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

Part 1:

Requirements and risk analysis

iTeh STANDARD PREVIEW

(standards) (En) all
*Informatique de santé — Management de la sécurité de l'information
pour la maintenance à distance des dispositifs médicaux et des
systèmes d'information médicale —*

ISO/TR 11633-1:2009
Partie 1: Exigences et analyse du risque

<https://standards.iteh.ai/catalog/standards/sist/51ec05d0-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>



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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TR 11633-1:2009](https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>



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
Web www.iso.org

Published in Switzerland

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

<https://standards.itech.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>

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)*

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TR 11633-1:2009](https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>

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

Part 1: Requirements and risk analysis

1 Scope

This part of ISO/TR 11633 focuses on remote maintenance services (RMS) for information systems in healthcare facilities as provided by vendors of medical devices or health information systems (RMS providers) and shows an example of carrying out a risk analysis 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 part of ISO/TR 11633 consists of:

- a catalogue of use cases for RMS;
- a catalogue of information assets in healthcare facilities (HCF) and RMS providers;
- an example of the risk analysis based on use cases.

<https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>

2 Terms and definitions

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

2.1

accountability

property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO/IEC 13335-1:2004, definition 2.1]

2.2

asset

anything that is of value to the organization

NOTE 1 Adapted from ISO/IEC 13335-1.

NOTE 2 In the context of health information security, information assets include:

- a) health information;
- b) IT services;
- c) hardware;
- d) software;
- e) communication facilities;
- f) media;
- g) IT facilities;
- h) medical devices that record or report data.

2.3 assurance
result of a set of compliance processes through which an organization achieves confidence in the status of its information security management

2.4 availability
property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 13335-1:2004, definition 2.4]

2.5 compliance assessment
processes by which an organization confirms that the information security controls put in place remain both operational and effective

NOTE Legal compliance relates specifically to the security controls put in place to deliver the requirements of relevant legislation such as the European Union Directive on the protection of personal data.

2.6 confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO/IEC 13335-1:2004, definition 2.6]

2.7 data integrity
property that data have not been altered or destroyed in an unauthorized manner

[ISO/IEC 9797-1:1999, definition 3.1.1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.8 information governance <https://standards.iteh.ai/catalog/standards/sist/51ec05d6-844a-4980-bfa2-11633-1-2009>
processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed

2.9 information security
preservation of confidentiality, integrity and availability of information

NOTE Other properties, particularly accountability of users, but also authenticity, non-repudiation, and reliability, are often mentioned as aspects of information security, but could be considered as derived from the three core properties in the definition.

2.10 risk
combination of the probability of an event and its consequence

[ISO/IEC Guide 73:2002, definition 3.1.1]

2.11 risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002, definition 3.3.1]

2.12 risk management
coordinated activities to direct and control an organization with regard to risk

NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

[ISO/IEC Guide 73:2002, definition 3.1.7]

2.13**risk treatment**

process of selection and implementation of measures to modify (typically reduce) **risk**

NOTE Adapted from ISO/IEC Guide 73:2002.

2.14**system integrity**

property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system

2.15**threat**

potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE Adapted from ISO/IEC 13335-1.

2.16**vulnerability**

weakness of an asset or group of assets that can be exploited by a threat

NOTE Adapted from ISO/IEC 13335-1.

3 Abbreviated terms

- iTeh STANDARD PREVIEW**
(standards.iteh.ai)
- HCF Healthcare facility
- ISP Information-stealing programme
- PHI Personal health information
- RMS Remote maintenance services
- RSC Remote maintenance service centre
- RSS Remote maintenance service security
- VPN Virtual private network

