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 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

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.

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.

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

standardized internationally as ISO/IEC 27001, therefore, it is convenient to construct and operate an ISMS referring to ISO/IEC 27001. This also helps to persuade patients, medical treatment evaluation organizations, and others of the efficacity of the security measures.

General steps of ISMS construction are shown in Figure 1.

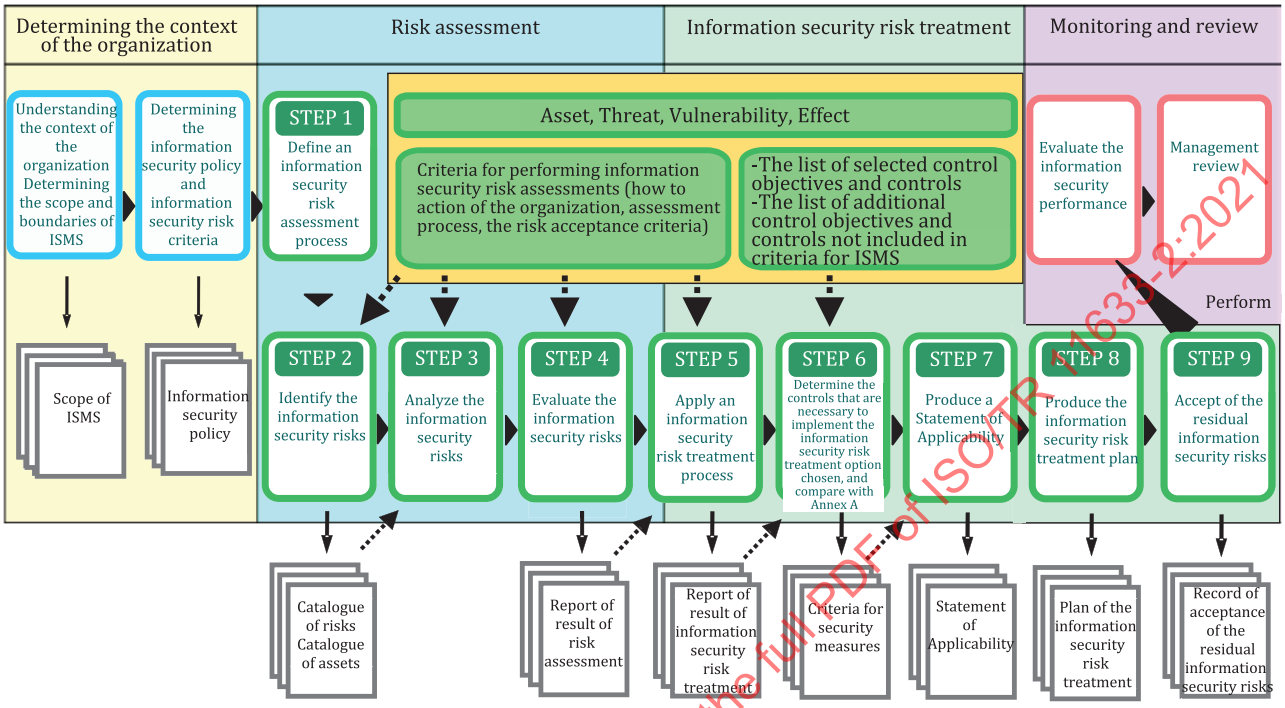

Figure 1 — ISMS steps

Security measures for protecting personal information in the remote maintenance services (RMS) are described below in accordance with the concepts of ISMS.

Both the healthcare organization and the RMS provider should construct the appropriate ISMS. Additionally, the healthcare organization should ideally do the work to adjust the information security management among all RMS providers to protect personal information. The RMS connects the network of the RMS provider and the network of the healthcare organization. After connecting these networks, there are risks of new security holes being created. In the RMS, a different problem may occur in system construction in a single organization, because the RMS acts between the healthcare organization and the remote maintenance service centre (RSC), two organizations that are independent of each other. It will therefore be a burden on both the healthcare organization and RSC, if security measures are not considered an integral part of the RMS from the outset. In this regard, using ISMS (a well-evaluated technique) can be considered as a better way to implement RMS security efficiently.

Under many jurisdictional laws for personal information protection, the healthcare organization will assume the obligations and responsibilities of being custodian of the personal information. In the RMS, the healthcare organization should request, from the RMS provider, appropriate measures for protecting personal information because the provider will access the target device set up in a healthcare facility from the RSC through the network. The healthcare organization must independently adjust all RMS providers' information security management systems that provide the RMS, and confirm that security holes have not been created. Additionally, the healthcare organization should confirm each RMS provider's security level is kept appropriate.

The following items should be documented and established in the ISMS:

— security policy;

— security measures standard;

— mapping of security policy;

— selection of solutions;

— operation execution rule;

— security auditing standards;

— security audit and audit trail.

A healthcare organization should write items into the maintenance contract or agreement between the healthcare organization and RMS provider that the RSC implements to ensure appropriate measures in the RSC. As a result, the healthcare organization will distribute the obligation and the responsibility concerning the protection of personal information during maintenance work to the RMS provider through the contract and agreement. The healthcare organization should construct the appropriate ISMS and, at the same time, should put into writing in the maintenance contract or the business consignment contract the obligation on the part of the RMS provider of providing supervision as the final authority in charge of personal information management.

The risk analysis and measures are illustrated in this document by the ISMS method. Therefore, it is thought that constructing the remote maintenance service security (RSS) with this content will bring advantages to both the healthcare organization and the RSC. When the content of this risk assessment is not complete, additional risk assessment need only be done on parts that are missing.

4.2 Compliance scope

The coverage of the ISMS in the operational model described in ISO/TS 11633-1:2019, Annex A is as follows:

— target device for maintenance in healthcare facility (HCF);

— internal network of healthcare organization;

— route from an RMS access point in healthcare organization to the RSC;

— internal network of the RSC;

— equipment management in the RSC.

Because the following risks exist independent of the presence of the RMS, they are excluded from the coverage of the ISMS of this clause:

— threats related to availability of equipment and software that treats protected health information (PHI);

— threats related to computer virus;

— threats related to staff which pertain to adoption, education and training.

4.3 Security policy

The desired content included in a basic policy is referred to in ISO/IEC 27002:2013, Clause 5.1.1.

When these considerations are applied to RSS, it should be able to secure the availability of the system, and to secure the integrity, readability, and preservation of patient personal information.

The technical, systematic, human resources and physical safety measures of the RSS should be specified in a basic security policy of the RSS.

The following explanations assume large-scale integrated HCF. Since it is possible that the RSC which receives RMS exists in two or more sections of a large-scale HCF, a united management policy is needed.

