© ISO 2008 – All rights reserved

ISO TC 215/SC

Date: 2008-11-13

ISO/TR 11636:2008(E)

ISO TC 215/SC /WG 4

Secretariat: ANSI

Health informatics — Dynamic on-demand virtual private network for health information infrastructure

Convenor of ISO/TC 215/WG 4	Secretary of ISO/TC215/WG 4
Ross Fraser , Sextant Software	Alice Rideau Association Française de Normalisation
27 Hillcrest Park Toronto ON M4X 1E8 Canada	11, rue Francis de Préssensé 93571 La Plaine Saint Denis cedex France
E-mail: RossFraser@aol.com	E-mail: Alice.rideau@afnor.org
Phone: +1-416-960-5872 Fax: +1-416-920-5202	Phone: + 33 (0)1 41 62 84 01 Fax: +33 (0)1 49 17 90 00

Document type: Technical Report
Document subtype:
Document stage: (30) Committee Stage
Document language: E

C:¥Documents and Settings¥nose¥デスクトップ¥Dynamic On-demand VPN for health information infrastructure.docSTD Version 2.1c2

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword 4

Introduction 5

1. Scope 6

2. Normative Reference 6

3. Terms and definitions 6

4. Abbreviated terms 8

5. Network features in the healthcare field 9

5.1. Pattern of current or expected information services in the healthcare field 9

5.2. Category of healthcare information to be protected (information assets) 11

5.3. Network requirements in the healthcare field 11

6. Concept of network construction in the healthcare field 12

6.1. Responsibility to manage security of healthcare information exchange including personal information between independent institutions 12

6.1.1 Clear demarcation of responsibility 12

6.1.2 Precautionary measures taken within a medical institution 12

6.2. Security concepts in network systems for medical institutions 13

6.2.1 Communication via closed networks 13

6.2.2 Communication via open networks 14

7. Threat analysis and measures 15

8. Network construction in the healthcare field 16

8.1. Minimum guidelines for security management of healthcare information exchange including personal information between external institutions 16

8.2. Technical and operational checklists for evaluation of network security 17

8.3. Application of an on-demand VPN 17

9. Cases of security measures in a dynamic on-demand VPN for exchange of healthcare information with external institutions 18

9.1. Regional healthcare cooperation model with a healthcare portal 18

9.2. Online maintenance model 19

9.3. Regional cooperation model with the lead taken by a regional core hospital 19

9.4. Model for teleradiology, remote maintenance, and network conferencing with the cooperation of university hospitals, research institutions, and regional hospitals 20

9.5. University hospital model centered around teleradiology, telepathology, and network conferences conducted between a university hospital and regional hospitals 21

© ISO 2008 – All rights reserved

Annex A (informative) Threat analysis and measures 23
A.1 Extraction of network-related security requirements 23
A.2 Channel security and object security as protected assets 25
A.3 Component features related to object security of network devices 26
A.4 Location of threats and problems 26
A.5 Summary of threats to the network and security measures (channel security) 27
A.5.1 Definition of threats to the network 27
A.5.2 Examination of measures against threats 28

Annex B (informative) Security management of medical information exchange including personal data between independent institutions 30
B.1 Basic concepts 30
B.2 Clear demarcation of responsibility 30
B.3 Precautionary measures taken within a medical institution 31
B.4 Concepts of appropriate network security 33
B.4.1 Overview 33
B.4.2 Communication via closed networks 34
B.4.3 Communication via open networks 36
B.4.4 Provision of medical records to patients 37
B.5 Minimum guidelines 38

Annex C (informative) Technical and Operational Checklists for the Guideline 40
C.1 Introduction 40
C.2 Instructions for the checklist for large hospitals 44
C.3 Instructions for the checklist for small hospitals 57
C.4 Instructions for the checklist for SPs 59

