure* that the *health*
197 *software* is being incorporated into, including:

198 a) administrative and technical *security control*s to protect and maintain the confidentiality,
199   integrity, availability, authenticity, accountability and non-repudiation of data and systems,

200 b) documentation,

201 c) *risk management*,

202 d) shared responsibility,

203 e) procurement, and

204 f) agreements.

205 A *security capability* represents broad categories of technical, administrative and organizational
206 *security controls* which are used to manage *risks* to confidentiality, integrity, availability,
207 authenticity, accountability, non-repudiation and other characteristics, such as authorization,
208 auditing, privacy, resilience, compliance and revocability, which are important for a
209 comprehensive *security* of data and systems. This document presents these categories of
210 *security controls* prescribed for a system and the operational environment to establish *security*
211 *capabilities* that protect, maintain, and ensure the confidentiality, integrity and availability of
212 data and systems. It is important to note that *security controls* for each *security capability* can
213 be added as the need arises. Controls are intended to protect both data and systems but special
214 attention is given to the protection of personal data and health data. Both special terms have
215 been defined to carefully avoid any law-specific references (e.g. European special categories
216 of personal data or sensitive data and *Personal Health Information* (PHI) in the USA).

217 The list is not intended to constitute or to support rigorous IT *security* standards-based controls
218 and associated programs of certification and assurance like other ISO/IEC documents (e.g.
219 ISO/IEC 15408 with its Common Criteria for Information Technology Security Evaluation and
220 IEC 62443 for Security for industrial automation and control systems). This document does not
221 contain sufficient detail for exact specification of requirements. However, the classification and
222 structure can be used to organize such requirements with underlying detail sufficient for
223 communication during the life cycle of *health software* or IT equipment component.

224 This document creates a framework for the disclosure of *security*-related capabilities necessary
225 for managing the *risk* when implementing *health software* as a component of *health IT system*s
226 operating on *health IT infrastructure*s and *IT Infrastructure* for *security* dialog that supports *key*
227 *properties* of *safety*, *effectiveness* and *security* as conceptualized in ISO 81001-1 and other
228 relevant *security* standards.