

ICS 35.240.80

CCS C 30



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 44585.1-2024

**Application of risk management for medical device connecting IT-network - Part
1: Safety, effectiveness and security in the implementation and use of connected
medical devices or connected health software**

风险管理在接入IT网络的医疗器械中的应用 第1部分：联网医疗器械或健康软件
在其实施和使用中的安全、有效性和网络安全

(English Translation)

Issued on: September 29, 2024

Implemented on: April 1, 2026

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Principles
5 Framework
5.1 Overview
5.2 Leadership and Commitment
5.3 Integrated Risk Management
5.4 Design/Planning
5.5 Implementation
5.6 Evaluation
5.7 Improvements
6 Risk Management Process
6.1 General requirements
6.2 Specific requirements for the life cycle
Appendix A (Informative) Mapping table of requirements of this document
Appendix B (Informative) Information Guide for Accompanying Documents
References

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting is required.

This document is Part 1 of GB/T 44585 "Application of risk management in medical devices connected to IT networks".

The following parts have been published.

Part 1: Safety, effectiveness and cybersecurity of networked medical devices or health software in their implementation and use.

This document is modified to adopt IEC 80001-1:2021 "Application of risk management to

IT networks containing medical devices - Part 1: Networked medical devices" Safety, effectiveness and cybersecurity of medical devices or health software in their implementation and use.

The technical differences between this document and IEC 80001-1:2021 and their reasons are as follows.

Added "Safety", "Assurance Case", "Change-Release Management", "Risk", "Risk Analysis", "Risk Estimation", "Risk Management", "Risk Control", "Risk Assessment", "Risk Evaluation", "Key Attributes", "Administrator", "Integrator", "Health IT", "Health IT Infrastructure", "Health IT Systems", "Health Software", "Role", "Availability", "Harm", "Society Technical Ecosystem", "Residual Risk", "Accompanying Documents", "Accompanying Files", "Accompanying Materials", "Cybersecurity", "Cyber Security capability", "Danger", "Threat", "Verification", "Severity", "Healthcare provider", "User", "Manufacturing Terms and definitions for "component", "asset", "component", "organization" and "top management" (see Chapter 3) (IEC 80001-1:2021 it inherits the terminology of ISO 81001-1:2021, but ISO 81001-1:2021 has not been converted into Chinese standards. Therefore, based on the differences, the terminology of ISO 81001-1:2021 has been added.

Added terms mentioned in ISO 81001-1:2021 for use in IEC 80001-1:2021);

The definitions of the terms "validation" and "process" have been changed to be consistent with GB/T 19000-2016.-the following editorial changes were made to this document.

The name of the standard was changed to Application of Risk Management to Medical Devices Connected to IT Networks Part 1: Networked Medical Devices or Health Devices Safety, effectiveness and network security of health software in its implementation and use";

The content format of Appendix B has been changed. -

Introduction

While the benefits of digital health are widely accepted, concerns remain about the safety, efficacy, and cybersecurity of health software and health IT systems.

The potential for unexpected and adverse effects is becoming increasingly apparent. Today's advanced health software and health IT systems provide advanced decision support.

However, in addition to the benefits to patients and the medical system, it also increases the possibility of harm to patients and medical institutions due to adverse events caused by software.

Healthcare providers rely on secure, effective, and cyber-secure systems as a critical element of their operations.

Poor management of the implementation and use of Internet systems may threaten their ability to provide health services.

Networked systems that deliver health services often involve multiple software applications, multiple medical devices, and complex health IT systems.

The system relies on a healthy IT infrastructure, including wired or wireless networks, point-to-point connections, application servers and data storage, interface engines, and Health IT infrastructure is typically used for clinical functions (e.g., patient monitoring systems) and non-clinical components.

Organizational functions (e.g., accounting, scheduling, social networking, multimedia, file sharing). Systems connected through the health IT infrastructure these range from small departmental networks to large integrated infrastructures across multiple locations, as well as cloud-based networks operated by third parties.

The requirements in this document apply to the application of risk management to systems that include health IT systems and/or health IT infrastructure.

multiple stakeholders.

Managing the safety, efficacy, and cybersecurity of health software and health IT systems, including medical devices, requires a comprehensive and coordinated approach.

To optimize these three attributes, many organizations and roles are involved in the entire life cycle of health software and health IT systems (see Figure 1).

This document covers the implementation and clinical use phases of the life cycle, while other related documents will cover different technical features.

At this stage, the application of the guidance or requirements are proposed, such as wireless network guidance, general implementation guidance, distributed alarm system guidance.

South et al.

This document helps organizations use or adapt, where feasible, existing work practices and processes, people and tools to meet the requirements of this document.

For example, if the organization has an existing risk management process, use or adapt that process to support safety, effectiveness, and cybersecurity.

Three key attributes. Defines requirements so that they can be evaluated and therefore supports the organization in validating and demonstrating conformity to this document.

GB/T 44585 "Application of risk management in medical devices connected to IT networks" stipulates the requirements for networked medical devices by various stakeholders.

It is intended to consist of one part, which contains general requirements on how risk

management should be applied during the life cycle of mechanical or health software.

Part 1: Safety, effectiveness and cybersecurity of networked medical devices or health software in their implementation and use.

Organizations can ensure that health IT systems are connected within the health IT infrastructure before, during, and after the health IT systems are connected.

These three key attributes are addressed in a manner that involves stakeholders and applies the general requirements for risk management.

Figure 1 Life cycle framework involving safety, availability, and cybersecurity of health software and health IT systems

Risk management in IT network access Application in medical devices Part 1:
Internet-connected medical devices or health software safety in its implementation and use,
Validity and Cybersecurity

1 Scope

This document defines the procedures that organizations should follow before, during, and after connecting health IT systems within the health IT infrastructure by simultaneously enabling appropriate the three key attributes of safety, availability and cybersecurity are addressed in a way that involves stakeholders.

Require.

This document applies to risk management of connected medical devices or health software during the implementation and use phases of their life cycle.

2 Normative references

This document has no normative references.

3 Terms and definitions

The following terms and definitions apply to this document.

consequence

The result of an event affecting a target.

Note 1 to entry. Consequences may be definite or indefinite and may have a positive or negative direct or indirect impact on objectives.

Note 2 to entry. Consequences may be expressed qualitatively or quantitatively.

Note 3: Any consequences may escalate through chain reactions and cumulative effects.

[Source. GB/T 24353-2022, 3.6, modified] 3.2 Healthcare Nursing activities, services,