When the HCF scale and the operation form are different from large-scale integrated HCF, it is important to implement in conformity with the actual situation.

4.4 Assessing risks

In risk assessment, analysis of information assets is performed with regard to the following.

— What threats exists?

— To what extent is each threat possible and what is its frequency of occurrence?

— When the threat is actualized, how much influence does it exert?

The technique of the analysis is broadly classified into the following four approaches.

a) Baseline approach

This is a technique for analysing risk based on the standards and guidelines that are required in the target field. This approach measures security based on standard risk assessment done beforehand in industry.

Though it is advantageous from the perspective of time and cost because the risk need not be evaluated by oneself, the adaptability of the standardized risks to the risks of a specific organization can be problematic.

b) Detailed risk analysis

Carrying out a detailed risk assessment includes risk analysis of details, and an appropriate management plan for management to select. A sizable budget for cost and time are needed for the risk assessment, including securing necessary human resources.

c) Combined approach

This approach combines the baseline approach with the detailed risk analysis and it has the advantages of each.

d) Informal approach

This approach implements risk analysis by exploiting the knowledge and the experience of the staff of the organization. It is difficult for a third party to evaluate the resulting risk analysis because the method is not structured.

The RMS is related to the healthcare organization and the RSC, so the risk analysis should be what both can agree upon. In this document, the typical use case is modelled, and the risk assessment concerning this model is carried out. Risk analysis by baseline approach a) and the combined approach of c) is enabled by using this risk assessment result. See Table A.1 for the result of the risk assessment. Table A.1 contains the selection of appropriate control purpose and management plan in ISO/IEC 27001 from the result of risk analysis in ISO/TS 11633-1. Table A.1 conforms to ISO/IEC 27001, and is composed of 14 management fields and 114 management plans.

The measures prescribed here specify the procedures which should be observed, at least in performing RMS. The healthcare organization, which is also the administrator of personal information, should evaluate whether the RSC conforms to this document, and should request that appropriate measures be taken if it does not. Moreover, if the healthcare organization's security level is below the level specified in this document, appropriate measures should be put in place. Each RMS provider is expected to implement appropriate measures in order to achieve the requirements described in ISO/TS 11633-1.

4.5 Risks to be managed

This subclause explains some examples from the viewpoint of personal information protection to avoid risks, which should be especially noted in an RMS. It is important to implement sufficient measures

against these risks. The risk discussed here is a mere example; the management of other risks is also important.

a) When the RSC handling personal information is managed by the healthcare organization.

In this case, the point that needs particular attention is a leak of information by the third party. Consideration needs to be given to information displayed on computer screens in the work environment and information printed out on paper, as well as to the threat of hacking into the system. The main risks are as follows:

— viewing of screens by persons other than persons concerned in RSC;

— leakage in third party trust;

— leakage from logs generated when data is analysed, from printed paper or cache memory, etc.;

— leakage in the network.

b) When the RSC accesses equipment of the healthcare organization for maintenance by the administrative authority.

In this case, the points that need particular attention are operator error and inappropriate access to the computer (submit operations that are permitted). The main risks are as follows:

— destruction of data in target device due to an operator mistake;

— destruction of data in target device due to malicious or subversive activities;

— leakage and destruction of more important information due to inside intrusion via the maintenance device.

c) When the RSC updates the software.

In this case, care is required not to install malicious software and computer viruses, etc., into the target devices. The main risks are as follows:

— leakage and destruction of data in target device due to malicious software;

— leakage and destruction of important information via internal intrusion due to a computer virus.

4.6 Identification of risks that are not described in this document

In this document, risk assessment is performed in accordance with the typical model, so the other use cases are outside its scope. If a business model is different from the model that this document assumes, the risk assessment results of this document can be misappropriated. There is also a possibility that not all cases can be covered. When coverage of all cases is not possible, a detailed risk analysis should be conducted using the combined risk assessment approach, not described by this document.

The risk assessment method in the detailed risk analysis is explained in ISO/TS 11633-1. By adopting the methods of ISO/TS 11633-1, the results of a risk assessment guided by a different business model can be easily integrated with the results of a risk assessment guided by this document.

4.7 Treating risks

Risk treatment is defined as treatment of the assumed risk in accordance with the results of risk assessment. Risk treatment choices are shown in Table 1. These choices are combined and implemented where necessary.

In the usual risk management process, a combination of these measures is selected by making an overall judgment of the severity of the risk or the ease of implementing the measures. It is especially important to adopt the risk control(s) specified by information privacy protection law and regulations. In this case, the risk should be controlled because risk retention or transfer are not typically adequate to meet

these privacy protection laws, otherwise it would be to adopt risk avoidance, which prevent any data that falls in scope of privacy protection law and regulations.

In this document, it is recommended that risk control be performed positively based on the ISMS. Concrete measures are explained in detail in Annex A.

Table 1 — Risk treatment

Risk control: Measures are adopted (management plan) to positively reduce damage. — Risk prevention — measures to reduce threats and vulnerabilities are implemented. — Minimization of damage — measures to reduce the damage when the risk is generated are implemented.	Risk transfer: Measures to transfer to third parties by contract, etc. — Insurance — utilizes damage insurance and other types of insurance so that the risk is transferred. — Outsourcing — information assets and information security measures are entrusted to an outside party.
Risk retention: Approach that accepts risk as belonging to the organization. — Financing — this corresponds to accumulating a reserve, etc. — Nothing is done.	Risk avoidance: Approach when appropriate measures cannot be found. — Abolition of business — the business is stopped. — Destruction of information assets — the management object is lost.

5 Security management measures for remote maintenance services

The possibility of leakage of personal information such as patient information from the RMS requires the healthcare organization to obtain the help of the RSC to achieve RMS security.

In order to take appropriate security measures for the actualization of the safety of the RMS, the healthcare organization and the RSC should select controls based upon the result of the risk assessment. Regardless of whether or not the RSC is supervised by the healthcare organization, the RSC should ensure the RMS meets security requirements.

Annex A illustrates concretely how to proceed with the safety management measures during RMS for the healthcare organization and the RSC. It is expected that referring to Table 1 will reduce risk assessment time when preparing the RMS.

Even if the RMS is already operational, auditing using Table 1 is recommended to make sure that the risk assessment is adequate.

6 Approving residual risks

Residual risk means the following among the risks identified by risk assessment.

— Risk that intentionally does not take sufficient measures.

— Risk that is difficult to identify.

— Risk whose cost is too expensive for complete measures.

When risks remain, even if the HCF performs risk control, risk retention or risk transfer, management should judge whether or not these residual risks are approved from a management point of view. When the HCF management approves these residual risks, it means that the HCF accepts the RMS as constituted by risk assessment based on the ISMS.