Annex D (informative) Technology used: Dynamic on-demand VPN 63
D.1 VPN security objectives 63
D.2 The purpose of a dynamic on-demand VPN 64
D.3 Dynamic on-demand VPN connection method 66
D.4 Features of the dynamic on-demand VPN 67
D.5 VPN device (router) using a double-layered PKI chip 68
D.6 Registration of VPN device and application of connection 69
D.7 Precautions on application of a dynamic on-demand VPN 70
D.8 Features of double-layered PKI 71
D.9 Summary 72

© ISO 2008 – All rights reserved

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 11636 was prepared by Technical Committee ISO/TC 215, *Health informatics*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

© ISO 2008 – All rights reserved

Introduction

Currently, healthcare information is normally transferred in the form of paper documents or electronic data through schemes such as dedicated fixed lines connecting the headquarters and branches within a company, through public networks such as an Integrated Services Digital Network (ISDN), or through a dedicated network between specific institutions, enabling a virtual network for the specified users in a dedicated service network managed by communication providers, such as an Internet Protocol virtual private network (IP-VPN). Therefore, healthcare information cannot be transferred easily while maintaining security in most cases, because network configurations adequate to these solutions are limited and the costs are very high.

The uses of various service networks in the healthcare field include online claims for medical fees, online maintenance of medical devices, and remote medical care, such as teleradiology, telepathology, and healthcare information services for regional healthcare cooperation. To provide such services, however, it is necessary for multiple medical institutions to pass healthcare information to each other. A network in which a single medical institution is dynamically connected to multiple medical institutions and switched to another institution is required.

To make such a network available to many medical institutions at low cost, an open network such as the Internet can be used for connecting with different medical institutions, medical device providers, and patients. We can be used following VPNs as secure channel systems in an open network, one is Internet Protocol Security (IPsec) with Internet key exchange (IKE), described as IPsec + IKE which runs in the network layer with authentication and exchange of encryption keys, and the other is Secure Sockets Layer (SSL) protocol, which runs in the session layer with encrypted communication between a Web browser on a client and SSL servers. Thus, this is adapted to Web applications, but other applications, such as e-mail, File Transfer Protocol (FTP), and unique client/server systems, cannot be used. On the other hand, the combination of IPsec + IKE can be used with any application needed by medical institutions to provide secure channels without reconstructing any application software. In addition, SSL has an inherent risk because it provides no protection methods against well-known lower-layer attacks, session hijacking, false Address Resolution Protocol (ARP) statements, and so on.

The conventional VPN using IPsec + IKE, however, requires complicated configuration of network devices, and setting up the system without expertise could result in failure to protect healthcare information. Also, it is a fixed-type VPN and can only be connected with fixed parties.

Lately, telecommunication carriers and online service providers (OSPs) have been developing systems to provide services with security on network lines, including setting up network devices to safeguard against these threats, even for a VPN connected in an open network. When a medical institution uses these types of services, most of the responsibilities related to managing the communication lines fall to these service providers (SPs). This reduces the responsibility of the medical institution in terms of its security-related liabilities, which is well suited for organizations without many IT engineers.

A dynamic on-demand VPN, which this technical report describes, is one type of VPN. It is not a fixed connection like 1-to-1, which is generally used in ordinary VPN services. It can easily change connection to N-to-N, and the connection parameters are provided automatically by the telecommunication carrier. This makes it suitable for healthcare network infrastructure, as medical institutes are not required to be responsible for or have expertise in setting up such networks. Also, utilizing the Internet makes the dynamic on-demand VPN an inexpensive network and thus readily acceptable to medical institutions in terms of cost.

This technical report describes the threats anticipated in a healthcare network, as well as how a dynamic on-demand VPN is actually applied in the healthcare field.

© ISO 2008 – All rights reserved

Health informatics — Dynamic on-demand virtual private network for health information infrastructure

1. Scope

This technical report (TR) explains the network requirements in the healthcare field, the network security of an open network for the healthcare field, and the minimum guidelines for security management of health information exchange, including personal data, between external institutions.

