TECHNICAL REPORT

ISO/TR 11633-2

First edition
2009-11-15

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 oeuvre d'un système de management de la sécurité de l'information (ISMS)

Reference number
ISO/TR 11633-2:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 11633-2 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

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

— *Part 1: Requirements and risk analysis*

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

Introduction

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

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

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

— clarify risks originating from using the RMS, where environmental conditions of the requesting vendor site (RSC) and maintenance target healthcare facility site (HCF) can be selected from the catalogue in Annex A;

— grasp the essentials of selecting and implementing both technical and non-technical “controls” to be applied in their own facility against the risks described in this part of ISO/TR 11633;

— request concrete countermeasures from business partners, as this document can identify the relevant security risks;

— clarify the boundary of responsibility between the healthcare facility owner and the RMS provider;

— plan a programme for risk retention or transfer as residual risks are clarified when selecting the appropriate “controls”.

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

— it will only be necessary to do the risk assessment for those organizational areas where this part of ISO/TR 11633 is not applicable, therefore, the risk assessment effort can be significantly reduced;

— it will be easy to show the validity of the RMS security countermeasures to a third party;

— if providing RMS to two or more sites, the provider can apply countermeasures consistently and efficiently.

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

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

1 Scope

This part of ISO/TR 11633 provides an example of selected and applied “controls” for RMS security based on the definition in the ISMS, on the basis of the risk analysis result mentioned in ISO/TR 11633-1. This part of ISO/TR 11633 excludes the handling of the communication problems and the use of encryption method.

This part of ISO/TR 11633 consists of:

— a catalogue of types of security environment in healthcare facilities and RMS providers;

— an example of combinations of threats and vulnerabilities identified under the environment in the “use cases”;

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

2 Terms and definitions

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

2.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

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

2.2
asset
anything that is of value to the organization

NOTE 1 Adapted from ISO/IEC 13335-1.

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

a) health information;

b) IT services;

c) hardware;

d) software;

e) communication facilities;

f) media;

g) IT facilities;

h) medical devices that record or report data.

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

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

[ISO 13335-1:2004, definition 2.4]

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

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

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

[ISO 13335-1:2004, definition 2.6]

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

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

2.8
information governance
processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed

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

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

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

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

2.11
risk assessment
overall process of risk analysis and risk evaluation

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

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

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

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

2.13
risk treatment
process of selection and implementation of measures to modify (typically reduce) **risk**

NOTE Adapted from ISO/IEC Guide 73:2002.

2.14
system integrity
property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system

2.15
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE Adapted from ISO/IEC 13335-1.

2.16
vulnerability
weakness of an asset or group of assets that can be exploited by a threat

NOTE Adapted from ISO/IEC 13335-1.

3 Abbreviated terms

— HCF Healthcare facility

— ISP Information-stealing programme

— ISMS Information security management system

— PHI Personal health information

— RMS Remote maintenance services

— RSC Remote maintenance service centre

— RSS Remote maintenance service security

— VPN Virtual private network

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 efficacy of the security measures.

General steps of ISMS construction are shown in Figure 1.

