TECHNICAL REPORT

ISO/TR 11633-1

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 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

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.

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.

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]

2.8
information governance
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

— 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.

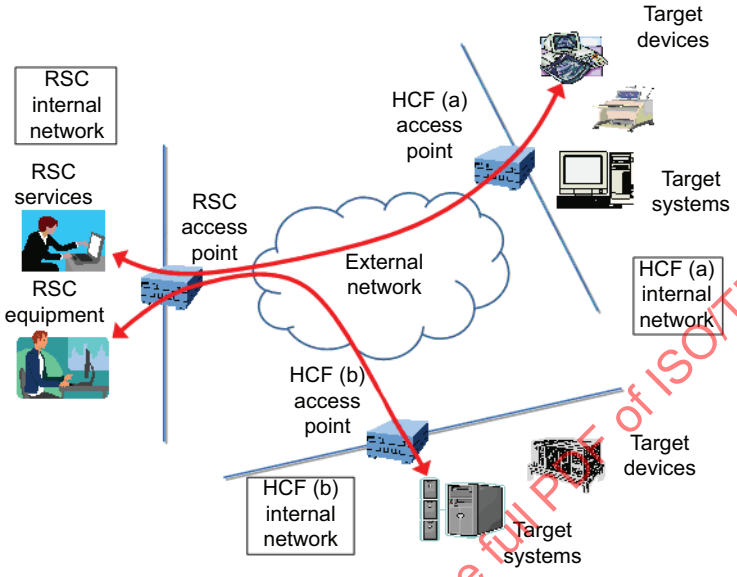


Figure 1 — Assumed remote maintenance services

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.

Because medical information is a particularly important type of personal information, it must be treated carefully and securely.

4.2.3.2 Responsibility and measures of privacy protection of personal information

United States HIPAA regulations requires healthcare organizations to assign a person to be in charge of information management, and assigns responsibility to the healthcare organization when personal information is leaked from the healthcare organization, irrespective of the reasons for the leak.

In Japan, guidelines for protection of personal information in the medical field place responsibility for the protection of personal information with healthcare organizations and require the person in charge of the protection of personal information at the healthcare organization to carry out this responsibility. The healthcare organizations should therefore manage information themselves.

However, this part of ISO/TR 11633 finds cases in which healthcare organizations leave the management of medical information systems entirely to the RMS providers of medical devices and medical information systems. It might be difficult for the persons in charge of the healthcare organization to manage a crisis appropriately from the viewpoint that the healthcare organizations manage information, given that they leave information management entirely to the RMS providers.

However, in cases of accidents leading to information leakage, etc., the problem might arise as to who should be responsible – an RMS provider or a healthcare provider? To resolve such a situation, this part of ISO/TR 11633 shows that it is preferable to review the system of information management of the healthcare organization to ensure conformity with any jurisdictional act(s) for privacy protection of personal information.

4.2.3.3 RMS coexisting with health information privacy protection

To protect personal information appropriately, healthcare organizations should provide security measures appropriate to the responsibility of the healthcare organization, as described in the previous paragraph.

Currently, healthcare organizations are chiefly providing medical centre management rules, instituting measures for appropriate management, implementing security measures for information systems and implementing technical measures to protect personal information.

In particular, on network security measures, many healthcare organizations provide policy measures such as “the connection with an external network is not permitted”, “use of VPN”, etc., and defend against outside hackers trying to invade by way of the internet. However, even if a healthcare organization's counter-measures against intrusion from the outside are almost perfect, RMS is the only route that permits access from outside.

Access by an RMS provider's maintenance worker to the system by way of the RMS line has been taken as a necessary service for a rapid function recovery.

RMS has advantages for both healthcare organizations and RMS providers, and is therefore a necessary service, even after acts for privacy protection of health information are approved and published.

