

This is a preview of "ISO/TR 11633-1:2009". [Click here to purchase the full version from the ANSI store.](#)

First edition  
2009-11-15

---

---

# 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/TR 11633-1:2009(E)

© ISO 2009

This is a preview of "ISO/TR 11633-1:2009". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/TR 11633-1:2009". [Click here to purchase the full version from the ANSI store.](#)

## Contents

Page

Foreword .....	iv
Introduction.....	v
1 Scope .....	1
2 Terms and definitions .....	1
3 Abbreviated terms .....	3
4 An outline of remote maintenance services security .....	3
4.1 Contents of remote maintenance services security .....	3
4.2 Security requirement of remote maintenance services .....	5
4.3 Roles of remote service centre and healthcare organization .....	6
5 Use case of remote maintenance services .....	7
5.1 Introduction.....	7
5.2 Trouble shooting for outages .....	8
5.3 Scheduled maintenance .....	9
5.4 Software updating .....	10
6 Risk analysis .....	11
6.1 General .....	11
6.2 Risk analysis criteria .....	11
Annex A (informative) Example of risk analysis result of remote maintenance services .....	12
Bibliography.....	17

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/TR 11633-1 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO/TR 11633 consists of the following parts, under the general title *Health informatics — Information security management for remote maintenance of medical devices and medical information systems*:

- *Part 1: Requirements and risk analysis*
- *Part 2: Implementation of an information security management system (ISMS)*

This is a preview of "ISO/TR 11633-1:2009". [Click here to purchase the full version from the ANSI store.](#)

## Introduction

Progress and spread of technology in information and communication fields and well-arranged infrastructure based on them have brought various changes into modern society. In the healthcare field, information systems formerly closed in each healthcare facility are now connected by networks, and they are coming to the point of being able to facilitate mutual use of health information accumulated in each information system. Such information and communication networks are spreading, not only amongst healthcare facilities but also amongst healthcare facilities and vendors of medical devices or healthcare information systems. By practicing so-called "remote maintenance services" (RMS), it becomes possible to reduce down-time and lower costs.

However, such connections with external organizations have come to bring healthcare facilities and vendors not only benefits but also risks regarding confidentiality, integrity and availability of information and systems, risks which previously received scant consideration.

Based on the information offered by this part of ISO/TR 11633, healthcare facilities and RMS providers will be able to perform the following activities:

- clarify risks originating from using the RMS, where environmental conditions of the requesting vendor site (RSC) and maintenance target healthcare facility site (HCF) can be selected from the catalogue in Annex A;
- grasp the essentials of selecting and implementing both technical and non-technical "controls" to be applied in their own facility against the risks described in this part of ISO/TR 11633;
- request concrete countermeasures from business partners, as this document can identify the relevant security risks;
- clarify the boundary of responsibility between the healthcare facility owner and the RMS provider;
- plan a programme for risk retention or transfer as residual risks are clarified when selecting the appropriate "controls".

By implementing the risk assessment and employing "controls" referencing this part of ISO/TR 11633, healthcare facilities owners and RMS providers will be able to obtain the following benefits:

- it will only be necessary to do the risk assessment for those organizational areas where this part of ISO/TR 11633 is not applicable, therefore, the risk assessment effort can be significantly reduced;
- it will be easy to show the validity of the RMS security countermeasures to a third party;
- if providing RMS to two or more sites, the provider can apply countermeasures consistently and efficiently.