The HCF approves the residual risks in the whole contract of the RMS, and the RSC operates the RMS while paying attention to residual risks. According to the result of the risk analysis in the RMS illustrated in Annex A, particularly in the RSC, there still is the possibility of leakage of personal information such

as PHI. The HCF should recognize these dangers, take into account guidelines issued by government, and audit appropriate security measures that are taken in the actual RMS.

7 Security audit

7.1 Security audit of remote maintenance services

The purpose of the security audit is to confirm whether the risk management related to security is effectively implemented and to confirm whether an appropriate control based on the risk assessment is done. The security audit comprehensively assesses the conformity of the information security management standard, but it is also possible to focus on auditing the RMS itself. In the security audit of the RMS, the auditor verifies and evaluates, if appropriate, whether controls based on the risk assessment are maintained and operated.

Moreover, it is an effective measure for both the HCF and RSC to evaluate the safety standards of the security by means of the security audit because the result of such audits become an effective evaluative material to improve the solidity of the RMS.

7.2 Recommendation of security audit by third parties

There are the following problems to conduct information security audits as internal audits:

— it is hard to notice that the risks to be assessed are missing;

— objectivity and independence will not be satisfied;

— it takes time to train auditors because specialized knowledge is required;

— it is difficult to make an audit report for the purpose of disclosure.

As mentioned above, the HCF should be audited by an external organization and by an auditor with a high degree of technical knowledge, in order to objectively evaluate the RMS. Performing an external audit based on an appropriate audit procedure facilitates information security certification such as the ISMS. Finally, the HCF can enhance its societal reputation. It is also recommended to adopt external audit to reduce any gap in reliability of the security audit reports of the HCF and RSC.

Annex A
(informative)

Example of risk assessment in remote maintenance services

This annex provides an example of risk assessment of remote maintenance services. The example is shown in Table A.1. The order of the rows in Table A.1 is the same as the relevant clause of ISO/IEC 27001.

Notes for the interpretation of Table A.1 are found in Table A.2 to Table A.7.

Table A.1 — Example of risk assessment of remote maintenance services

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.5 Information security policies	A.5.1 Management direction for information security	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	-	-	-	-		-	-	-	-
			The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	-	-	-	-		-	-	-	-
A.6 Organization of information security	A.6.1 Internal organization	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	All information security responsibilities should be defined and allocated.	-	-	-	-		-	-	-	-
			Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.									
			Appropriate contacts with relevant authorities should be maintained.	-	-	-	-		-	-	-	-
			Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	-	-	-			-	-	-	-
			Information security should be addressed in project management, regardless of the type of the project.	-	-	-	-		-	-	-	-
	A.6.2 Mobile devices and teleworking	To ensure the security of teleworking and use of mobile devices.	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	-	-	-	-		-	-	-	-
			A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	-	-	-	-		-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	-	-	-	-		-	-	-	-
			The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	1-1	A1	a	Unauthorized use "C" by RSC service personnel of PHI information in onsite RSC equipment leads to exposure of information.	Internal audits of the records can detect unauthorized use by RSC service personnel. In addition, unauthorized use by RSC service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by RSC service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits".	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	1-2	A1	a	Unauthorized use "C" of PHI information in RSC equipment by RSC service personnel from an inside source leads to exposure of the information.	Internal audits of the records can detect unauthorized use by RSC service personnel. In addition, unauthorized use by RSC service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by RSC service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits".	3>2	3	1	9>6
				1-9	A1	b	Bribery "C" leads to exposure "C" of PHI information.	Confidentiality and background checks can restrict unauthorized use due to bribery by containing and preventing irregular practices by operators.	3>2	3	1	9>6
				2-8	B1	o						
				2-8	B2							
				4-8	D1							

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	5-1	E1	a	Unauthorized use "C" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to exposure "C" of the information.	Internal audits of the records can detect unauthorized use by primary service personnel. In addition, unauthorized use by primary service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by primary service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits."	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to concoction "I" of the information.	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent primary service personnel from replacing files.	3	3	1	9

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	5-2	E1	a	Unauthorized use "C" of PHI information in the equipment subject to maintenance by RSC service personnel from an external source leads to exposure "C" of the information.	Internal audits of the records can detect unauthorized use by RSC service personnel. In addition, unauthorized use by RSC service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by RSC service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits."	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to maintenance by RSC service personnel, from an external path, leads to concoction "I".	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent RSC service personnel from replacing files.	3>2	3	1	9>6
				5-3	E1	c	Removing "C" or replacement "I" onsite by a physician leads to exposure "C" or concoction of PHI information.	Confidentiality can restrict unauthorized use by containing and preventing irregular practices, however it has little effect in itself.	3	3	1	9

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.1 Prior to employment	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	5-9	E1	h	Bribery "C" leads to PHI information exposure.	Confidentiality and background checks can restrict unauthorized use due to bribery by containing and preventing irregular practices by operators.	3>2	3	1	9>6
	A.7.2 During employment	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	-	-	-	-		-	-	-	-
			All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	1-9	A1	h	Incorrect input "I" and accidental deletion "A" lead to service trouble "A" of the remote service.	Training and skill standards can prevent service trouble due to incorrect input and accidental deletion by maintaining and improving the qualifications of operators.	3>2	3	2	18>12
			There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	2-8	B1	o	Bribery "C" leads to exposure "C" of PHI information.	Confidentiality and background checks can restrict unauthorized use due to bribery by containing and preventing irregular practices by operators.	3>2	3	2	18>12
				4-8	D1							
				5-9	E1	h	Incorrect input "I" and accidental deletion "A" lead to service trouble "A" of the remote service.	Training and skill standards can prevent service trouble due to incorrect input and accidental deletion by maintaining and improving the qualifications of operators.	3>2	3	2	18>12