To use RMS securely and responsibly, healthcare organizations should correctly understand RMS, contract appropriately and implement technical security measures and operational measures. It is important to clarify responsibility between a healthcare organization and RMS providers, and construct a well-assessed safe mechanism for such clarifications to conform to privacy protection of health information. Both the healthcare organization and RMS providers shall recognize each obligation correctly and take appropriate RMS under mutual agreement.

4.3 Roles of remote service centre and healthcare organization

Where the HCF, by concluding a maintenance contract with the RMS providers, has entrusted the RMS provider with providing security in RMS, the security is implemented under the judgment and responsibility of each RMS provider.

The following issues arise:

— there is no statement that the third party can take to mean that the RMS provider is providing enough security measures;

— HCF has not considered management measures as much as technological measures in present security measures;

— HCF has insufficiently examined the sequence of events after an accident occurs;

— HCF has not examined broad threats such as computer viruses.

Privacy protection acts require HCFs to take responsibility for individual medical information security. The HCF will also have to take responsibility for the security maintenance of the RMS. Therefore, this part of ISO/TR 11633 explains the role of HCF and RMS providers. Implementing security in RMS is the role of RMS providers, because only the RMS provider can implement the RMS function for the medical information system. RMS providers should consider that implementing with different security technologies inhibits the spread of RMS.

In preparing access points for each RMS, providers can make security management complicated. Such complicated management allows security breaches to take place. Therefore each RMS provider needs to adopt and implement standard and widely-used security technology.

Management measures are important, as are technological measures. These are necessary for both HCF and RSC. They should document a current information security management system based on an international standard such as ISO/IEC 27001 that supports the implementation of a security policy. After that, they should compare and associate with security policies; it is also important to clarify the minimum standard of security in an RMS. The HCF decides and takes measures based on its own security policy and examines and evaluates the security policy and the circumstances of the security measures in the RMS indicated by the RMS providers. After that, the HCF contracts with RMS providers about compliance on operation and confidentiality. As a result, RMS security is assured.

5 Use case of remote maintenance services

5.1 Introduction

This part of ISO/TR 11633 extracts three typical use cases of remote maintenance services considered as a model of basic operational site.

a) Trouble shooting for outages

In case of outages of equipment within the HCF site and responding to a request from the HCF site, maintenance operations are done by accessing the targeted devices from the RSC site.

b) Scheduled maintenance

Scheduled maintenance operations are carried out from the RSC site by obtaining consent of the HCF site. This may cause periodic access to target devices in the HCF.

c) Software updating

Update software of targeted devices within the HCF site by accessing them from the RSC site.

5.2 Trouble shooting for outages

Workflow in case of trouble shooting for outages is shown in Figure 2.