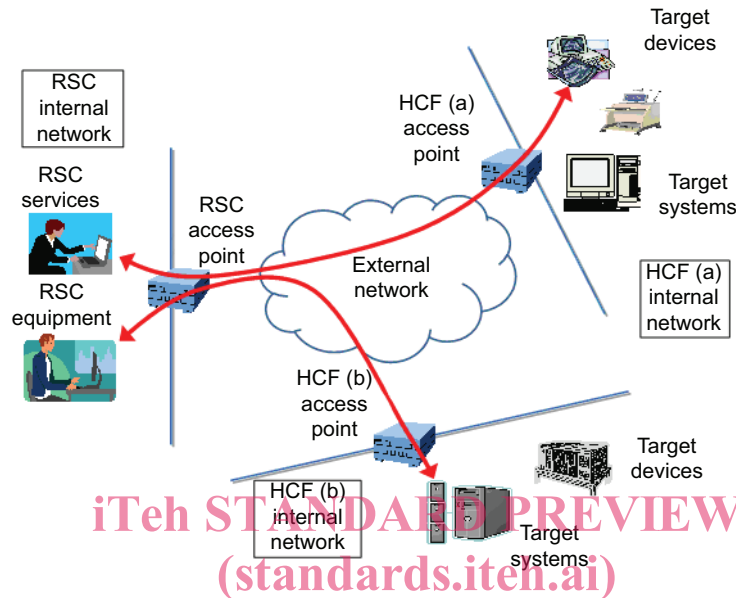
4 An outline of remote maintenance services security**4.1 Contents of remote maintenance services security****4.1.1 General**

Remote maintenance services (RMS) have three main purposes:

- response at the time of medical equipment malfunction;
- routine maintenance;
- updating of the software.

In this part of ISO/TR 11633, a system which consists of target devices and an internal network within healthcare facilities (HCF) site, an external network connecting HCF and remote maintenance service centre (RSC), and an internal network and equipments or services within RSC is assumed. See Figure 1.

This part of ISO/TR 11633 introduces the styles of the RMS that each RMS provider provides and the current state of the security measures.



ISO/TR 11633-1:2009
Figure 1 — Assumed remote maintenance services
<https://standards.iteh.ai/catalog/standards/sist/51ecc05d6-844a-4980-bfa2-35165c711434/iso-tr-11633-1-2009>

4.1.2 Styles of remote maintenance services and technical security measures

4.1.2.1 Remote maintenance services using a public switched telephone network

HCF sets up a machine for dial-up server function. This machine connects with a public switched telephone network by modem, etc., and waits for access from RSC remote equipment. Telecommunications equipment that offers all functions such as dial-up routers are in widespread use.

In the use of the public switched telephone network, telecommunication lines have the following features:

- a one-to-one communication pathway between HCF and RSC can be secured;
- tapping is difficult because a public switched telephone network is fully-digitalized.

Using these features, security is maintained by the following technical measures:

- a) determination of caller number — use of call back certification function or caller ID specification certification function;
- b) user certification — use of one-time password and encryption of password;
- c) review of communication audit log — detection of illegal access to a computer.

4.1.2.2 Remote maintenance services using the Internet

A device for internet connection with fixed global IP address is placed on the HCF. The RSC prepares the Internet connection environment and connects itself to HCF through the Internet.

This part of ISO/TR 11633 specifies more technologies for communication and user authentication between HCF and RSC, because this is the same as a typical Internet connection and not a one-to-one communication like the public switched telephone network.

This part of ISO/TR 11633 illustrates the following examples:

- a) erecting a fire-wall;
- b) using tools such as anti-virus software;
- c) communication using VPN for encryption of the communication path;
- d) use of a variety of user authentication methods such as one-time passwords, password encryption and use of digital certificates.

4.2 Security requirement of remote maintenance services

4.2.1 Security measures in remote maintenance service operation

Regulations are commonly used to securely operate the system and protect the privacy of personal information. This part of ISO/TR 11633 illustrates the following examples of regulation:

- a) regulations concerning RSC operator;
- b) regulation measures for excluding from the operation of RSC remote terminals those who are not authorized;
- c) regulations when RSC remote terminals are increased and moved;
- d) regulations concerning access from mobile terminals.

4.2.2 Contracts between HCF and RCS

The following regulations may have been put in place in case of unexpected accidents:

- a) regulations for the delineation of responsibility between the HCF and RSC;
- b) conclusion of contracts concerning confidentiality of information.

There are various means for providing security measures in an RMS. Each RMS provider maintains security by using these means with original regulations.

However, this part of ISO/TR 11633 envisages that the expense for security will increase, and maintaining the security level will become more difficult for the HCF in the future, because methods used differ depending on the RMS provider.

4.2.3 Protection of personal information and remote maintenance services

4.2.3.1 Privacy protection of health information in healthcare organizations

Because of jurisdictional privacy protection acts, the management of personal information confidentiality is shifting from physicians to the establishment of the right of control over information and its privacy protection by patients themselves.

Healthcare organizations are required to manage personal information, explain the risks to the confidentiality of personal information to the patient, and to ensure that healthcare professionals do not use health information outside the purpose for which it was collected.