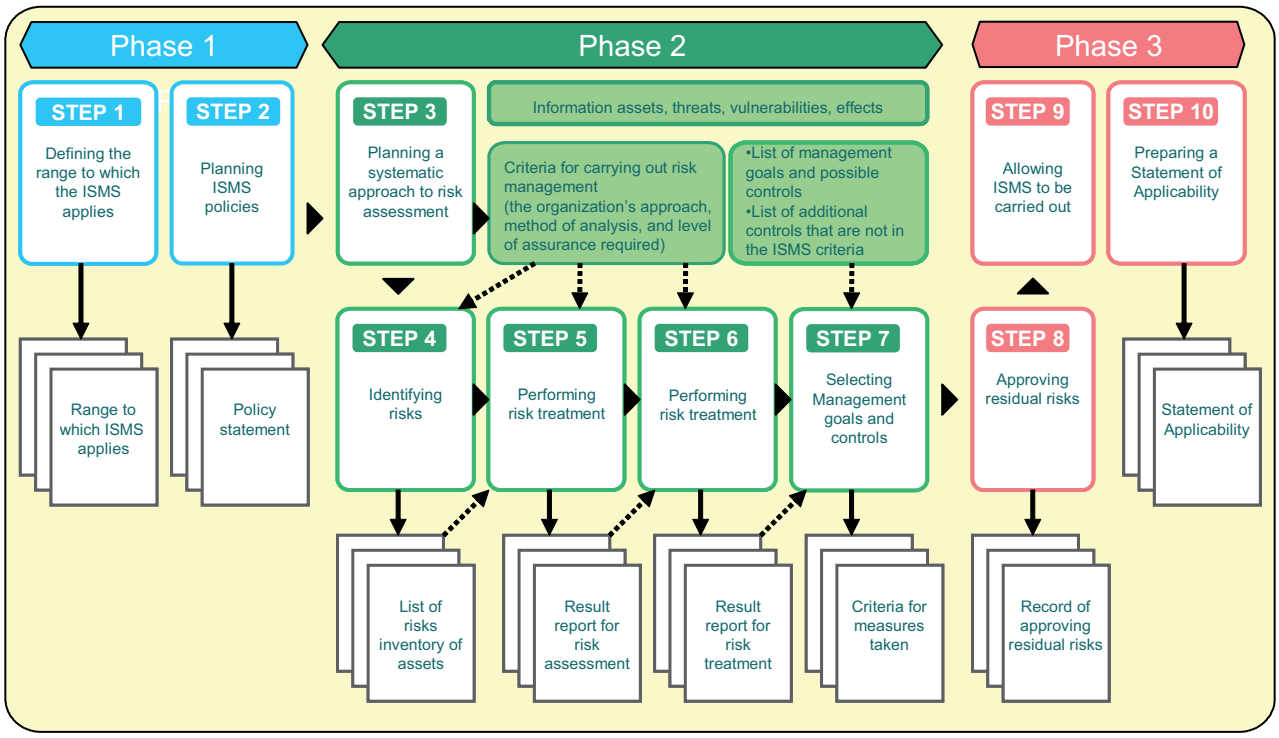

Figure 1 — ISMS steps

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.

It is necessary to document and comply with the following items to adjust 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 shall construct the appropriate ISMS and, at the same time, shall 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 part of ISO/TR 11633 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 Clause 6 of ISO/TR 11633-1 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

In 5.1.1 of ISO/IEC 27002:2005, the desired content to be included in a basic policy is prescribed, as follows:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, including:

   — compliance with legislative, regulatory, and contractual requirements,

   — security education, training, and awareness requirements,

   — business continuity management,

   — consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

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

It is necessary for the technical, systematic, human resources and physical safety measures of the RSS to 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 part of ISO/TR 11633, 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/TR 11633-1. Table A.1 conforms to ISO/IEC 27001, and is composed of 11 management fields and 133 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 part of ISO/TR 11633, 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 part of ISO/TR 11633, necessary measures will have to be put in place. Each RMS provider is expected to implement necessary measures in order to achieve the requirements described in this part of ISO/TR 11633.

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 part of ISO/TR 11633

In this part of ISO/TR 11633, 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 part of ISO/TR 11633 assumes, the risk assessment results of this part of ISO/TR 11633 can be misappropriated. There is also a possibility that not all cases can be covered. When coverage of all cases is not possible, it is necessary to conduct a detailed risk analysis using the combined risk assessment approach, not described by this part of ISO/TR 11633.

The risk assessment method in the detailed risk analysis is explained in ISO/TR 11633-1. By adopting the methods of ISO/TR 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 part of ISO/TR 11633.

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, it is necessary to control the risk positively, because measures such as risk retention or transfer are not adequate, or to adopt risk avoidance and not treat the personal information object, in law, in the RMS at all.

In this part of ISO/TR 11633, 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 risks are those risks where the HCF does not intentionally take sufficient countermeasures or where the HCF is having difficulty with the identification of these risks, or risks that will incur large costs if the HCF wishes to implement full countermeasures as derived by the risk evaluation. When risks remain, even if the HCF performs risk control, risk retention or risk transfer, it is necessary for management to judge whether or not these residual risks are to be 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 shall 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

When the HCF performs an information security audit as an internal audit, the following problems may arise:

— it is hard to notice whether there are risks of information having leaked from risk assessment;

— objectivity and independence will not be satisfied;

— because professional knowledge is required, the training of the audit team takes time;

— 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. Carrying out 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 to be found on pages 64 and 65.

