# IEC 80001-1

Edition 1.0 2010-10

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities

## Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux – Partie 1: Fonctions, responsabilités et activités

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 11.040.01; 35.240.80

ISBN 978-2-88912-221-9

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

## Part 1: Roles, responsibilities and activities

## 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 ISO technical committee 215: Health informatics.

It is published as a double logo standard.

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

| FDIS | Report on voting |
|---|---|
| 62A/703/FDIS | 62A/718/RVD |

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 17 P-members out of 18 having cast a vote.

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

Terms defined in Clause 2 of this standard are printed in SMALL CAPITALS.

For the purposes of this standard:

- “shall” means that compliance with a requirement is mandatory for compliance with this standard;
- “should” means that compliance with a requirement is recommended but is not mandatory for compliance with this standard;
- “may” is used to describe a permissible way to achieve compliance with a requirement; and
- “establish” means to define, document, and implement.

A list of all parts of the IEC 80001 series, published under the general title *Application of risk management for IT-networks incorporating medical devices,* can be found on the IEC website.

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

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- withdrawn,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

**IMPORTANT – The 'colour inside' logo on the cover page of this publication 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

An increasing number of MEDICAL DEVICEs are designed to exchange information electronically with other equipment in the user environment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature.

At the same time, IT-NETWORKS are becoming increasingly vital to the clinical environment and are now required to carry increasingly diverse traffic, ranging from life-critical patient data requiring immediate delivery and response, to general corporate operations data and to email containing potential malicious content (e.g. viruses).

For many jurisdictions, design and production of MEDICAL DEVICES is subject to regulation, and to standards recognized by the regulators. Traditionally, regulators direct their attention to MEDICAL DEVICE manufacturers, by requiring design features and by requiring a documented PROCESS for design and manufacturing. MEDICAL DEVICES cannot be placed on the market in these jurisdictions without evidence that those requirements have been met.

The use of the MEDICAL DEVICES by clinical staff is also subject to regulation. Members of clinical staff have to be appropriately trained and qualified, and are increasingly subject to defined PROCESSES designed to protect patients from unacceptable RISK.

In contrast, the incorporation of MEDICAL DEVICES into IT-NETWORKS in the clinical environment is a less regulated area. IEC 60601-1:2005 [1][1)] requires MEDICAL DEVICE manufacturers to include some information in ACCOMPANYING DOCUMENTS if the MEDICAL DEVICE is intended to be connected to an IT-NETWORK. Standards are also in place covering common information technology activities including planning, design and maintenance of IT-NETWORKS, for instance ISO 20000-1:2005 [9]. However, until the publication of this standard, no standard addressed how MEDICAL DEVICES can be connected to IT-NETWORKS, including general-purpose IT-NETWORKS, to achieve INTEROPERABILITY without compromising the organization and delivery of health care in terms of SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY.

There remain a number of potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, including:

– lack of consideration for RISK from use of IT-NETWORKS during evaluation of clinical RISK;
– lack of support from manufacturers of MEDICAL DEVICES for the incorporation of their products into IT-NETWORKS, (e.g. the unavailability or inadequacy of information provided by the manufacturer to the OPERATOR of the IT-NETWORK);
– incorrect operation or degraded performance (e.g. incompatibility or improper configuration) resulting from combining MEDICAL DEVICES and other equipment on the same IT-NETWORK;
– incorrect operation resulting from combining MEDICAL DEVICE SOFTWARE and other software applications (e.g. open email systems or computer games) in the same IT-NETWORK;
– lack of security controls on many MEDICAL DEVICES; and
– the conflict between the need for strict change control of MEDICAL DEVICES and the need for rapid response to the threat of cyberattack.

When these problems manifest themselves, unintended consequences frequently follow.

This standard is addressed to RESPONSIBLE ORGANIZATIONS, to manufacturers of MEDICAL DEVICES, and to providers of other information technology.

---

1) Numbers in square brackets refer to the Bibliography.