These requirements will assist in understanding the operation of security and evaluation of security issues in the healthcare field, and the usefulness of a managed VPN, like a dynamic on-demand VPN.

This TR introduce examples of security measures taken in a dynamic on-demand VPN for exchange of medical information; it is not intended to specify the dynamic on-demand VPN itself.

These examples provide network solutions to potential risks in such a user environment.

2. Normative Reference

The following referenced documents are essential for the application of this document. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18028-1: Information technology - Security techniques - IT network security - Part 1: Network security management

ISO/IEC 18028-5: Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks

ISO/IEC 27799: Health informatics - Security management in health using ISO/IEC 17799

“Security and Privacy Requirements for Remote Servicing”, by NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

3. Terms and definitions

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

3.1
DMZ (demilitarized zone)
An area of a network in which any data exchange is allowed with areas outside.

3.2
HSZ (high security zone)
An area of a network in which no data shall be exchanged directly with areas outside, except for the purpose of certain remote maintenance.

© ISO 2008 – All rights reserved

3.3
IPsec
IPsec is a standard for cipher communication. It is a protocol that prevents data tampering and provides confidentiality functions for each IP packet by using an encryption technique.

3.4
Internet VPN
This is a VPN created via the Internet. By using the Internet, connections between remote networks can be managed as connections in a LAN, while maintaining confidentiality.

3.5
IP-VPN
This is a VPN created via a wide-area IP network owned by a communication carrier. By using an IP-VPN, connection between remote networks can be managed in the same manner as connection in a local area network (LAN).

3.6
LAN (local area network)
A network in which computers, printers, and other equipment are connected and data are transferred within one building.

3.7
OSI reference model
This is a model that divides the functions of communication equipment, such as computers, into a layer structure based on the design policy of Open Systems Interconnection (OSI) established by ISO for network structuring, in order to facilitate heterogeneous network data transfer. Communication functions are divided into seven layers, and the standard function module for each layer is defined.

3.8
Provider service
A service that exchanges data between a telecommunication carrier and an OSP.

3.9
Relay service
A service that establishes a connection for the sole purpose of exchanging data between a network-connected device within a medical institute and an outside device.

3.10
Remote access
This refers to connecting to a network or computer from outside by using lines such as telephone lines. Remotely accessing a distant computer enables direct operation of the computer as though it is right in front of the user.

3.11
Social insurance medical fee payment fund
This is an organization that reviews medical fees invoiced by medical institutions and makes appropriate payments. The reviews are performed by a three-party committee consisting of representatives of medical institute workers, medical insurers (e.g., health insurance companies), and academic experts. The medical institute submits a medical bill statement (receipt) and claims a payment for the treatment from the health insurance organization. An organization such as a social insurance medical fee payment fund reviews the receipt and makes a payment to the medical institution submitting the invoice.

3.12
SSL
This is a protocol that encrypts and transfers data on the Internet. It can encrypt current widely used data, such as World Wide Web (WWW) and File Transfer Protocol (FTP) data, and can securely transmit and receive privacy-related information and credit card numbers.

© ISO 2008 – All rights reserved

3.13
SZ (security zone)
An area of a network in which limited data exchange is allowed with areas outside.

3.14
VPN (virtual private network)
This is a service in which a public line can be used as if it is a dedicated line. It is used for connecting different bases of a company's internal network, instead of installing dedicated lines, to reduce cost.

3.15
WAN (wide area network)
In this network, computers in geographically different locations (e.g., at a headquarters building and multiple branches) are connected through telephone lines or dedicated lines to transfer data.

4. Abbreviated terms

For the purposes of this document, the following notations apply.