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

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Security policy	A.5.1 Information security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	—	—	—	—	—	—	—	—	—
			The information security policy shall be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness.	—	—	—	—	—	—	—	—	—
A.6 Organization of information security	A.6.1 Internal organization	To manage information security within the organization.	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities.	—	—	—	—	—	—	—	—	—
			Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.	—	—	—	—	—	—	—	—	—
			All information security responsibilities shall be clearly defined.	—	—	—	—	—	—	—	—	—
			A management authorization process for new information processing facilities shall be defined and implemented.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
A.6 Organization of information security	A.6.1 Internal organization	To manage information security within the organization.	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed. Appropriate contacts with relevant authorities shall be maintained.	—	—	—	—	—	—	—	—	—
			Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	—	—	—	—	—	—	—	—	—
			The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes to the security implementation occur.	—	—	—	—	—	—	—	—	—
	A.6.2 External parties	To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties.	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
A.6 Organization of information security	A.6.2 External parties	To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties.	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	—	—	—	—	—	—	—	—	—
			Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	36	C1	m	Failure “A” of network equipment on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (maintenance, checkout and backup) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	2	12 > 4
							The disaster-affected network equipment “A” on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (disaster measures and business continuation plans) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	1	6 > 4
							Destruction “A” of network equipment on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (key management) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	1	6 > 4
				37	C1	n	Failure “A” or cable disconnection “A” of an environmental facility for network equipment on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (maintenance, checkout and backup) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	1	6 > 4
							The disaster-affected environmental facility “A” for network equipment on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (disaster measures and business continuation plans) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	1	6 > 4

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							Destruction “A” of an environmental facility for network equipment on the ISP side leads to service unavailability “A” of the RMS.	External request contracts (key management) prevent service unavailability by setting out the scope of responsibilities on the ISP side.	3 > 2	2	1	6 > 4
A.7 Asset management	A.7.1 Responsibility for assets	To achieve and maintain appropriate protection of organizational assets.	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. All information and assets associated with information processing facilities shall be “owned” by a designated part of the organization. Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented and implemented.	—	—	—	—	—	—	—	—	—
	A.7.2 Information classification	To ensure that information receives an appropriate level of protection.	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	—	—	—	—	—	—	—	—	—
			An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	—	—	—	—	—	—	—	—	—
			Background verification checks on all candidates for employment, contractors and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	—	—	—	—	—	—	—	—	—
			As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their responsibilities, as well as those of the organization, for information security. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	11	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their responsibilities, as well as those of the organization, for information security. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	12	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
				19	A1	h	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
				28	B1	o						
				28	B2							
				48	D1							

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their responsibilities, as well as those of the organization, for information security. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	51	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				52	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
A.8 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their responsibilities, as well as those of the organization, for information security. Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	52	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
				53	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
				59	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
		security policy in the course of their normal work, and to reduce the risk of human error. To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.										
			Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	—	—	—	—	—	—	—	—	—
			All employees of the organization and, where relevant, contractors and third party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	19	A1	h	Incorrect input “I” and accidental deletion “A” lead to service trouble “A” of the RMS.	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
				28	B1	o	Wrong setting “C” leads to unexpected exposure “C” of PHI information.	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
				48	D1							
				59	E1	h	Incorrect input “I” and accidental deletion “A” lead to service trouble “A” of the RMS.	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment		All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement. The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	51	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
			There shall be a formal disciplinary process for employees who have committed a security breach.	—	—	—	—	—	—	—	—	—
A.9 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	51	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 shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	11	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	13	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
				14	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
				16	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
				17	A1	f	Destruction “A” of RSC equipment leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4
				18	A1	g	Destruction “A” of an environmental facility for RSC equipment leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to destruction by preventing unauthorized persons from accessing the equipment.				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				22	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
A.9 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	23	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
				25	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
				26	B1 B2	m	Destruction “A” of RSC equipment leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4
				27	B1 B2	n	Destruction “A” of an environmental facility for RSC network equipment leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				42	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
				43	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
A.9 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	45	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 RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				47	D1	n	Destruction “A” of an environmental facility for HCF network equipment leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4
				54	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
				56	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
				57	E1	f	Destruction “A” of equipment subject to maintenance leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to equipment destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4
A.9 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	58	E1	g	Destruction “A” of an environmental facility for equipment subject to maintenance leads to service unavailability “A” of the RMS.	Key management can prevent service unavailability due to destruction by preventing unauthorized persons from accessing the equipment.	3 > 2	2	1	6 > 4