This standard adopts the following principles as a basis for its normative and informative sections:

– The incorporation or removal of a MEDICAL DEVICE or other components in an IT-NETWORK is a task which requires design of the action; this might be out of the control of the manufacturer of the MEDICAL DEVICE.

– RISK MANAGEMENT should be used before the incorporation of a MEDICAL DEVICE into an IT-NETWORK takes place, and for any changes during the entire life cycle of the resulting MEDICAL IT-NETWORK, to avoid unacceptable RISKS, including possible RISK to patients, resulting from the incorporation of the MEDICAL DEVICE into the IT-NETWORK. Many things are part of a RISK decision, such as liability, cost, or impact on mission. These should be considered in determining acceptable RISK in addition to the requirements described in this standard.

– Aspects of removal, maintenance, change or modification of equipment, items or components should be addressed adequately in addition to the incorporation of MEDICAL DEVICES.

– The manufacturer of the MEDICAL DEVICE is responsible for RISK MANAGEMENT of the MEDICAL DEVICE during the design, implementation, and manufacturing of the MEDICAL DEVICE. This standard does not cover the RISK MANAGEMENT PROCESS for the MEDICAL DEVICE.

– The manufacturer of a MEDICAL DEVICE intended to be incorporated into an IT-NETWORK might need to provide information about the MEDICAL DEVICE that is necessary to allow the RESPONSIBLE ORGANIZATION to manage RISK according to this standard. This information can include, as part of the ACCOMPANYING DOCUMENTS, instructions specifically addressed to the person who incorporates a MEDICAL DEVICE into an IT-NETWORK.

– Such ACCOMPANYING DOCUMENTS should convey instructions about how to incorporate the MEDICAL DEVICE into the IT-NETWORK, how the MEDICAL DEVICE transfers information over the IT-NETWORK, and the minimum IT-NETWORK characteristics necessary to enable the INTENDED USE of the MEDICAL DEVICE when it is incorporated into the IT-NETWORK. The ACCOMPANYING DOCUMENTS should warn of possible hazardous situations associated with failure or disruptions of the IT-NETWORK, and the misuse of the IT-NETWORK connection or of the information that is transferred over the IT-NETWORK.

– RESPONSIBILITY AGREEMENTS can establish roles and responsibilities among those engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK, all aspects of the life cycle of the resulting MEDICAL IT-NETWORK and all activities that form part of that life cycle.

– The RESPONSIBLE ORGANIZATION is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of those roles. The most important of those roles is the MEDICAL IT-NETWORK RISK MANAGER. This role can be assigned to someone within the RESPONSIBLE ORGANIZATION or to an external contractor.

– The MEDICAL IT-NETWORK RISK MANAGER is responsible for ensuring that RISK MANAGEMENT is included during the PROCESSES of:

  - planning and design of new incorporations of MEDICAL DEVICES or changes to such incorporations;
  - putting the MEDICAL IT-NETWORK into use and the consequent use of the MEDICAL IT-NETWORK; and
  - CHANGE-RELEASE MANAGEMENT and change management of the IT-NETWORK during the IT-NETWORK'S entire life cycle.

– RISK MANAGEMENT should be applied to address the following KEY PROPERTIES appropriate for the IT-NETWORK incorporating a MEDICAL DEVICE:

  - SAFETY (freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment);
- EFFECTIVENESS (ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION); and

- DATA AND SYSTEM SECURITY (an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability).

# APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

## Part 1: Roles, responsibilities and activities

## 1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.

This standard applies where there is no single MEDICAL DEVICE manufacturer assuming responsibility for addressing the KEY PROPERTIES of the IT-NETWORK incorporating a MEDICAL DEVICE.

NOTE 4 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, the installation or assembly of the MEDICAL DEVICE according to the manufacturer's ACCOMPANYING DOCUMENTS is not subject to the provisions of this standard regardless of who installs or assembles the MEDICAL DEVICE.

NOTE 5 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, additions to that MEDICAL DEVICE or modification of the configuration of that MEDICAL DEVICE, other than as specified by the manufacturer, is subject to the provisions of this standard.