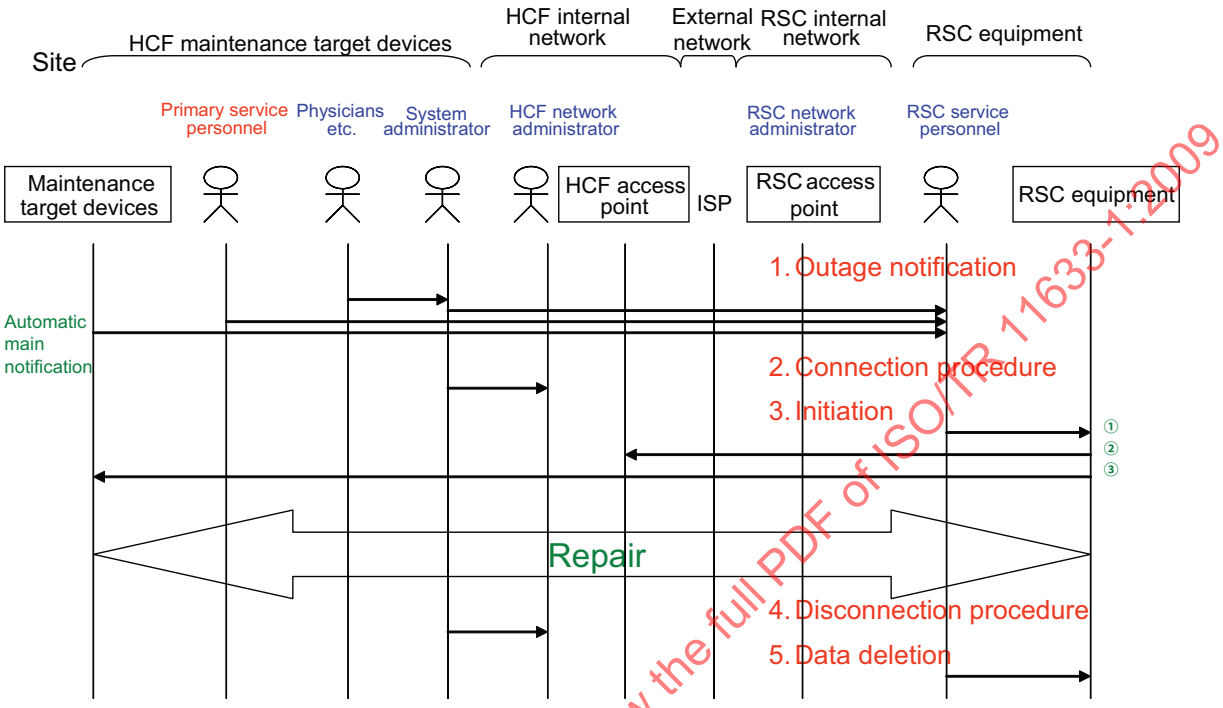


Figure 2 — Workflow in case of trouble shooting for outages

Steps are as follows:

a) RSC is notified by HCF that a problem occurred (this may be an automatic notification by email).

b) RSC requests HCF to connect network for the RMS.

c) RSC performs initiation for network connection.

d) RSC service people carry out inspection, treatment, and acknowledgement through the network connection:

   1) implementation of an automatic inspection programme;

   2) collection of related information from targeted equipments:

      i) operation logs;

      ii) image data;

      iii) configuration files/system configurations;

      iv) contents of database;

3) investigation of the problem;

4) if the problem has its origin in software, modification or update of the targeted equipment:

   i) modification of configuration files;

   ii) update software;

   iii) restoring data;

5) if the problem has its origin in hardware, contact of primary service people to exchange damaged parts;

6) carrying out inspection after repair.

e) RSC reports the work result to the HCF.

f) RSC disconnects network connection for the RMS.

g) RSC requests the HCF to disconnect network connection for the RMS.

h) If RSC transferred PHI, RSC deletes all copies of the PHI at their site.

5.3 Scheduled maintenance

Workflow in case of scheduled maintenance is shown in Figure 3.