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.	—	—	—	—	—	—	—	—	—
			Physical security for offices, rooms and facilities shall be designed and applied. Physical protection and guidelines for working in secure areas shall be designed and applied.	13	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
				14	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
				16	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
				21	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Physical security for offices, rooms and facilities shall be designed and applied. Physical protection and guidelines for working in secure areas shall be designed and applied.	21	B1	i	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
				22	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
				23	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
				25	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
				41	D1	p	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Physical security for offices, rooms and facilities shall be designed and applied. Physical protection and guidelines for working in secure areas shall be designed and applied.	41	D1	p	Tapping “C” into the HCF network from an internal source by an 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
				42	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
				43	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
				45	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Physical and environmental security	A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	Physical security for offices, rooms and facilities shall be designed and applied. Physical protection and guidelines for working in secure areas shall be designed and applied.	54	E1	d	Bringing out "C" or replacement 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
				56	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 may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	—	—	—	—	—	—	—	—	—
	A.9.2 Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	18	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
				25	B1	m	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
							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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				45	D1	m	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
A.9 Physical and environmental security	A.9.2 Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	45	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
				56	E1	f	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
							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
			Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	—	—	—	—	—	—	—	—	—
			Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	—	—	—	—	—	—	—	—	—
			Equipment shall be correctly maintained to ensure its continued availability and integrity.	—	—	—	—	—	—	—	—	—
			Equipment, information or software shall not be taken off site without prior authorization.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal.	11	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
A.9 Physical and environmental security	A.9.2 Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	Equipment, information or software shall not be taken off site without prior authorization. Security shall be applied to off site equipment, taking into account the different risks of working outside the organization's premises. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.(A.11.3.3)	53	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
A.10 Communications and operations management	A.10.1 Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	Operating procedures shall be documented, maintained and made available to all users who need them.	—	—	—	—	—	—	—	—	—
			Changes to information processing facilities and systems shall be controlled.	15	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 programme because of virus measures. Virus measures can detect and eliminate backdoors or information-stealing programmes.	3 > 2	3	2	18 > 12
				21	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
A.10 Communications and operations management	A.10.1 Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	Changes to information processing facilities and systems shall be controlled.	24	B1	I	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 programmes.	3 > 2	3	2	18 > 12
				41	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
				44	D1	I	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 programme.	3 > 2	3	2	18 > 12
				55	E1	e						

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	—	—	—	—	—	—	—	—	—
			Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	16	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.10 Communica-tions and operations management	A.10.2 Third party service delivery management	To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.									
			The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.									
			Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.									

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
	A.10.3 System planning and acceptance	To minimize the risk of systems failures.	The use of resources shall be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.	—	—	—	—	—	—	—	—	—
			Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	—	—	—	—	—	—	—	—	—
A.10 Communica-tions and operations management	A.10.4 Protection against malicious and mobile code	To protect the integrity of software and information.	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	15	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 programme because of virus measures. Virus measures can detect and eliminate backdoors or information-stealing programmes.	3 > 2	3	2	18 > 12
				24	B1	I						
				44	D1							
				55	E1	e						
	A.10.5 Back-up	To maintain the integrity and availability of information and information processing facilities.	Backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	17	A1	f	Failure “A” of RSC equipment leads to service unavailability “A” of the RMS.	Maintenance, checkout and backup can prevent service unavailability.	3 > 2	2	2	12 > 8
				18	A1	g	Failure “A” of RSC equipment leads to service unavailability “A” of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
				26	B1	m	Failure “A” of RSC network equipment leads to service unavailability “A” of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
					B2							