This standard applies to RESPONSIBLE ORGANIZATIONS, MEDICAL DEVICE manufacturers and providers of other information technology for the purpose of RISK MANAGEMENT of an IT-NETWORK incorporating MEDICAL DEVICES as specified by the RESPONSIBLE ORGANIZATION.

This standard does not apply to personal use applications where the patient, OPERATOR and RESPONSIBLE ORGANIZATION are one and the same person.

NOTE 6 In cases where a MEDICAL DEVICE is used at home under the supervision or instruction of the provider, that provider is deemed to be the RESPONSIBLE ORGANIZATION. Personal use where the patient acquires and uses a MEDICAL DEVICE without the supervision or instruction of a provider is out of scope of this standard.

This standard does not address regulatory or legal requirements.

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# APPLICATION DE LA GESTION DES RISQUES AUX RÉSEAUX DES TECHNOLOGIES DE L'INFORMATION CONTENANT DES DISPOSITIFS MÉDICAUX –

## Partie 1: Fonctions, responsabilités et activités

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 80001-1 a été établie par un groupe de travail mixte du sous-comité 62A: *Aspects généraux des équipements électriques utilisés en pratique médicale*, du comité d'études 62 de la CEI: Equipements électriques dans la pratique médicale, et du comité technique 215 de l'ISO: Informatique médicale.

La présente publication est une norme double logo.

Le texte de la présente norme est issu des documents suivants:

| FDIS | Rapport de vote |
|---|---|
| 62A/703/FDIS | 62A/718/RVD |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme. A l'ISO, la norme a été approuvée par 17 membres P sur 18 ayant voté.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Les termes définis à l'Article 2 de la présente norme sont imprimés en PETITES MAJUSCULES.

Pour les besoins de la présente norme:

- "devoir" mis au présent de l'indicatif signifie que la satisfaction à une exigence est obligatoire pour la conformité à la présente norme;
- "il convient/il est recommandé" signifie que la satisfaction à une exigence est recommandée mais n'est pas obligatoire pour la conformité à la présente norme;
- "pouvoir" mis au présent de l'indicatif est utilisé pour décrire un moyen admissible pour satisfaire à une exigence; et.
- "établir" signifie définir, documenter et mettre en application.

Une liste de toutes les parties de la série CEI 80001, publiées sous le titre général *Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.**

# INTRODUCTION

De plus en plus de DISPOSITIFS MÉDICAUX sont conçus afin d'échanger des informations électroniquement avec d'autres appareils de l'environnement utilisateur, y compris d'autres DISPOSITIFS MÉDICAUX. Ces informations sont fréquemment échangées par l'intermédiaire d'un réseau de technologies de l'information (RÉSEAU TI) également capable de transférer des données de nature plus générale.

Parallèlement, les RÉSEAUX TI se révèlent de plus en plus vitaux pour l'environnement clinique et doivent désormais supporter des trafics de plus en plus diversifiés, allant des données essentielles à la vie du PATIENT nécessitant une livraison et une réaction immédiates à des données générales relatives aux actions d'entreprise et aux courriels dont le contenu est potentiellement malveillant (ex. les virus).

Pour de nombreuses collectivités publiques, la conception et la production des DISPOSITIFS MÉDICAUX sont soumises à des réglementations et à des normes reconnues par les autorités de réglementation. En général, les autorités de réglementation accordent leur attention aux fabricants de DISPOSITIFS MÉDICAUX, en exigeant des caractéristiques de conception ainsi qu'un PROCÉSSUS documenté pour la conception et la fabrication. Les DISPOSITIFS MÉDICAUX ne peuvent pas être mis sur le marché de ces collectivités publiques s'il n'a pas été clairement établi que ces exigences ont été remplies.

L'utilisation des DISPOSITIFS MÉDICAUX par le personnel médical est également soumise à des réglementations. Les membres du personnel médical doivent être correctement formés et qualifiés, et sont de plus en plus sujets à des PROCESSUS spécifiques, conçus afin de protéger les PATIENTS d'un RISQUE inacceptable.