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.7 Human resource security	A.7.3 Termination and change of employment	To protect the organization's interests as part of the process of changing or terminating employment.	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	5-1	E1	a	Unauthorized use "C" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to exposure "C" of the information.	Internal audits of the records can detect unauthorized use by primary service personnel. In addition, unauthorized use by primary service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by primary service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits."	3>2	3	1	9>6
A.8 Asset management	A.8.1 Responsibility for assets	To identify organizational assets and define appropriate protection responsibilities.	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	-	-	-	-		-	-	-	-
			Assets maintained in the inventory should be owned.	-	-	-	-		-	-	-	-
			Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.	-	-	-	-		-	-	-	-
			All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	-	-	-	-		-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.8 Asset management	A.8.2 Information classification	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	-	-	-	-		-	-	-	-
			An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	-	-	-	-		-	-	-	-
			Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	-	-	-	-		-	-	-	-
	A.8.3 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	-	-	-	-		-	-	-	-
			Media should be disposed of securely when no longer required, using formal procedures.	1-3	A1	c	If a physician leaves the relevant asset for repair or for reasons of non-separability, "C" may be viewed or "C" sheets of paper may be removed by third parties, RSC personnel, or RSC network administrators, leading to exposure (C) of PHI information.	Disposal by shredding machine can prevent third parties, RSC personnel, or RSC network administrators from viewing or removing sheets of paper. Room entry management can restrict room entry by third parties, RSC personnel, or RSC network administrators and block viewing or removing sheets of paper.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.8 Asset management	A.8.3 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Media should be disposed of securely when no longer required, using formal procedures.	2-2	B1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-RSC network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-RSC network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	3>2	3	1	9>6
				4-2	D1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-HCF network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-HCF network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-HCF network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	3>2	3	1	9>6
			Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	-	-	-	-		-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.1 Business requirements of access control	To limit access to information and information processing facilities.	An access control policy should be established, documented and reviewed based on business and information security requirements.	-	-	-	-		-	-	-	-
			Users should only be provided with access to the network and network services that they have been specifically authorized to use.	-	-	-	-		-	-	-	-
	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	1-2	A1	a	Unauthorized login "C" by third parties, RSC personnel, or RSC network administrators using a dictionary attack in RSC equipment leads to unauthorized use "C" of PHI information in RSC equipment and exposure "C" of the information.	(No measures necessary)	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	2-1	B1	i	Unauthorized login "C" by means of a dictionary attack on RSC network equipment from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. Route control (no connection to RSC equipment) prevents remote connection to RSC equipment. General network administrative measures for RSC network equipment include access control (login) especially at RSC exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
							Unauthorized login "C" by means of a dictionary attack on RSC network equipment, from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent non-RSC network administrators from unauthorized login.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	2-1	B2	i	Unauthorized login "C" by means of a dictionary attack on RSC network equipment from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. Route control (no connection to RSC equipment) prevents remote connection to RSC equipment. General network administrative measures for RSC network equipment include access control (login) especially at RSC exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
				4-1	D1	p	Unauthorized login "C" by dictionary attack on HCF network equipment from an external source by non-RSC personnel including RSC personnel of other companies leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. General network administrative measures for HCF network equipment include access control (login) especially at HCF exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	4-1	D1	p	Unauthorized login "C" by means of a dictionary attack on HCF network equipment, from an internal source by a non-HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent non-HCF network administrators from unauthorized logins.	3>2	3	1	9>6
				5-1	E1	a	Unauthorized login "C" by means of a dictionary attack on equipment subject to maintenance by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies, from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent a third party, HCF personnel, HCF network administrator, and primary service personnel of other companies from illegal login (effect) since it blocks operation by an unauthorized person.	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to concoction "I" of the information.	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent primary service personnel from replacing files.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	5-2	E1	a	Unauthorized login "C" from an external source by means of a dictionary attack on equipment subject to maintenance by RSC service personnel of other companies leads to unauthorized use "C" of PHI information stored in the equipment subject to maintenance, and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent RSC service personnel of other companies from unauthorized login.	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to maintenance by RSC service personnel, from an external path, leads to concoction "I".	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent RSC service personnel from replacing files.	3>2	3	1	9>6
							Unauthorized login "C" from an internal source by means of a dictionary attack of the equipment subject to maintenance by third parties, HCF personnel, or HCF network administrators leads to unauthorized use "C" of PHI information stored in the equipment subject to maintenance and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent third parties, HCF personnel, and HCF networkadministrators from illegal login.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation and use of privileged access rights should be restricted and controlled.	1-2	A1	a	Unauthorized login "C" by third parties, RSC personnel, or RSC network administrators using a dictionary attack in RSC equipment leads to unauthorized use "C" of PHI information in RSC equipment and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent third parties, RSC personnel, or RSC network administrators from unauthorized login.	3>2	3	1	9>6
				2-1	B1	i	Unauthorized login "C" by means of a dictionary attack on RSC network equipment from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Privilege management (user/privilege login) in combination with Access Control.				
				4-1	D1	p	Unauthorized login "C" by means of a dictionary attack on HCF network equipment, from an internal source by a non-HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Route control is designed to enforce a path and specify the connecting equipment.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation and use of privileged access rights should be restricted and controlled.	5-1	E1	a	Unauthorized login "C" by means of a dictionary attack on equipment subject to maintenance by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies, from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent a third party, HCF personnel, HCF network administrator, and primary service personnel of other companies from illegal login (effect) since it blocks operation by an unauthorized person.	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to concoction "I" of the information.	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent primary service personnel from replacing files.	3>2	3	1	9>6
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation and use of privileged access rights should be restricted and controlled.	5-1	E1	a	Unauthorized login "C" by means of a dictionary attack on equipment subject to maintenance by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies, from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent a third party, HCF personnel, HCF network administrator, and primary service personnel of other companies from illegal login (effect) since it blocks operation by an unauthorized person.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
				5-2	E1	a	Replacement "I" of PHI information in equipment subject to maintenance by RSC service personnel, from an external path, leads to concoction "I".	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent RSC service personnel from replacing files.	3>2	3	1	9>6
							Unauthorized login "C" from an internal source by means of a dictionary attack of the equipment subject to maintenance by third parties, HCF personnel, or HCF network administrators leads to unauthorized use "C" of PHI information stored in the equipment subject to maintenance and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent third parties, HCF personnel, and HCF network administrators from illegal login.	3>2	3	1	9>6
A.9 Access control	A.9.2 User access management	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation of secret authentication information should be controlled through a formal management process.	-	-	-	-		-	-	-	-
			Asset owners should review users' access rights at regular intervals.	-	-	-	-		-	-	-	-
			The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	-	-	-	-		-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.3 User responsibilities	To make users accountable for safeguarding their authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	1-2	A1	a	Third parties, RSC personnel, or RSC network administrators using a leaked password from RSC equipment to pose as an authorized user leads to unauthorized use "C" of PHI information in RSC equipment and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of RSC equipment.	3>2	3	1	9>6
				2-1	B1	i	Spoofing "C" of RSC network equipment by using a leaked password, from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of RSC network equipment.	3>2	3	1	9>6
					B2	i	Spoofing "C" of RSC network equipment by using a leaked password, from an external source by anyone leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of RSC network equipment.				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.3 User responsibilities	To make users accountable for safeguarding their authentication information.	Users should be required to follow the organization's practices in the use of secret authentication information.	4-1	D1	p	Spoofing "C" of HCF network equipment by using a leaked password, from an external source by non-RSC personnel including RSC personnel of other companies leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of HCF network equipment.	3>2	3	1	9>6
							Spoofing "C" of HCF network equipment by using a leaked password, from an internal source by a non-HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of HCF network equipment.				
				5-1	E1	a	Spoofing "C" by using a password leaked from equipment subject to onsite maintenance by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies, leads to unauthorized use "C" of PHI information in the equipment subject to maintenance and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of equipment subject to maintenance.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.3 User responsibilities	To make users accountable for safeguarding their authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	5-2	E1	a	Spoofing "C" of equipment subject to maintenance by RSC service personnel of other companies, from an external source by using a leaked password leads to unauthorized use "C" of PHI information stored in the equipment subject to maintenance, and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of the equipment subject to maintenance.	3>2	3	1	9>6
							Use of a leaked password from an internal source, or spoofing "C" by physicians, third parties, HCF personnel, or HCF system administrators leads to unauthorized use "C" of PHI information stored in the equipment subject to maintenance and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of the equipment subject to maintenance.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.9 Access control	A.9.4 System and application access control	To prevent unauthorized access to systems and applications.	Access to information and application system functions should be restricted in accordance with the access control policy.	-	-	-	-	-	-	-	-	-
			Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	-	-	-	-	-	-	-	-	-
			Password management systems should be interactive and should ensure quality passwords.	-	-	-	-	-	-	-	-	-
			The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	-	-	-	-	-	-	-	-	-
			Access to program source code should be restricted.	-	-	-	-	-	-	-	-	-
A.10 Cryptography	A.10.1 Cryptographic controls	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	1-a	A2	b	If the strength "C" of the encryption algorithm, key and delivery method is insufficient, encoded data is decrypted and leads to exposure "C" of PHI information.	Applying an approved encryption algorithm, safety key, and key delivery method can prevent coded PHI information from being decrypted.	3>2	3	1	9>6
				2-9	B2							
				3-9	C1							
			A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	-	-	-	-	-	-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	5-1	E1	a	Peeping "C" on a screen onsite by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies leads to unauthorized use "C" of PHI information in equipment subject to maintenance, and exposure "C" of the information.	Partition restricts parties other than those concerned from casual visits.	3>2	3	1	9>6
			Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	1-1	A1	a	Unauthorized login "C" by third parties, HCF personnel, HCF network administrators, or primary service personnel of other companies, by means of viewing "C" on a screen, a dictionary attack on RSC equipment, or posing as an authorized user using a leaked password, leads to unauthorized use "C" of PHI information in RSC equipment and exposure "C" of the information.	Room entry management can restrict entry to the room by third parties, RSC personnel, or RSC network administrators, thereby preventing viewing of the screen, unauthorized login, or posing as authorized users.	3>2	3	1	9>6
				1-3	A1	c	If a physician leaves the relevant asset for repair or for reasons of non-separability, "C" may be viewed or "C" sheets of paper may be removed by third parties, RSC personnel, or RSC network administrators, leading to exposure "C" of PHI information.	Disposal by shredding machine can prevent third parties, RSC personnel, or RSC network administrators from viewing or removing sheets of paper. Room entry management can restrict room entry by third parties, RSC personnel, or RSC network administrators and block viewing or removing sheets of paper.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	1-4	A1	d	If the relevant asset is left for repair or for reasons of non-separability, removal of "C" sheets of paper by third parties, RSC personnel, or RSC network administrators leads to exposure "C" of PHI information.	Key management can prevent removal of disks by third parties, RSC personnel, or RSC network administrators.	3>2	3	1	9>6
				1-3	A1	c	If the relevant asset is left for repair or for reasons of non-separability, removing "C" sheets of paper by RSC service personnel leads to exposure "C" of PHI information.	Key management by multiple persons can restrict RSC service personnel from entering the room alone, thus preventing removal of sheets of paper.	3>2	3	1	9>6
				1-6	A1	f	Removal of "C" RSC equipment and disks by non-RSC service personnel leads to exposure "C" of PHI information.	Room entry management can prevent non-RSC service personnel from entering the room and removing RSC equipment and disks.	3>2	3	1	9>6
				1-7	A1	f	Destruction "A" of RSC equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3>2	2	1	6>4
				1-8	A1	g	Destruction "A" of an environmental facility for RSC equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to destruction by preventing unauthorized persons from accessing the equipment.				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	2-2	B1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-RSC network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-RSC network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	3>2	3	1	9>6
				2-3	B1	k	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Key management can prevent non-RSC network administrators from accessing and removing disks by preventing unauthorized persons from accessing the disks.	3>2	3	1	9>6
				2-5	B1	m	Removal of "C" RSC equipment, mail servers, and their disks by non-RSC network administrators leads to exposure "C" of PHI information.	Key management can prevent non-RSC network administrators from removing RSC network equipment, mail servers, or disks by preventing unauthorized persons from access.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	2-6	B1 B2	m	Destruction "A" of RSC equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3>2	2	1	6>4