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
				27	B1	n	Failure "A" or cable disconnection "A" of an environmental facility for RSC network equipment leads to service unavailability "A" of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
					B2							
				46	D1	m	Failure "A" of HCF network equipment leads to service unavailability "A" of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
				47	D1	n	Failure "A" or cable disconnection "A" of an environmental facility for HCF network equipment leads to service unavailability "A" of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
				57	E1	f	Failure "A" of equipment subject to maintenance leads to service unavailability "A" of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
				58	E1	g	Failure "A" of the environmental facility for equipment subject to maintenance leads to service unavailability "A" of the RMS.	Maintenance, checkout and backup can prevent service unavailability.				
A.10 Communications and operations management	A.10.6 Network security management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	Networks shall be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.	27	B2	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. Access control (login) can prevent non-RSC network administrators from unauthorized login.	1	3	1	3
			Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.				Hoaxing "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 hoaxing of RSC network equipment.				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							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.				
							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.				
A.10 Communica-tions and operations management	A.10.6 Network security management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	Networks shall be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit. Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	22	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							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.				
				23	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.	Internal path check on the RSC side to detect traces of tapping on the path.				
							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.				
				24	B2	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 programme because of virus measures. Virus measures can detect and eliminate backdoors and information-stealing programmes.	1	3	2	6
A.10 Communica-tions and operations management	A.10.6 Network security management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	Networks shall be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.	25	B2	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 access by unauthorized persons.	1	3	1	3

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.									
							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 access by authorized persons while alone.				
							Tampering “C” with RSC network equipment leads to unexpected exposure “C” of PHI information.	Sealing is designed to detect traces of tampering.				
							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.				
				28	B2	o	Wrong setting “C” leads to unexpected exposure “C” of PHI information.	Training and skill standards can prevent service trouble due to incorrect input and accidental deletion by maintaining and improving the qualifications of operators.				
	A.10.7 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.	There shall be procedures in place for the management of removable media.	—	—	—	—	—	—	—	—	—
			Media shall be disposed of securely and safely when no longer required, using formal procedures.	13	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 a shredding machine can prevent third parties, RSC personnel or RSC network administrators from viewing or removing sheets of paper.	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								Room entry management can restrict room entry by third parties, RSC personnel or RSC network administrators and block viewing or removing sheets of paper.				
A.10 Communica-tions and operations management	A.10.7 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.	Media shall be disposed of securely and safely when no longer required, using formal procedures.	22	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
				42	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
			Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			System documentation shall be protected against unauthorized access.	—	—	—	—	—	—	—	—	—
	A.10.8 Exchange of information A.10.9 Electronic commerce services	To maintain the security of information and software exchanged within an organization and with any external entity. To ensure the security of electronic commerce services and their secure use.	Agreements shall be established for the exchange of information and software between the organization and external parties.	—	—	—	—	—	—	—	—	—
A.10 Communications and operations management	A.10.8 Exchange of information A.10.9 Electronic commerce services	To maintain the security of information and software exchanged within an organization and with any external entity. To ensure the security of electronic commerce services and their secure use.	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	—	—	—	—	—	—	—	—	—
			Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	—	—	—	—	—	—	—	—	—
			Formal exchange policies, procedures and controls shall be in place to protect the exchange of information	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			through the use of all types of communication facilities.									
			Information involved in electronic messaging shall be appropriately protected. The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	—	—	—	—	—	—	—	—	—
			Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	—	—	—	—	—	—	—	—	—
A.10 Communica-tions and operations management	A.10.10 Monitoring	To detect unauthorized information processing activities.	Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. Logging facilities and log information shall be protected against tampering and unauthorized access. System administrator and system operator activities shall be logged. Faults shall be logged, analysed, and appropriate action taken.	11	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
				12	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				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								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".				
A.10 Communications and operations management	A.10.10 Monitoring	To detect unauthorized information processing activities.	Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. Logging facilities and log information shall be protected against tampering and unauthorized access. System administrator and system operator activities shall be logged. Faults shall be logged, analysed, and appropriate action taken.	51	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
				52	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 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	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								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."				
A.10 Communica-tions and operations management	A.10.10 Monitoring	To detect unauthorized information processing activities.	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	11	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
				12	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.				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								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”.				
A.10 Communica-tions and operations management	A.10.10 Monitoring	To detect unauthorized information processing activities.	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	51	E1	a	Replacement “I” of PHI information in equipment subject to onsite maintenance by primary service personnel leads to concoction “I” of the information.	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
				52	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.	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								Access control (write protection and file erasure prohibition) can prevent RSC service personnel from replacing files.				
A.10 Communica-tions and operations management	A.10.10 Monitoring	To detect unauthorized information processing activities.	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	52	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
			The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	—	—	—	—	—	—	—	—	—
A.11 Access control	A.11.1 Business requirement for access control	To control access to information.	An access control policy shall be established, documented and reviewed based on business and security requirements for access.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
	A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	12	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
				21	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
A.11 Access control	A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	21	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	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								RSC network equipment include access control (login), especially at RSC exit, network separation/forced path (FW)/filtering and remote diagnosis port protection.				
				41	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 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
A.11 Access control	A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	51	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							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
				52	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 network administrators from illegal login.	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Access control	A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	The allocation and use of privileges shall be restricted and controlled.	12	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
				21	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. Access control (login) can prevent third parties, RSC personnel or RSC network administrators from unauthorized login.				
				41	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
				51	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	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 Access control	A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	The allocation and use of privileges shall be restricted and controlled.	51	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
				51	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
				52	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