Par contre, l'incorporation des DISPOSITIFS MÉDICAUX au sein de RÉSEAUX TI dans l'environnement clinique est beaucoup moins réglementée. Il est stipulé dans la CEI 60601-1:2005 [1][1)] que les fabricants de DISPOSITIFS MÉDICAUX doivent fournir certaines informations dans les DOCUMENTS D'ACCOMPAGNEMENT si le DISPOSITIF MÉDICAL est destiné à être connecté à un RÉSEAU TI. Il existe également des normes relatives aux activités associées aux technologies de l'information telles que la planification, la conception ainsi que la maintenance des RÉSEAUX TI. C'est le cas par exemple de l'ISO 20000-1:2005 [9]. Cependant, avant la publication de la présente norme, il n'existait aucune norme indiquant la manière dont les DISPOSITIFS MÉDICAUX peuvent être connectés aux RÉSEAUX TI, y compris aux RÉSEAUX TI généraux, afin d'obtenir l'INTEROPÉRABILITÉ sans compromettre l'organisation et la délivrance des soins en termes de SÉCURITÉ, EFFICACITÉ, et de SÉCURITÉ DES DONNÉES ET DES SYSTÈMES.

Il subsiste un certain nombre de problèmes potentiels liés à l'incorporation des DISPOSITIFS MÉDICAUX au sein des RÉSEAUX TI, tels que:

– l'absence de prise en considération du RISQUE engendré par l'utilisation de réseaux TI durant l'évaluation du RISQUE clinique;
– l'absence de soutien des fabricants de DISPOSITIFS MÉDICAUX dans l'incorporation de leurs produits au sein des RÉSEAUX TI, (ex. l'indisponibilité ou l'inadéquation des informations fournies par le fabricant à l'OPERATEUR du RÉSEAU TI);
– le fonctionnement incorrect ou les performances altérées (ex. incompatibilité ou configuration incorrecte) résultant de l'association de DISPOSITIFS MÉDICAUX et d'autres appareils sur le même RÉSEAU TI;
– le fonctionnement incorrect résultant de l'association de LOGICIELS DE DISPOSITIFS MÉDICAUX et d'autres applications logicielles (ex. systèmes ouverts de messagerie électronique ou jeux sur ordinateur) au sein du même RÉSEAU TI;

---

1) Les chiffres entre crochets se réfèrent à la Bibliographie.

– l'absence de contrôles de sécurité sur de nombreux DISPOSITIFS MÉDICAUX; et
– le conflit entre le besoin de contrôle strict des modifications apportées aux DISPOSITIFS MÉDICAUX et le besoin d'une réaction rapide face à la menace des cyberattaques.

Lorsque ces problèmes se manifestent, des conséquences indésirables surviennent fréquemment.

La présente norme s'adresse aux ORGANISMES RESPONSABLES, aux fabricants de DISPOSITIFS MÉDICAUX, ainsi qu'aux fournisseurs en technologies de l'information.

La présente norme adopte les principes suivants en tant que base pour les sections normatives et informatives:

