Technical Specification

ISO/TS 11633-1

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 1: Requirements and risk analysis

Informatique de santé — Management de la sécurité de l'information pour la maintenance à distance des dispositifs médicaux et des systèmes d'information médicale —

Partie 1: Exigences et analyse du risque

Second edition
2026-09

Reference number
ISO/TS 11633-1:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 3

4 Contents of RMS of medical devices and medical information systems **3**
4.1 Assumed RMS architecture 3
4.2 RMS using one to one communication on telephone network 4
4.2.1 One to one communication on telephone network features 4
4.2.2 Security features for one to one communication on telephone network 4
4.3 RMS using the Internet connections 5
4.3.1 Internet connections features 5
4.3.2 Security features for internet connections 5

5 Security requirement and risk analysis of RMS of medical devices and medical information systems **5**
5.1 Risk analysis 5
5.2 Security measures in RMS operation 6
5.3 Contracts involving HCF, RSC, and necessary third parties 6
5.4 Protection of personal information 6
5.5 Management measures 7

Annex A (informative) **Use cases of RMSs** **8**

Annex B (informative) **Examples of threats by assets of remote maintenance services** **13**

Annex C (informative) **Example of how to conduct risk analysis** **18**

Bibliography **19**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO/TS 11633-1:2019), which has been technically revised.

The main changes are as follows:

— complete revision to correspond to the latest editions of ISO/IEC 27001 and ISO/IEC 27002;

— revision of the clause structure;

— update of Clause 3 and the Bibliography.

A list of all parts in the ISO 11633 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Advancement of information and communications technology (ICT) has changed how networks are used in society. Similarly, in healthcare, information systems which were once closed in each healthcare facility (HCF) are now connected to the outside by networks and are progressing to the point of being able to facilitate sharing and exchange of health information accumulated in these information systems. Such information and communication networks are spreading not only in between HCFs but also between HCFs and vendors of medical devices and healthcare information systems. Maintenance of such systems is paramount to keeping them up-to-date. By practicing remote maintenance services (RMS), it becomes possible to reduce down-time and lower costs for this maintenance activity.

While there are benefits to remote maintenance, such remote connections with external organizations also expose HCFs and vendors to risks regarding confidentiality, integrity and availability of information and systems, risks which previously received scant consideration.

Although normal remote maintenance is generally done on a contract basis, in the case of medical devices, risk assessment is commonly a legal prerequisite. Therefore, it is necessary to implement appropriate risk assessment where remote maintenance is provided in any healthcare context. The risk assessment examples provided in ISO/TR 11633-2 provide support for HCFs and RMS providers to implement risk assessment effectively.

By implementing the risk assessment process and employing controls referencing ISO/TR 11633-2, HCFs owners and RMS providers will be able to obtain the following benefits:

— Risk assessment can result in improved efficiency. If the risk assessment document created through the use of ISO/TR 11633-2 does not fully conform to ISO/IEC 27001, it can be used in part in a risk assessment of an incompatible area, thus reducing the risk assessment effort required.

— Documented validity of the RMS security countermeasures in place will be available to third parties.

If providing RMS to two or more sites, the provider can apply countermeasures consistently and effectively.

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 1: Requirements and risk analysis

1 Scope

This document specifies requirements and recommendations for remote maintenance services (RMSs) of medical devices and medical information systems in healthcare facilities (HCFs). This document is applicable to HCFs and remote service centres (RSCs) providing remote maintenance services for medical devices and medical information systems.

This document specifies the risk assessment necessary to protect remote maintenance activities, taking into consideration the special characteristics of the healthcare field such as patient safety, regulations and privacy protections.

This document provides practical examples of risk analysis to protect both the HCF and RMS provider information assets in a safe and efficient (i.e. economical) manner. These assets are primarily the information system itself and personal health data held in the information system.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms and definitions

3.1.1
asset
anything that has value to the organization

Note 1 to entry: In the context of health *information security* (3.1.4), information assets include:

a) health information;

b) technical information (credentials, passwords, calibration data, etc.);

c) non-health information (e.g. financials, administrative, legal, human resources);

d) IT services;