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			The allocation of passwords shall be controlled through a formal management process.	—	—	—	—	—	—	—	—	—
			Management shall review users' access rights at regular intervals using a formal process.	—	—	—	—	—	—	—	—	—
A.11 Access control	A.11.3 User responsibilities	To prevent unauthorized user access and compromise or theft of information and information processing facilities.	Users shall be required to follow good security practices in the selection and use of passwords.	12	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 hoaxing of RSC equipment.	3 > 2	3	1	9 > 6
				21	B1	i	Hoaxing “C” of RSC network equipment by using a leaked password, 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.	Periodic changing of passwords prevents hoaxing of RSC network equipment.	3 > 2	3	1	9 > 6
							Hoaxing “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 hoaxing of RSC network equipment.				
					B2		Hoaxing “C” of RSC network equipment by using a leaked password, 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.	Periodic changing of passwords prevents spoofing of RSC network equipment.				
				41	D1	p	Hoaxing “C” of HCF network equipment by using a leaked password, from an external source by non-RSC personnel, including	Periodic changing of passwords prevents hoaxing of HCF network equipment.	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							RSC personnel of other companies, leads to unauthorized use “C” of PHI information stored on the HCF network and exposure “C” of the information.					
A.11 Access control	A.11.3 User responsibili-ties	To prevent unauthorized user access and compromise or theft of information and information processing facilities.	Users shall be required to follow good security practices in the selection and use of passwords.	41	D1	p	Hoaxing “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 hoaxing of HCF network equipment.	3 > 2	3	1	9 > 6
				51	E1	a	Hoaxing “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 hoaxing of equipment subject to maintenance.	3 > 2	3	1	9 > 6
				52	E1	a	Hoaxing “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 hoaxing of the equipment subject to maintenance.	3 > 2	3	1	9 > 6
							Use of a leaked password from an internal source, or hoaxing “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 hoaxing of the equipment subject to maintenance.	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Users shall ensure that unattended equipment has appropriate protection.	—	—	—	—	—	—	—	—	—
A.11 Access control	A.11.4 Network access control	To prevent unauthorized access to networked services.	Users shall only be provided with access to the services that they have been specifically authorized to use.	—	—	—	—	—	—	—	—	—
			Appropriate authentication methods shall be used to control access by remote users.	21	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
				40	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 of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
							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
A.11 Access control	A.11.4 Network access control	To prevent unauthorized access to networked services.	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	—	—	—	—	—	—	—	—	—
			Physical and logical access to diagnostic and configuration ports shall be controlled.	21	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
				41	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)	3 > 2	3	1	9 > 6