– L'incorporation ou la suppression d'un DISPOSITIF MÉDICAL ou autres composants dans un RÉSEAU TI est une tâche nécessitant la conception de l'action; ceci pourrait se révéler hors de contrôle du fabricant du DISPOSITIF MÉDICAL.
– Il est recommandé que la GESTION DES RISQUES soit utilisée avant qu'un DISPOSITIF MÉDICAL ne soit incorporé au sein d'un RÉSEAU TI, et pour toute modification durant le cycle de vie entier du RÉSEAU TI contenant le DISPOSITIF MÉDICAL, afin d'éviter les RISQUES inacceptables, y compris le RISQUE pouvant affecter les PATIENTS, résultant de l'incorporation du DISPOSITIF MÉDICAL au sein du RÉSEAU TI. Plusieurs critères rentrent en ligne de compte lors d'une décision relative au RISQUE comme la fiabilité, le coût ou l'impact sur la mission. Il convient qu'ils soient pris en compte lors de la détermination des RISQUES acceptables tout comme les exigences décrites dans la présente norme.
– Il convient que les aspects relatifs à la suppression, à la maintenance, au changement ou à la modification des appareils, des éléments ou des composants soient correctement abordés en plus de l'incorporation des DISPOSITIFS MÉDICAUX.
– Le fabricant d'un DISPOSITIF MÉDICAL est responsable de la GESTION DES RISQUES de ce DISPOSITIF MÉDICAL lors de sa conception, de son implémentation et de sa fabrication. La présente norme ne couvre pas le PROCESSUS DE GESTION DES RISQUES pour le DISPOSITIF MÉDICAL.
– Le fabricant d'un DISPOSITIF MÉDICAL destiné à être incorporé au sein d'un RÉSEAU TI pourrait être amené à fournir des informations relatives au DISPOSITIF MÉDICAL, informations se révélant nécessaires afin de permettre à l'ORGANISME RESPONSABLE de contrôler les RISQUES conformément à la présente norme. Ces informations peuvent inclure, dans les DOCUMENTS D'ACCOMPAGNEMENT, les instructions s'adressant spécifiquement à la personne incorporant un DISPOSITIF MÉDICAL dans un RÉSEAU TI.
– Il convient que ces DOCUMENTS D'ACCOMPAGNEMENT communiquent les instructions à suivre lors de l'incorporation du DISPOSITIF MÉDICAL au sein du RÉSEAU TI, ainsi que la manière dont le DISPOSITIF MÉDICAL transfère les informations sur le RÉSEAU TI, et fassent état des caractéristiques minimales du RÉSEAU TI nécessaires afin d'assurer l'EMPLOI PRÉVU du DISPOSITIF MÉDICAL lorsque ce dernier est incorporé au sein du RÉSEAU TI. Il convient que les DOCUMENTS D'ACCOMPAGNEMENT avertissent des situations dangereuses possibles associées à la défaillance ou aux interruptions du RÉSEAU TI et à la mauvaise utilisation de la connexion au RÉSEAU TI ou des informations qui sont transférées sur le RÉSEAU TI.

– Des ACCORDS DE RESPONSABILITÉ peuvent établir les fonctions et responsabilités des acteurs impliqués dans l'incorporation d'un DISPOSITIF MÉDICAL au sein d'un RÉSEAU TI, tous les aspects du cycle de vie du RÉSEAU TI MÉDICAL qui en résulte ainsi que toutes les activités faisant partie de ce cycle de vie.

– L'ORGANISME RESPONSABLE doit affecter les personnes à certaines fonctions définies dans la présente norme. La présente norme définit les responsabilités inhérentes à ces fonctions. La plus importante de ces fonctions est celle de GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL. Cette fonction peut être attribuée à une personne de l'ORGANISME RESPONSABLE ou à un fournisseur externe.

– Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL est chargé de s'assurer que la GESTION DES RISQUES est incluse au cours des PROCESSUS suivants:

  - la planification et la conception des nouvelles incorporations de DISPOSITIFS MÉDICAUX ou les modifications apportées à ces incorporations;
  - la mise en service du RÉSEAU TI MÉDICAL et son utilisation; et
  - la GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et la gestion des modifications du RÉSEAU TI durant le cycle de vie entier du RÉSEAU TI.

– Il convient que la GESTION DES RISQUES s'applique afin d'aborder les PROPRIÉTÉS CLÉS suivantes appropriées au RÉSEAU TI comportant un DISPOSITIF MÉDICAL:

  - SÉCURITÉ (absence de RISQUE inacceptable d'une blessure physique ou d'une atteinte à la santé des personnes ou de dommages sur les biens ou l'environnement);

- EFFICACITÉ (capacité à obtenir le résultat prévu pour le patient et l'ORGANISME RESPONSABLE);
- SÉCURITÉ DES DONNÉES ET DU SYSTÈME (un état de fonctionnement d'un RÉSEAU TI MÉDICAL dans lequel les éléments d'actif informationnel (données et systèmes) sont suffisamment protégés de l'altération en matière de confidentialité, d'intégrité et de disponibilité).

