



# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**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**

**Application de la gestion des risques aux réseaux des technologies de  
l'information contenant des dispositifs médicaux –  
Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des  
dispositifs médicaux connectés ou des logiciels de santé connectés**



This is a preview of "IEC 80001-1:2021". [Click here to purchase the full version from the ANSI store.](#)



### Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

#### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

#### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

#### IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC online collection - [oc.iec.ch](http://oc.iec.ch)

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

---

#### A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

#### A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

#### Recherche de publications IEC -

[webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC online collection - [oc.iec.ch](http://oc.iec.ch)

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.



# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**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**

**Application de la gestion des risques aux réseaux des technologies de  
l'information contenant des dispositifs médicaux –  
Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des  
dispositifs médicaux connectés ou des logiciels de santé connectés**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

FOREWORD.....	4
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references .....	9
3 Terms and definitions .....	9
4 Principles .....	10
5 Framework .....	11
5.1 General.....	11
5.2 Leadership and commitment .....	11
5.3 Integrating RISK MANAGEMENT .....	11
5.4 Design/planning .....	12
5.4.1 General .....	12
5.4.2 RISK MANAGEMENT FILE .....	13
5.4.3 Understanding the organization and the SOCIOTECHNICAL ECOSYSTEM.....	13
5.4.4 Articulating RISK MANAGEMENT commitment .....	13
5.4.5 Assigning organizational roles, authorities, responsibilities and accountabilities.....	13
5.4.6 Allocating resources .....	14
5.4.7 Establishing communication and consultation .....	14
5.5 Implementation .....	15
5.6 Evaluation.....	15
5.7 Improvement.....	15
6 RISK MANAGEMENT PROCESS.....	15
6.1 Generic requirements.....	15
6.1.1 General .....	15
6.1.2 RISK ANALYSIS .....	16
6.1.3 RISK EVALUATION .....	18
6.1.4 RISK CONTROL .....	19
6.2 Lifecycle specific requirements .....	21
6.2.1 General .....	21
6.2.2 Acquisition.....	21
6.2.3 Installation, customization and configuration.....	22
6.2.4 Integration, data migration, transition and validation .....	22
6.2.5 Implementation, workflow optimization and training .....	22
6.2.6 Operation and maintenance .....	23
6.2.7 Decommission .....	24
Annex A (informative) IEC 80001-1 requirements mapping table.....	25
Annex B (informative) Guidance for accompanying document Information.....	31
B.1 Foreword .....	31
B.2 Information system categorization.....	32
B.3 Overview.....	32
B.4 Reference documents .....	32
B.5 System level description .....	32
B.5.1 Environment description .....	32
B.5.2 Network ports, protocols and services .....	33
B.5.3 Purpose of connection to the health IT infrastructure .....	33

This is a preview of "IEC 80001-1:2021". [Click here to purchase the full version from the ANSI store.](#)

B.5.4	Networking requirements .....	33
B.5.5	Required IT-network services .....	33
B.5.6	Data flows and protocols .....	33
B.6	Security and user access .....	34
B.6.1	General .....	34
B.6.2	Malware / antivirus / allow-list.....	34
B.6.3	Security exclusions .....	34
B.6.4	System access .....	34
B.7	RISK MANAGEMENT .....	36
	Bibliography.....	37

Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health software and health IT systems.....	8
--	---

Figure 2 – RISK MANAGEMENT PROCESS .....	12
--	----

Table A.1 – IEC 80001-1 requirements table.....	25
---	----

Table B.1 – Organization name and location .....	31
--	----

Table B.2 – Cybersecurity device characterization level.....	32
--	----

Table B.3 – Ports, protocols and services .....	33
---	----

Table B.4 – Information system name and title.....	34
--	----

Table B.5 – Roles and privileges.....	35
---------------------------------------	----

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

### **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**

#### 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;

This is a preview of "IEC 80001-1:2021". [Click here to purchase the full version from the ANSI store.](#)

- 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/1434/FDIS	62A/1448/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.

This is a preview of "IEC 80001-1:2021". [Click here to purchase the full version from the ANSI store.](#)

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.**



This is a preview of "IEC 80001-1:2021". [Click here to purchase the full version from the ANSI store.](#)

## 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).