				2-7	B1 B2	n	Destruction "A" of an environmental facility for RSC network equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.				
				4-2	D1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-HCF network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-HCF network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-HCF network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	3>2	3	1	9>6
				4-3	D1	k	If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by non-HCF network administrators leads to exposure "C" of PHI information.	Key management can prevent non-HCF network administrators from accessing and removing disks by preventing unauthorized persons from accessing the disks.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	4-5	D1	m	Removal of "C" RSC equipment, mail servers, and their disks by non-HCF network administrators leads to exposure "C" of PHI information.	Room entry management can prevent non-HCF network administrators from entering the room to prevent removal of HCF network equipment, mail servers, or their disks by prevention of unauthorized persons from entering the room.	3>2	3	1	9>6
							Destruction "A" of RSC equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3>2	2	1	6>4
				4-7	D1	n	Destruction "A" of an environmental facility for HCF network equipment leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.				
				5-4	E1	d	When a physician retains this asset at his/her practice, removal of "C" onsite by third parties, HCF personnel, HCF network administrators, primary service personnel of other companies, primary service personnel, and HCF system administrators leads to exposure "C" of PHI information.	Key management can prevent third parties, HCF personnel, HCF network administrators, primary service personnel of other companies, primary service personnel, or HCF system administrators from access to media to prevent removal of media.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	5-6	E1	f	Removal of "C" equipment subject to maintenance by non-HCF system administrators and its disks leads to exposure "C" of PHI information.	Removal of "C" equipment subject to maintenance by non-HCF system administrators and its disks leads to exposure "C" of PHI information.	3>2	3	1	9>6
				5-7	E1	f	Destruction "A" of equipment subject to maintenance leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3>2	2	1	6>4
				5-8	E1	g	Destruction "A" of an environmental facility for equipment subject to maintenance leads to service unavailability "A" of the remote service.	Key management can prevent service unavailability due to destruction by preventing unauthorized persons from accessing the equipment.				
			Physical security for offices, rooms and facilities should be designed and applied.	1-4	A1	d	If the relevant asset is left for repair or for reasons of non-separability, removal of "C" sheets of paper by RSC service personnel leads to exposure "C" of PHI information.	Key management by multiple persons can restrict RSC service personnel from access to the disks while alone.	3>2	3	1	9>6
				1-6	A1	f	Removal of "C" RSC equipment and disks by RSC service personnel leads to exposure "C" of PHI information.	Key management by multiple persons can restrict removal of RSC equipment and disks by RSC network administrators by preventing authorized persons from access while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Physical security for offices, rooms and facilities should be designed and applied.				Tapping "C" into the RSC network from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side to detect traces of tapping on the path.	3>2	3	1	9>6
				2-1	B1	i	Tapping "C" into the RSC network from an internal source by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side by multiple persons to detect traces of tapping on the path by multiple persons.	3>2	3	1	9>6
							Peeping "C" through RSC network equipment by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Key management by multiple persons can restrict access to disks by RSC network administrators while alone, and prevent exposure of PHI information through the RSC network equipment by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Physical security for offices, rooms and facilities should be designed and applied.	2-2	B1	j	If the relevant asset is left for monitoring or repair, removing "C" sheets of paper by an RSC network administrator leads to exposure "C" of PHI information.	Room entry management (communication trace machine room) by multiple persons can prevent room entry by an RSC network administrator while alone, and restricts removal of sheets of paper by prevention of authorized persons from entering the room while alone.	3>2	3	1	9>6
				2-3	B1	k	If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by an RSC network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to disks by an RSC network administrator while alone by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6
				2-5	B1	m	Removal of "C" RSC equipment, mail servers, and their disks by an RSC network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to network equipment, mail servers, or their disks by RSC network administrators by preventing authorized persons from access while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Physical security for offices, rooms and facilities should be designed and applied.				Tapping "C" into the HCF network from an internal source by a non-HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	An internal path check on the HCF side detects traces of tapping on the path.	3>2	3	1	9>6
				4-1	D1	p	Tapping "C" into the HCF network from an internal source by a HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	An internal path check on the HCF side by multiple persons detects traces of tapping on the path by multiple persons.	3>2	3	1	9>6
							Peeping "C" through HCF network equipment by an HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Key management by multiple persons can restrict access to disks by HCF network administrators while alone, and prevent exposure of PHI information through the HCF network equipment by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6
				4-2	D1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by an HCF network administrator leads to exposure "C" of PHI information.	Room entry management (communication trace machine room) by multiple persons can prevent room entry by an HCF network administrator while alone, and restricts removal of sheets of paper by prevention of authorized persons from entering the room while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Physical security for offices, rooms and facilities should be designed and applied.	4-3	D1	k	If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by an HCF network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to disks by an RSC network administrator while alone by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6
				4-5	D1	m	Removal of "C" network equipment, mail servers, and their disks by an HCF network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to network equipment, mail servers, or their disks by HCF network administrators by preventing authorized persons from access while alone.	3>2	3	1	9>6
				5-4	E1	d	Bringing out "C" or replacement I onsite by a physician leads to exposure "C" or concoction of PHI information.	Key management by multiple persons can put restraints on contacting the disk media by a physician only by himself/herself (effect) because of prevention of an authorized person going solo from contacting the media.	3>2	3	1	9>6
				5-6	E1	f	Removal "C" or changing "I" of equipment subject to maintenance by HCF system administrators and its disks, leads to exposure "C" or concoction of PHI information.	Key management by multiple persons can restrict removal of equipment subject to maintenance by HCF administrators and its disks by preventing authorized persons from accessing disks while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	-	-	-	-		-	-	-	-
			Procedures for working in secure areas should be designed and applied.	1-4	A1	d	If the relevant asset is left for repair or for reasons of non-separability, removal of "C" sheets of paper by third parties, RSC personnel, or RSC network administrators leads to exposure "C" of PHI information.	Key management can prevent removal of disks by third parties, RSC personnel, or RSC network administrators.	3>2	3	1	9>6
				1-6	A1	f	Analysis "C" of electromagnetic wave leakage from RSC equipment leads to exposure "C" of PHI information.	Ensuring a distance between the site and the road can prevent PHI information exposure by preventing reception of electromagnetic wave leakage.	3>2	3	1	9>6
				2-1	B1	i	Tapping "C" into the RSC network from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side to detect traces of tapping on the path.	3>2	3	1	9>6
							Tapping "C" into the RSC network from an internal source by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side by multiple persons to detect traces of tapping on the path by multiple persons.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
							Peeping "C" through RSC network equipment by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Key management by multiple persons can restrict access to disks by RSC network administrators while alone, and prevent exposure of PHI information through the RSC network equipment by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Procedures for working in secure areas should be designed and applied.	2-2	B1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-RSC network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-RSC network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	3>2	3	1	9>6
				2-3	B1	k	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Key management can prevent non-RSC network administrators from accessing and removing disks by preventing unauthorized persons from accessing the disks.	3>2	3	1	9>6
				2-5	B1	m	Removal of "C" RSC equipment, mail servers, and their disks by non-RSC network administrators leads to exposure "C" of PHI information.	Key management can prevent non-RSC network administrators from removing RSC network equipment, mail servers, or disks by preventing unauthorized persons from access.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Procedures for working in secure areas should be designed and applied.				Tapping "C" into the HCF network from an internal source by a non-HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	An internal path check on the HCF side detects traces of tapping on the path.	3>2	3	1	9>6
				4-1	D1	p	Tapping "C" into the HCF network from an internal source by a HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	An internal path check on the HCF side by multiple persons detects traces of tapping on the path by multiple persons.	3>2	3	1	9>6
							Peeping "C" through HCF network equipment by an HCF network administrator leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Key management by multiple persons can restrict access to disks by HCF network administrators while alone, and prevent exposure of PHI information through the HCF network equipment by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6
				4-2	D1	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by an HCF network administrator leads to exposure "C" of PHI information.	Room entry management (communication trace machine room) by multiple persons can prevent room entry by an HCF network administrator while alone, and restricts removal of sheets of paper by prevention of authorized persons from entering the room while alone.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	Procedures for working in secure areas should be designed and applied.	4-3	D1	k	If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by an HCF network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to disks by an RSC network administrator while alone by preventing authorized persons from accessing the disks while alone.	3>2	3	1	9>6
				4-5	D1	m	Removal of "C" network equipment, mail servers, and their disks by an HCF network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to network equipment, mail servers, or their disks by HCF network administrators by preventing authorized persons from access while alone.	3>2	3	1	9>6
				5-4	E1	d	Bringing out "C" or replacement I onsite by a physician leads to exposure "C" or concoction of PHI information.	Key management by multiple persons can put restraints on contacting the disk media by a physician only by himself/herself (effect) because of prevention of an authorized person going solo from contacting the media.	3>2	3	1	9>6
				5-6	E1	f	Removal "C" or changing "I" of equipment subject to maintenance by HCF system administrators and its disks leads to exposure "C" or concoction of PHI information.	Key management by multiple persons can restrict removal of equipment subject to maintenance by HCF administrators and its disks by preventing authorized persons from accessing disks while alone.	3>2	3	1	9>6
			Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	-	-	-	-	-	-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.2 Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	1-6	A1	f	Analysis "C" of electromagnetic wave leakage from RSC equipment leads to exposure "C" of PHI information.	Ensuring a distance between the site and the road can prevent PHI information exposure by preventing reception of electromagnetic wave leakage.	3>2	3	1	9>6
							Tampering "C" with RSC network equipment leads to unexpected exposure "C" of PHI information.	Sealing is designed to detect traces of tampering.	3>2	3	1	9>6
				2-5	B1	m	Analysis "C" of electromagnetic wave leakage from RSC network equipment or cables leads to exposure "C" of PHI information.	Ensuring a distance between the site and the road can prevent PHI information exposure by preventing reception of electromagnetic wave leakage.	3>2	3	1	9>6
							Tampering "C" with HCF network equipment leads to unexpected exposure "C" of PHI information.	Sealing is designed to detect traces of tampering.	3>2	3	1	9>6
				4-5	D1	m	Analysis "C" of electromagnetic wave leakage from HCF network equipment or cables leads to exposure "C" of PHI information.	Ensuring a distance between the site and the road can prevent PHI information exposure by preventing reception of electromagnetic wave leakage.	3>2	3	1	9>6
							Tampering "C" of equipment subject to maintenance leads to unexpected exposure "C" of PHI information.	Sealing is designed to detect traces of tampering.	3>2	3	1	9>6
				5-6	E1	f	Analysis "C" of electromagnetic wave leakage from equipment subject to maintenance leads to exposure "C" of PHI information.	Ensuring a distance between the site and the road can prevent PHI information exposure by preventing reception of electromagnetic wave leakage.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.11 Physical and environmental security	A.11.2 Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	-	-	-	-	-	-	-	-	-
			Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.	-	-	-	-	-	-	-	-	-
			Equipment should be correctly maintained to ensure its continued availability and integrity.	-	-	-	-	-	-	-	-	-
			Equipment, information or software should not be taken off-site without prior authorization.	-	-	-	-	-	-	-	-	-
			Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	-	-	-	-	-	-	-	-	-
			All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	1-1	A1	a	If RSC service personnel forget to delete PHI information onsite, it leads to unexpected exposure of information.	Automatic erasure during logoff obviates the need for RSC service personnel to remember to delete PHI information, thus reducing the scope for human error.	3>2	3	1	9>6
			Users should ensure that unattended equipment has appropriate protection.	-	-	-	-	-	-	-	-	-
			A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	5-3	E1	c	When a physician leaves the relevant asset by his/her practice, viewing or removing "C" onsite by third parties, HCF personnel, HCF network administrators, primary service personnel of other companies, primary service personnel, or HCF system administrators leads to exposure "C" of PHI information.	Disk clearing can prevent viewing or removing sheets of paper by third parties, HCF personnel, HCF network administrators, primary service personnel of other companies, primary service personnel, or HCF system administrators by preventing the asset from being left unattended.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.1 Operational procedures and responsibilities	To ensure correct and secure operations of information processing facilities.	Operating procedures should be documented and made available to all users who need them.	-	-	-	-		-	-	-	-
			Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	1-5	A1	e	Insertion of a backdoor or information-stealing program "I" leads to exposure "C" of PHI information.	The Incident Response Team (IRT) quickly recovers damage caused by a backdoor or information-stealing program because of virus measures. Virus measures can detect and eliminate backdoors or information-stealing programs.	3>2	3	2	18>12
				2-1	B1	f	Unauthorized login "C" by means of a dictionary attack on RSC network equipment from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. Route control (no connection to RSC equipment) prevents remote connection to RSC equipment. General network administrative measures for RSC network equipment include access control (login) especially at RSC exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
					B2							
				2-4	B1	l	Insertion of a backdoor or information-stealing program "I" leads to exposure "C" of PHI information.	The Incident Response Team (IRT) quickly recovers damage caused by a backdoor or information-stealing program because of virus measures. Virus measures can detect and eliminate backdoors and information-stealing programs.	3>2	3	2	18>12