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
								especially at HCF exit, network separation/forced path (FW)/filtering and remote diagnosis port protection.				
			Groups of information services, users and information systems shall be segregated on networks.	—	—	—	—	—	—	—	—	—
A.11 Access control	A.11.4 Network access control	To prevent unauthorized access to networked services.	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.	—	—	—	—	—	—	—	—	—
			Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	—	—	—	—	—	—	—	—	—
	A.11.5 Operating system access control	To prevent unauthorized access to operating systems.	Access to operating systems shall be controlled by a secure log-on procedure.	—	—	—	—	—	—	—	—	—
			All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	—	—	—	—	—	—	—	—	—
			Systems for managing passwords shall be interactive and shall ensure quality passwords.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	—	—	—	—	—	—	—	—	—
			Inactive sessions shall shut down after a defined period of inactivity.	—	—	—	—	—	—	—	—	—
			Restrictions on connection times shall be used to provide additional security for high-risk applications.	—	—	—	—	—	—	—	—	—
A.11 Access control	A.11.6 Application and information access control	To prevent unauthorized access to information held in application systems.	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	—	—	—	—	—	—	—	—	—
			Sensitive systems shall have a dedicated (isolated) computing environment.	—	—	—	—	—	—	—	—	—
	A.11.7 Mobile computing and teleworking	To ensure information security when using mobile computing and teleworking facilities.	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	—	—	—	—	—	—	—	—	—
			A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	—	—	—	—	—	—	—	—	—
A.12 Information systems acquisition, development and maintenance	A.12.1 Security requirements of information systems	To ensure that security is an integral part of information systems.	Statements of business requirements for new information systems or enhancements to existing information systems shall specify the requirements for security controls.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
	A.12.2 Correct processing in applications	To prevent errors, loss, unauthorized modification or misuse of information in applications.	Data input to applications shall be validated to ensure that this data is correct and appropriate.	—	—	—	—	—	—	—	—	—
			Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	—	—	—	—	—	—	—	—	—
			Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and appropriate controls identified and implemented.	—	—	—	—	—	—	—	—	—
			Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	—	—	—	—	—	—	—	—	—
	A.12.3 Cryptographic controls	To protect the confidentiality, authenticity or integrity of information by cryptographic means.	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	1a 29 39	A2 B2 C1	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
			Key management shall be in place to support the organization's use of cryptographic techniques.	—	—	—	—	—	—	—	—	—
A.12 Information systems acquisition, development and maintenance	A.12.4 Security of system files	To ensure the security of system files.	There shall be procedures in place to control the installation of software on operational systems.	—	—	—	—	—	—	—	—	—
			Test data shall be selected carefully, and protected and controlled.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Access to program source code shall be restricted.	—	—	—	—	—	—	—	—	—
	A.12.5 Security in development and support processes	To maintain the security of application system software and information.	The implementation of changes shall be controlled by the use of formal change control procedures.	—	—	—	—	—	—	—	—	—
			When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	—	—	—	—	—	—	—	—	—
			Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	—	—	—	—	—	—	—	—	—
			Opportunities for information leakage shall be prevented.	—	—	—	—	—	—	—	—	—
			Outsourced software development shall be supervised and monitored by the organization.	—	—	—	—	—	—	—	—	—
	A.12.6 Technical Vulnerability Management	To reduce risks resulting from exploitation of published technical vulnerabilities.	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	—	—	—	—	—	—	—	—	—
A.13 Information security incident management	A.13.1 Reporting information security events and weaknesses	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing	Information security events shall be reported through appropriate management channels as quickly as possible.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
		timely corrective action to be taken.	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.									
	A.13.2 Management of information security incidents and improvements	To ensure a consistent and effective approach is applied to the management of information security incidents.	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	—	—	—	—	—	—	—	—	—
			There shall be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.	—	—	—	—	—	—	—	—	—
			Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	—	—	—	—	—	—	—	—	—
A.14 Business continuity management	A.14.1 Information security aspects of business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	—	—	—	—	—	—	—	—	—
			Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	17	A1	f	The disaster-affected RSC equipment “A” leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.	3 > 2	2	1	6 > 4
				18	A1	g	The disaster-affected environmental facility “A” of the RSC leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				
				26	B1 B2	m	The disaster-affected RSC network facility “A” leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				
				27	B1 B2	n	The disaster-affected environmental facility “A” for RSC network equipment leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				
				46	D1	m	The disaster-affected HCF network facility “A” leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				
				47	D1	n	The disaster-affected environmental facility “A” for HCF network equipment leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				
A.14 Business continuity management	A.14.1 Information security aspects of business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	57	E1	f	The disaster-affected equipment subject to maintenance “A” leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.	3 > 2	2	1	6 > 4
				58	E1	g	The disaster-affected environmental facility “A” of the equipment subject to maintenance leads to service unavailability “A” of the RMS.	Disaster measures and business continuation plans can minimize damage loss and enable quick recovery.				