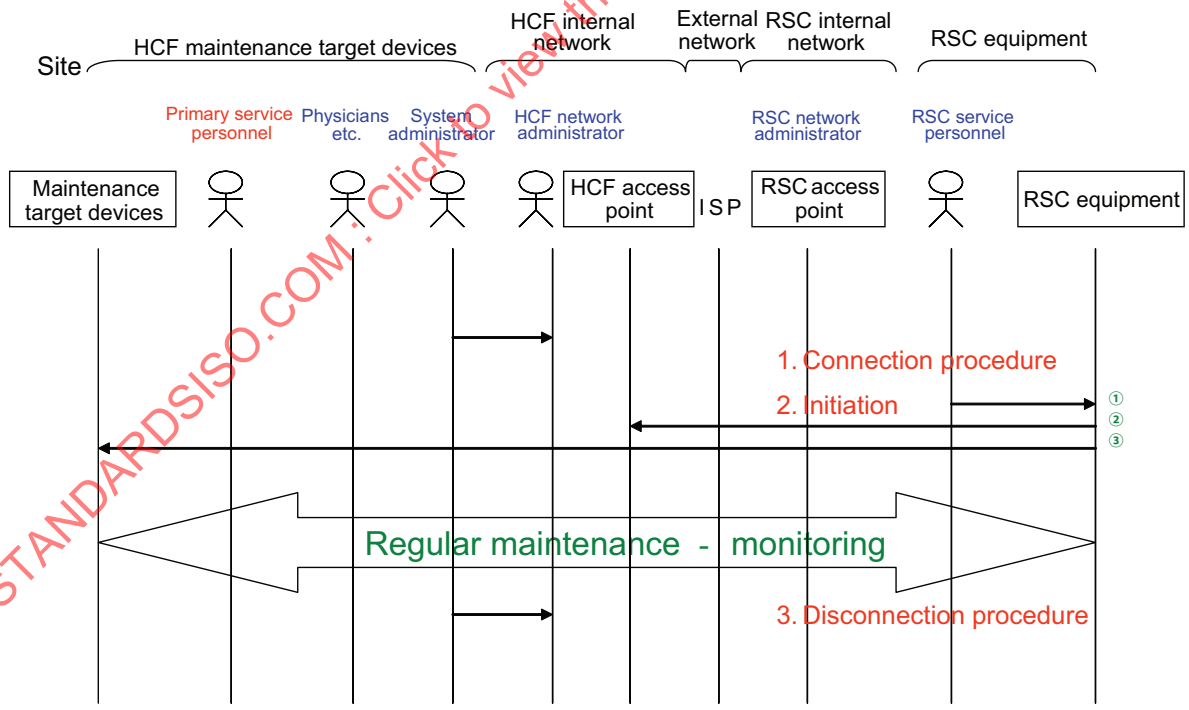


Figure 3 — Workflow in case of scheduled maintenance

Steps are as follows:

a) RSC requests the HCF to connect the network for the RMS.

b) RSC initiates the network connection.

c) RSC service people carry out scheduled inspection through the network connection:

   1) implementation of an automatic inspection programme;

   2) checking of logs;

   3) checking image quality (accuracy);

   4) collection of operational information.

d) RSC reports the work result to the HCF.

e) RSC disconnects the network connection for the RMS.

f) RSC requests HCF to disconnect the network connection for the RMS.

g) If RSC transferred PHI, RSC deletes all copies of the PHI at their site.

5.4 Software updating

Workflow in case of software updating is shown in Figure 4.