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.1 Operational procedures and responsibilities	To ensure correct and secure operations of information processing facilities.	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	4-1	D1	p	Unauthorized login "C" by dictionary attack on HCF network equipment from an external source by non-RSC personnel including RSC personnel of other companies leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. General network administrative measures for HCF network equipment include access control (login) especially at HCF exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
				4-4	D1	l	Insertion of a backdoor or information-stealing program "I" leads to exposure "C" of PHI information.	The Incident Response Team (IRT) quickly recovers damage caused by a backdoor or information-stealing program because of virus measures. Virus measures can detect and eliminate a backdoor or information-stealing program.	3>2	3	2	18>12
				5-5	E1	e						
			The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	-	-	-	-	-	-	-	-	-
			Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	1-6	A1	f	Tampering "C" of RSC equipment leads to unexpected exposure "C" of PHI information.	Sealing is designed to detect traces of tampering.	3>2	3	1	9>6
A.12 Operations security	A.12.2 Protection from malware	To ensure that information and information processing facilities are protected against malware.	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	1-5	A1	e	Insertion of a backdoor or information-stealing program "I" leads to exposure "C" of PHI information.	The Incident Response Team (IRT) quickly recovers damage caused by a backdoor or information-stealing program because of virus measures. Virus measures can detect and eliminate backdoors or information-stealing programs.	3>2	3	2	18>12
				2-4	B1	l						
				4-4	D1							
				5-5	E1	e						

