PD ISO/TS 11633-1:2019

BSI Standards Publication

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

Part 1: Requirements and risk analysis

bsi.

National foreword

This Published Document is the UK implementation of ISO/TS 11633-1:2019. It supersedes PD ISO/TR 11633-1:2009, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2019

ISBN 978 0 580 52444 8

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 August 2019.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 11633-1:2019

TECHNICAL SPECIFICATION

ISO/TS 11633-1

First edition
2019-08

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

Reference number
ISO/TS 11633-1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 and definitions **1**
4 An outline of RMS security of medical devices and medical information systems **2**
4.1 Contents of RMS security of medical devices and medical information systems 2
4.1.1 General 2
4.1.2 RMS using a public switched telephone network 3
4.1.3 RMS using the Internet 4
4.2 Security requirement of RMS of medical devices and medical information systems 4
4.2.1 General 4
4.2.2 Security measures in RMS operation 4
4.2.3 Contracts between HCF and RSC including 3rd parties 4
4.2.4 Protection of personal information 4
4.3 Roles of RSC and HCF 5
5 Risk analysis **5**
Annex A (informative) **Use case of RMSs** **6**
Annex B (informative) **Example of risk analysis result of remote maintenance services** **11**
Annex C (informative) **Example of risk analysis criteria** **15**
Bibliography **16**

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 first edition cancels and replaces ISO/TR 11633-1:2009, which has been technically revised. The main changes compared to the previous edition are as follows:

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

— addition of use case 'remote monitoring'.

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

The advancement and spread of technology in the information and communication technology field, and the infrastructure based on them, have brought many changes in how technology and networks are used in modern 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 mutual use 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 so-called 'remote maintenance services', it becomes possible to reduce down-time and lower costs for this maintenance activity.

Whilst 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.

TECHNICAL SPECIFICATION **ISO/TS 11633-1:2019(E)**

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 focuses on remote maintenance services (RMS) for information systems in healthcare facilities (HCFs) as provided by vendors of medical devices and health 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 and definitions

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

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

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

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

3.1
asset
anything that has value to the organization

[SOURCE: ISO/IEC 21827:2008, 3.4]

Note 1 to entry: In the context of health information security, 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, etc.),

d) IT services,

e) hardware,

f) software,

g) communications facilities,