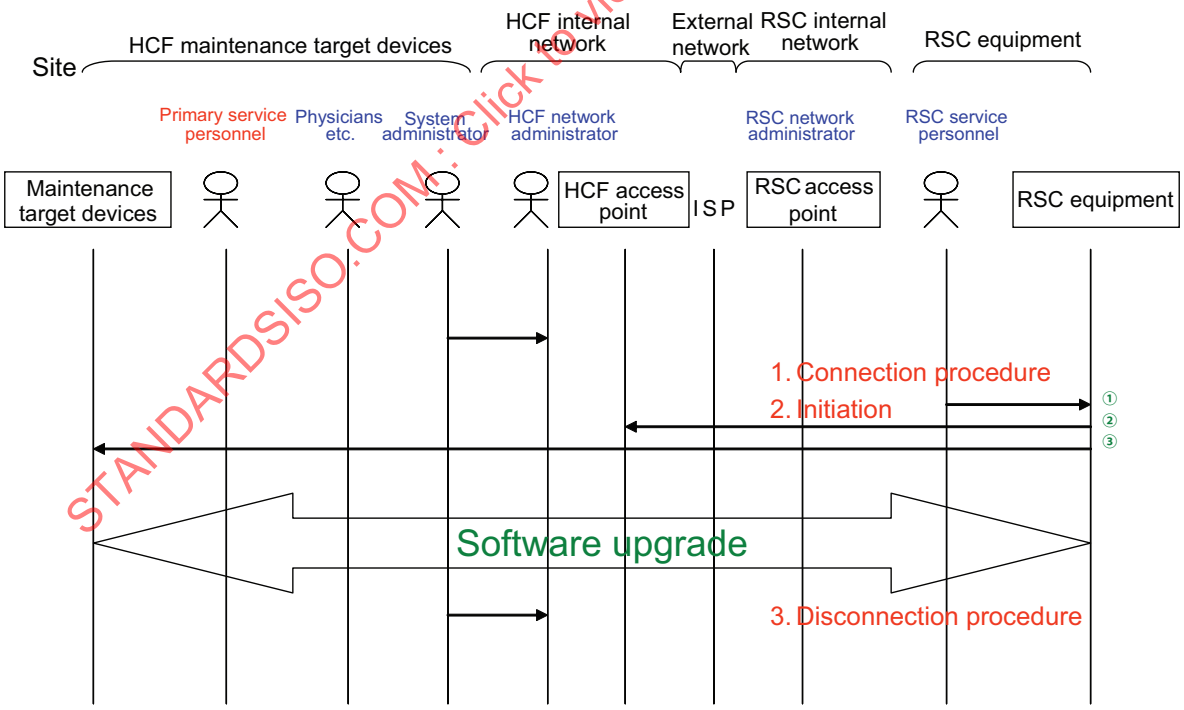


Figure 4 — Workflow in case of software updating

Steps are as follows:

a) RSC requests the HCF to connect network for the RMS.

b) RSC initiates network connection.

c) RSC service people update the software through the network connection:

   1) replacing software;

   2) changing configurations;

   3) confirmation of functional operations.

d) RSC reports the work result to the HCF.

e) RSC disconnects network connection for the RMS.

f) RSC requests HCF to disconnect network connection for the RMS.

g) If RSC transferred PHI, RSC deletes all the existing data in their site.

6 Risk analysis

6.1 General

In this clause, a risk analysis based on the use cases in Clause 5 is described.

6.2 Risk analysis criteria

6.2.1 Policy

Policy requires the information administrator in charge of the healthcare organization to think about security and about the risk to the healthcare organization by the HIPAA method. Therefore, it is necessary for predicting risk, and for thinking about security when information is exchanged with those outside the organization.

This analysis is placed with HCF as a supplementary document or a guide to the contract between RSC. Management needs to perform the analysis for every extra healthcare organization.

6.2.2 Classification of the site

— RSC equipment.

— RSC internal network.

— External network.

— HCF internal network.

— HCF target devices.

6.2.3 Protection profile

The protection profile is as follows:

— Confidentiality: shoulder hacking/misappropriation, unauthorized login/hoaxing and trial-and-error tactics.

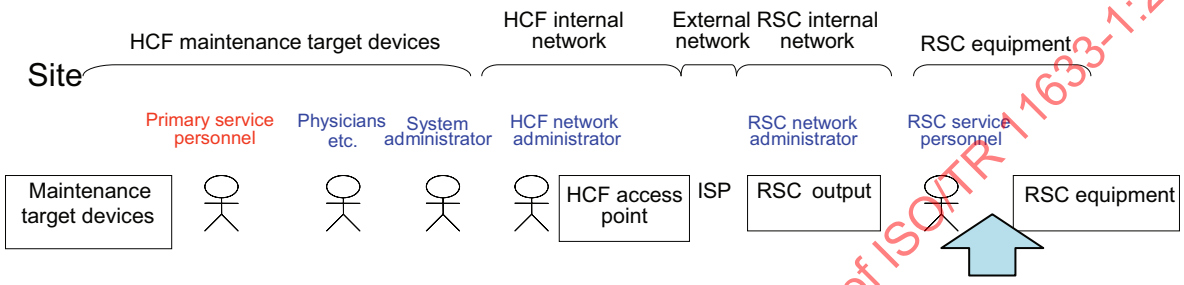
— Integrity: falsification, substitution, forgery and non-repudiation.

— Availability: equipment trouble, disaster, loss of service by cable interruption/denial of service.

