TECHNICAL REPORT

ISO/TR 11633-2

Second edition
2021-02

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

Part 2: Implementation of an information security management system (ISMS)

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 2: Mise en œuvre d'un système de management de la sécurité de l'information (ISMS)

Reference number
ISO/TR 11633-2:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 and definitions **1**
4 Application of ISMS to remote maintenance services **1**
4.1 Overview 1
4.2 Compliance scope 3
4.3 Security policy 3
4.4 Assessing risks 4
4.5 Risks to be managed 4
4.6 Identification of risks that are not described in this document 5
4.7 Treating risks 5
5 Security management measures for remote maintenance services **6**
6 Approving residual risks **6**
7 Security audit **7**
7.1 Security audit of remote maintenance services 7
7.2 Recommendation of security audit by third parties 7
Annex A (informative) **Example of risk assessment in remote maintenance services** **8**
Bibliography **70**

© ISO 2021 – All rights reserved

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 second edition cancels and replaces the first edition (ISO/TR 11633-2:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

— complete revision of the bibliography;

— update of Figure 1;

— update of Annex A.

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.

© ISO 2021 – All rights reserved

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 once closed systems in each healthcare facility (HCF) are now connected 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' (RMS), 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.

This document stipulates the risk assessment to protect remote maintenance activities, taking into consideration the special characteristics of the healthcare field such as patient safety, and applicable requirements and privacy protections. 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, appropriate risk assessment where remote maintenance is provided in any healthcare context should be implemented. The risk assessment examples provided in this document support for HCFs and RMS providers to implement risk assessment effectively.

By implementing the risk assessment process and employing controls referenced in this document, 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 this document, does not fully conform, it may 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.

© ISO 2021 – All rights reserved

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

Part 2: Implementation of an information security management system (ISMS)

1 Scope

This document gives a guideline for implementation of an ISMS by showing practical examples of risk analysis on remote maintenance services (RMS) for information systems in healthcare facilities (HCFs) as provided by vendors of medical devices or health information systems in order to protect both sides' information assets (primarily the information system itself and personal health data) in a safe and efficient (i.e. economical) manner.

This document consists of:

— application of ISMS to RMS;

— security management measures for RMS;

— an example of the evaluation and effectiveness based on the "controls" defined in the ISMS.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 11633-1 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/

4 Application of ISMS to remote maintenance services

4.1 Overview

The information security management system (ISMS) is a mechanism that operates as a series of plan/do/check/act processes under the security policy. This series of processes means that the organization plans out proper security measures (plan), puts those security measures into practice (do), reviews those security measures (check), and reconsiders them if necessary (act). The ISMS is already

© ISO 2021 – All rights reserved