# APPLICATION DE LA GESTION DES RISQUES AUX RÉSEAUX DES TECHNOLOGIES DE L'INFORMATION CONTENANT DES DISPOSITIFS MÉDICAUX –

## Partie 1: Fonctions, responsabilités et activités

## 1 Domaine d'application

Etant donné que les DISPOSITIFS MÉDICAUX sont incorporés dans des RÉSEAUX TI afin d'en tirer des bénéfices (par exemple, l'INTEROPÉRABILITÉ), la présente norme internationale définit les fonctions, responsabilités et activités nécessaires à la GESTION DES RISQUES des RÉSEAUX TI comportant des DISPOSITIFS MÉDICAUX afin de traiter la SÉCURITÉ, L'EFFICACITÉ et la SÉCURITÉ DES DONNÉES ET DU SYSTÈME (les PROPRIÉTÉS CLÉS). La présente norme internationale ne spécifie pas les niveaux de RISQUES acceptables.

NOTE 1 Les activités de GESTION DES RISQUES décrites dans la présente norme sont tirées de celles de l'ISO 14971 [4]. La relation entre l'ISO 14971 et la présente norme est décrite à l'Annexe A.

La présente norme s'applique dès lors qu'un DISPOSITIF MÉDICAL a été acquis par un ORGANISME RESPONSABLE et qu'il est envisagé de l'incorporer dans un RÉSEAU IT.

NOTE 2 La présente norme ne couvre pas la GESTION DES RISQUES avant mise sur le marché.

La présente norme s'applique tout au long du cycle de vie des RÉSEAUX TI comportant des DISPOSITIFS MÉDICAUX.

NOTE 3 Les activités de gestion du cycle de vie décrites dans la présente norme sont très proches de celles de l'ISO/CEI 20000-2 [10]. La relation entre l'ISO/CEI 20000-2 et la présente norme est décrite à l'Annexe D.

La présente norme s'applique lorsqu'il n'existe aucun fabricant de DISPOSITIFS MÉDICAUX se portant responsable de la définition des PROPRIÉTÉS CLÉS du RÉSEAU TI comportant un DISPOSITIF MÉDICAL.

NOTE 4 Si un fabricant individuel décrit un DISPOSITIF MÉDICAL complet comportant un réseau, l'installation ou l'assemblage du DISPOSITIF MÉDICAL conformément aux DOCUMENTS D'ACCOMPAGNEMENT du fabricant n'est pas soumis aux spécifications de la présente norme quelle que soit la personne installant ou assemblant le DISPOSITIF MÉDICAL.

NOTE 5 Si un fabricant individuel décrit un DISPOSITIF MÉDICAL complet comportant un réseau, les ajouts effectués à ce DISPOSITIF MÉDICAL ou les modifications apportées à la configuration de ce DISPOSITIF MÉDICAL, autres que ceux décrits par le fabricant, sont soumis aux spécifications de la présente norme.

La présente norme s'applique aux ORGANISMES RESPONSABLES, aux fabricants de DISPOSITIFS MÉDICAUX et aux fournisseurs d'autres technologies de l'information pour les besoins de la GESTION DES RISQUES d'un RÉSEAU IT incorporant des DISPOSITIFS MÉDICAUX tels que spécifiés par l'ORGANISME RESPONSABLE.

La présente norme ne s'applique pas aux applications d'utilisation personnelle où le PATIENT, l'OPERATEUR et l'ORGANISME RESPONSABLE ne désignent qu'une seule et même personne.

NOTE 6 Lorsqu'un DISPOSITIF MÉDICAL est utilisé à domicile sous la surveillance et/ou dans le respect des instructions du fournisseur, ce fournisseur est considéré comme L'ORGANISME RESPONSABLE. L'utilisation à titre personnel où le patient acquiert et utilise un DISPOSITIF MÉDICAL sans la surveillance ou les instructions d'un fournisseur ne relève pas du domaine d'application de la présente norme.

La présente norme ne couvre pas les exigences réglementaires ou légales.