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance.	—	—	—	—	—	—	—	—	—
			Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.	—	—	—	—	—	—	—	—	—
A.15 Compliance	A.15.1 Compliance with legal requirements	To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented and kept up to date for each information system and the organization.	—	—	—	—	—	—	—	—	—
			Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	—	—	—	—	—	—	—	—	—
A.15 Compliance	A.15.1 Compliance with legal requirements	To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.	—	—	—	—	—	—	—	—	—
			Data protection and privacy shall be ensured as required in relevant legislation,	—	—	—	—	—	—	—	—	—

Table A.1 (*continued*)

Clause of ISO/IEC 27001:2005	Subclause of ISO/IEC 27001:2005	Control objectives	Controls	No.	Site	Asset	Example of threat (C: confidentiality, I: integrity, A: availability)	Example of control measures	V	I	L	E
			regulations, and, if applicable, contractual clauses.									
			Users shall be deterred from using information processing facilities for unauthorized purposes.	—	—	—	—	—	—	—	—	—
			Cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations.	—	—	—	—	—	—	—	—	—
	A.15.2 Compliance with security policies and standards, and technical compliance	To ensure compliance of systems with organizational security policies and standards.	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	—	—	—	—	—	—	—	—	—
			Information systems shall be regularly checked for compliance with security implementation standards.	—	—	—	—	—	—	—	—	—
	A.15.3 Information systems audit considera-tions	To maximize the effectiveness of and to minimize interference to/from the information systems audit process.	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed upon to minimize the risk of disruptions to business processes.	—	—	—	—	—	—	—	—	—
			Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	—	—	—	—	—	—	—	—	—

Notes for the interpretation of Table A.1.

1: Items of columns

Items	Meaning
Clause	Clause, subclause, control objective and control are provided in ISO/IEC 27001:2005.
Subclause	
Control objective	
Control	
No.	Number of the threat shown in Annex A of ISO/TR 11633-1:2009
Sites	A1: RSC equipment A2: A1 on using VPN B1: RSC internal network B2: B1 on using VPN C1: External network D1: HCF internal network E1: HCF target device
Assets	a: PHI on memory, disk and screen b: Encryption algorithm, keys, and key distribution method c: Memos and print-outs of PHI d: Backup media of PHI e: Software dealing with PHI f: Equipment dealing with PHI g: Environmental facilities for equipment dealing with PHI h: Operators dealing with PHI i: PHI on RSC internal network j: Memos and print-outs of communication trace of PHI k: Backup media of communication trace of PHI l: Software of network equipment m: Network equipment n: Environmental facilities of network equipment o: Operators of network equipment p: PHI on HCF internal network
Example of threat	Example of threat
Example of control measures	Example of control measures
V (Vulnerability)	Level of confidentiality, integrity or availability (Table A.2 to A.4 of ISO/IEC 27001:2005) Level of before selecting controls and after are shown
I (Influence)	Level of influence (see 5 below)
L (Outage likelihood)	Level of outage likelihood (see 6 below)
E (Evaluation)	Level of evaluation = vulnerability × influence × outage likelihood Level of before selecting controls and after are shown

2: Level of confidentiality

3	Serious vulnerability to exposure by peeping/theft, unauthorized login/hoaxing or carrying out.
2	Moderate vulnerability to exposure by peeping/theft, unauthorized login/hoaxing or carrying out.
1	Negligible vulnerability to exposure by peeping/theft, unauthorized login/hoaxing or carrying out.

3: Level of integrity

3	Serious vulnerability to fabrication or denial by alteration, replacement or deletion.
2	Moderate vulnerability to fabrication or denial by alteration, replacement or deletion.
1	Negligible vulnerability to fabrication or denial by alteration, replacement or deletion.

4: Level of availability

3	Serious vulnerability to service interruption due to failure, disaster, cable discontinuity or service failure.
2	Moderate vulnerability to service interruption due to failure, disaster, cable discontinuity or service failure.
1	Negligible vulnerability to service interruption due to failure, disaster, cable discontinuity or service failure.

5: Level of influence

3	Likelihood of large amount of influence in operations.
2	Likelihood of some influence in operations.
1	Negligible influence in operations.

6: Level of outage likelihood

3	High likelihood of occurrence.
2	Low likelihood of occurrence.
1	Negligible likelihood of occurrence.

Bibliography

[1] ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[2] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[3] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[4] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[5] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

ICS 35.240.80

Price based on 66 pages