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.3 Backup	To protect against loss of data.	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	1-7	A1	f	Failure "A" of RSC equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				1-8	A1	g	Failure "A" of RSC equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				2-6	B1 B2	m	Failure "A" of RSC network equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				2-7	B1 B2	n	Failure "A" or cable disconnection "A" of an environmental facility for RSC network equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				4-6	D1	m	Failure "A" of HCF network equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.	3>2	2	2	12>8
				4-7	D1	n	Failure "A" or cable disconnection "A" of an environmental facility for HCF network equipment leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				5-7	E1	f	Failure "A" of equipment subject to maintenance leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				
				5-8	E1	g	Failure "A" of the environmental facility for equipment subject to maintenance leads to service unavailability "A" of the remote service.	Maintenance, checkout and backup can prevent service unavailability.				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.4 Logging and monitoring	To record events and generate evidence.	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	1-1	A1	a	Unauthorized use "C" by RSC service personnel of PHI information in onsite RSC equipment leads to exposure of information.	Internal audits of the records can detect unauthorized use by RSC service personnel. In addition, unauthorized use by RSC service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by RSC service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits".	3>2	3	1	9>6
			Logging facilities and log information should be protected against tampering and unauthorized access.	1-2	A1	a	Unauthorized use "C" of PHI information in RSC equipment by RSC service personnel from an inside source leads to exposure of the information.	Internal audits of the records can detect unauthorized use by RSC service personnel. In addition, unauthorized use by RSC service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by RSC service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits".				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.4 Logging and monitoring	To record events and generate evidence.	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	5-1	E1	a	Replacement "I" of PHI information in equipment subject to onsite maintenance by primary service personnel leads to concoction "I" of the information.	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent primary service personnel from replacing files.	3>2	3	1	9>6
							Replacement "I" of PHI information in equipment subject to maintenance by RSC service personnel, from an external path, leads to concoction "I".	Privilege management (access control) in combination with Access Control. Access control (write protection and file erasure prohibition) can prevent RSC service personnel from replacing files.	3>2	3	1	9>6
				5-2	E1	a	Unauthorized use "C" or replacement "I" of PHI information from an internal source in equipment subject to maintenance by physicians, HCF system administrators, or primary service personnel leads to exposure "C" or concoction "I".	Internal audits of the records can detect unauthorized use by physicians, HCF system administrators, or primary service personnel. In addition, unauthorized use by physicians, HCF system administrators, or primary service personnel can also be detected as it restricts illegal operation. Confidentiality and background checks (confirmation of qualification) can restrict unauthorized use by physicians, HCF system administrators, or primary service personnel by preventing irregular practices by operators. Keeping records (of the person requesting an event, type, date, etc.) in combination with "internal audits."	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.12 Operations security	A.12.4 Logging and monitoring	To record events and generate evidence.	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	-	-	-	-	-	-	-	-	-
	A.12.5 Control of operational software	To ensure the integrity of operational systems.	Procedures should be implemented to control the installation of software on operational systems.	-	-	-	-	-	-	-	-	-
	A.12.6 Technical vulnerability management	To prevent exploitation of technical vulnerabilities.	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	-	-	-	-	-	-	-	-	-
			Rules governing the installation of software by users should be established and implemented.	-	-	-	-	-	-	-	-	-
	A.12.7 Information systems audit considerations	To minimise the impact of audit activities on operational systems.	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimise disruptions to business processes.	-	-	-	-	-	-	-	-	-

