

# IEC 80001-1:2021-09 (E/F)

## Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management

## Sécurité, efficacité et sûreté dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés - Partie 1: Application de la gestion des risques

---

<b>Contents</b>	<b>Page</b>
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
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

## SOMMAIRE

AVANT-PROPOS .....	40
INTRODUCTION.....	43
1 Domaine d'application .....	45
2 Références normatives .....	45
3 Termes et définitions .....	45
4 Principes .....	46
5 Cadre .....	47
5.1 Généralités .....	47
5.2 Leadership et engagement.....	47
5.3 Intégration de la GESTION DES RISQUES.....	48
5.4 Conception/planification.....	48
5.4.1 Généralités .....	48
5.4.2 DOSSIER DE GESTION DES RISQUES .....	49
5.4.3 Comprendre l'organisation et l'ECOSYSTEME SOCIOTECHNIQUE .....	49
5.4.4 Articulation de l'engagement en matière de GESTION DES RISQUES .....	49
5.4.5 Attribution de rôles, autorités, responsabilités et imputabilités dans l'organisation .....	49
5.4.6 Allocation de ressources.....	50
5.4.7 Établissement de la communication et de la consultation.....	50
5.5 Mise en œuvre .....	51
5.6 Évaluation.....	51
5.7 Amélioration.....	51
6 PROCESSUS DE GESTION DES RISQUES .....	52
6.1 Exigences générales.....	52
6.1.1 Généralités .....	52
6.1.2 ANALYSE DU RISQUE .....	52
6.1.3 ÉVALUATION DU RISQUE .....	55
6.1.4 MAITRISE DU RISQUE.....	55
6.2 Exigences spécifiques au cycle de vie .....	58
6.2.1 Généralités .....	58
6.2.2 Acquisition.....	58
6.2.3 Installation, personnalisation et configuration .....	58
6.2.4 Intégration, migration de données, transition et validation.....	59
6.2.5 Mise en œuvre, optimisation du flux de travaux et formation.....	59
6.2.6 Exploitation et maintenance.....	59
6.2.7 Mise hors service.....	61
Annexe A (informative) Tableau de correspondance des exigences de l'IEC 80001-1 .....	62
Annexe B (informative) Recommandations pour les informations dans les documents d'accompagnement.....	69
B.1 Avant-propos .....	69
B.2 Catégorisation du système d'information.....	70
B.3 Vue d'ensemble .....	70
B.4 Documents de référence .....	70
B.5 Description à l'échelle du système .....	70
B.5.1 Description de l'environnement.....	70
B.5.2 Accès, protocoles et services du réseau .....	71

B.5.3	Objet de la connexion à l'infrastructure TI de santé .....	71
B.5.4	Exigences de mise en réseau .....	71
B.5.5	Services des réseaux TI exigés .....	71
B.5.6	Flux de données et protocoles de données .....	71
B.6	Sécurité et accès utilisateur .....	72
B.6.1	Généralités .....	72
B.6.2	Logiciel malveillant / antivirus / liste blanche .....	72
B.6.3	Exclusions en matière de sécurité .....	72
B.6.4	Accès au système.....	73
B.7	GESTION DES RISQUES .....	74
	Bibliographie.....	75

Figure 1 – Cadre de cycle de vie traitant de la sécurité, de l'efficacité et de la sûreté des logiciels de santé et des systèmes TI de santé .....	44
--	----

Figure 2 – PROCESSUS DE GESTION DES RISQUES.....	48
--	----

Tableau A.1 – Tableau des exigences de l'IEC 80001-1.....	62
---	----

Tableau B.1– Nom et emplacement de l'organisation .....	69
---	----

Tableau B.2 – Niveau de caractérisation des dispositifs de cybersécurité .....	70
--	----

Tableau B.3 – Accès, protocoles et services .....	71
---	----

Tableau B.4 – Nom et titre du système d'information .....	72
---	----

Tableau B.5 – Rôles et privilèges.....	73
--	----