Annex A
(informative)

Example of risk analysis result of remote maintenance services

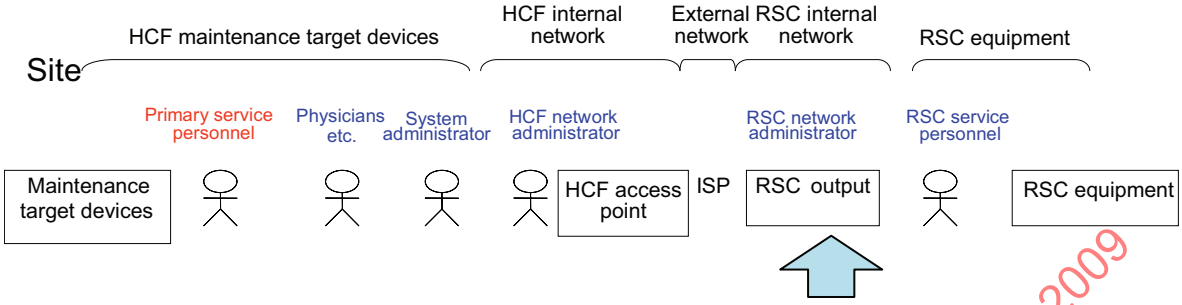
A.1 Assets and threats (site: RSC equipment)



Assets	No.	Threat (C: confidentiality, I: integrity, A: availability)
PHI information on memory, disk, and screen	11	Exposure [C] by deletion failure on site [C], peeping [C]/theft [C], unauthorized login to RSC equipment [C]/hoaxing [C]
	12	Exposure [C] by theft from path [C], unauthorized login to RSC equipment [C]/hoaxing [C]
Memos and print-outs of above PHI information	13	Exposure [C] by peeping of paper records for repair [C], carrying out [C]
Backup media of above PHI information	14	Exposure [C] by carrying out of recorded media for repair [C]
Software dealing with PHI information	15	Exposure [C] by back door/installation of information-stealing programme [I]
Equipment dealing with PHI information	16	Exposure [C] by carrying out [C], tampering [C], leakage electromagnetic radiation [C]
	17	Service impossible [A] due to failure [A], disaster [A], damage [A]
Equipment dealing with PHI information[a]	18	Service impossible [A] due to failure [A], disaster [A], damage [A]
Operators dealing with PHI information	19	Exposure by bribery [C], service failure [A] by incorrect input [I]/deletion failure [A]
Encryption algorithm, keys, and key distribution method	1a	Exposure [C] by decoding of encrypted data [C]

[a] Indicates the power/disaster facilities. However, the network equipment is not included.

A.2 Assets and threats (site: RSC internal network)



Assets	No.	Threat (C: confidentiality, I: integrity, A: availability)	
		Without countermeasures on VPN	With counter measures on VPN
PHI information on RSC internal network	21	Exposure [C] by peeping of path [C], unauthorized login to RSC network equipment [C]/hoaxing [C], tapping [C]	Threat other than [A] availability is negligible
Memos and print-outs of communication trace of above information	22	Exposure [C] by peeping of monitor recording sheet [C], carrying out [C]	
Backup media of communication trace of above information	23	Exposure [C] by carrying out of monitor recording media [C]	
Network equipment software	24	Exposure [C] by back door/installation of information-stealing programme [I]	
Network equipment	25	Exposure [C] by carrying out [C], tampering [C], leakage electromagnetic radiation [C]	
	26	Service impossible [A] due to failure [A], disaster [A], damage [A]	
Environmental facilities of network equipment[a]	27	Service impossible [A] due to failure [A], disaster [A], damage [A], cable discontinuity [A]	
Network equipment operators	28	Exposure by bribery [C], exposure [C] by incorrect setting [C]	
Encryption algorithm, keys, and key distribution method	29	Exposure [C] by decoding of encrypted data [C]	

[a] Indicates the power/disaster facilities.