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.13 Communications security	A.13.1 Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	Networks should be managed and controlled to protect information in systems and applications.	2-1	B1 B2	i	Unauthorized login "C" by means of a dictionary attack on RSC network equipment from an external source by any person leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. Route control (no connection to RSC equipment) prevents remote connection to RSC equipment. General network administrative measures for RSC network equipment include access control (login) especially at RSC exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
				4-1	D1	p	Unauthorized login "C" by dictionary attack on HCF network equipment from an external source by non-RSC personnel including RSC personnel of other companies leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	The Incident Response Team (IRT) is designed to expedite recovery from damage caused by unauthorized access. General network administrative measures for HCF network equipment include access control (login) especially at HCF exit, network separation/ forced path (FW)/filtering, and remote diagnosis port protection.	3>2	3	1	9>6
							Unauthorized login "C" by means of a dictionary attack on HCF network equipment, from an external source by RSC service personnel of other companies or RSC service personnel leads to unauthorized use "C" of PHI information stored on the HCF network and exposure "C" of the information.	Route control is designed to enforce a path and specify the connecting equipment.	3>2	3	1	9>6

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.13 Communications security	A.13.1 Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.				Unauthorized login "C" by means of a dictionary attack on RSC network equipment, from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Privilege management (user/privilege login) in combination with Access Control. Access control (login) can prevent non-RSC network administrators from unauthorized login.	1	3	1	3
				2-1	B2	i	Spoofing "C" of RSC network equipment by using a leaked password, from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Periodic changing of passwords prevents spoofing of RSC network equipment.				
							Tapping "C" into the RSC network from an internal source by a non-RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side to detect traces of tapping on the path.				
							Tapping "C" into the RSC network from an internal source by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Internal path check on the RSC side by multiple persons to detect traces of tapping on the path by multiple persons.				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
							Peeping "C" through RSC network equipment by an RSC network administrator leads to unauthorized use "C" of PHI information stored on the RSC network and exposure "C" of the information.	Key management by multiple persons can restrict access to disks by RSC network administrators while alone, and prevent exposure of PHI information through the RSC network equipment by preventing authorized persons from accessing the disks while alone.				

Table A.1 *(continued)*

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.13 Communications security	A.13.1 Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	2-2	B2	j	If the relevant asset is left for monitoring or repair, viewing or removing sheets of paper "C" by a non-RSC network administrator leads to exposure "C" of PHI information.	Disposal by a shredding machine can prevent non-RSC network administrators from viewing or removing sheets of paper. Room entry management (communication trace machine room) can restrict room entry by non-RSC network administrators and prevent viewing or removing sheets of paper by preventing unauthorized persons from entering the room.	1	3	1	3
							If the relevant asset is left for monitoring or repair, removing "C" sheets of paper by an RSC network administrator leads to exposure "C" of PHI information.	Room entry management (communication trace machine room) by multiple persons can prevent room entry by an RSC network administrator while alone, and restricts removal of sheets of paper by prevention of authorized persons from entering the room while alone.				
				2-3	B2	k	If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by non-RSC network administrators leads to exposure "C" of PHI information.	Key management can prevent non-RSC network administrators from accessing and removing disks by preventing unauthorized persons from accessing the disks.				
							If the relevant asset is left for monitoring or repair, removal of "C" sheets of paper by an RSC network administrator leads to exposure "C" of PHI information.	Key management by multiple persons can restrict access to disks by an RSC network administrator while alone by preventing authorized persons from accessing the disks while alone.				