AES	Advanced Encryption Standard
AH	authentication header
ASP	application service provider
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HEASNET	HEAlthcare information Secure NETwork consortium
HMAC	Hash Message Authentication Code
IC	integrated circuit
IKE	Internet key exchange
IPsec	Internet Protocol Security
IP-VPN	Internet-Protocol-based virtual private network
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IT	information technology
LAN	local area network
L2TP	Layer 2 Tunneling Protocol
NAT	network address translation
OSI	Open Systems Interconnection
OSP	online service provider

© ISO 2008 – All rights reserved

OSPF	Open Shortest Path First
PKI	public key infrastructure
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SHA	Secure Hash Algorithm
SI	System Integrator
TLS	Transport Layer Security
TOS	Type of Service
TTL	time to live
WAN	wide area network

5. Network features in the healthcare field

5.1. Pattern of current or expected information services in the healthcare field

In the healthcare field, the information services listed below are provided. In a healthcare network, both data security and security by way of access control must be considered so that these services will not influence each other. In order to clarify the form of network use for currently available or future information services, the form of service provision for these services will be defined according to the characteristics of data access.

a) Information provision service

This is a service to provide a particular medical institution with access to patient healthcare information from another medical institution. It includes the following:

— Local collaboration service (for medical institutions and healthcare-related services, such as welfare and nursing care)

Patient medical treatment or nursing care records, including medical records, examination data, medical record summaries, physical check-up data, and care records are provided in a variety of forms, such as letters of referral and local collaboration databases.

— Medical treatment / Nursing care information provision service (for patient enquiry)

A patient medical treatment and nursing care records are disclosed to the patient according to certain criteria.

— Medical treatment / Nursing care information provision service (for general enquiry)

Information on hospitals, diseases, and various medical and nursing care practices are provided for general enquiry.

b) Internet connection service

This is a service to provide medical institutions with access to information sites on the Internet. It includes the following:

© ISO 2008 – All rights reserved

— Internet connection service (for businesses)

Medical institutions access sites judged safe by institutions related to business clients, via the Internet according to the medical institutions' security policies, obtaining academic information sites and sites providing service information, such as that of Japan's Ministry of Health, Labor and Welfare.

c) Storage / Relay service

Information is stored in a location within or outside a medical institution and then transferred to another medical institution in order to exchange the information with the distant institution. This service includes the following:

— Mail service

E-mails are stored and relayed by mail servers.

— Online claim for medical fee service

Online claims for medical fees are electronically received and transferred to other institutions. For example, a social insurance medical fee payment fund receives and examines a claim and then relays or transmits the claim to an insurer.

— Examination data delivery service

Results of clinical examination or image diagnosis are delivered from an examination company. The examination results are later used for electronic medical charts and the ordering and information processing department systems in a hospital, so that the data is readily available in these systems for reference.

d) Information processing service

An external institution that has been entrusted with information processing functions by a medical institution receives information from the medical institution and processes the information as a proxy. This service includes the following:

— ASP service

Services for medical institutions, such as electronic medical charts and online claims for medical fees, are provided as shared-use services. The healthcare information is externally stored.

— External storage (backup) service

In the event of faults or disasters, to perform system recovery of electronic medical charts and data from ordering and information processing department systems in a hospital, backup data is transmitted to and stored in an external institution.

e) Remote maintenance service

Various maintenance services, such as fault diagnosis of medical devices and fault recovery, are remotely provided by a subcontracted service company. Only connections with specific medical devices whose services are subcontracted should be available to the service company.

f) Authentication / Audit service

Fundamental authentication and audit services, such as public key infrastructure, digital signatures, and time delivery, are used by medical institutions to access particular information. These services include the following:

© ISO 2008 – All rights reserved

— Time stamp service

Time stamps affixed on digital signatures are issued, and a system clock is adjusted to collect audit logs.

— Validation authority (VA) service

The validity of public key certificates issued by a certificate authority (CA) is verified.

The forms of provision of these systems are analyzed, and the form of secure connection in the network is defined.

5.2. Category of healthcare information to be protected (information assets)

External attacks on networks are becoming more and more frequent. To protect healthcare information against such network threats requires maintaining its confidentiality, integrity, and availability. Information to be protected in the healthcare field includes the following, in accordance with ISO/IEC27799 5.4:

— personal healthcare information

— pseudonymised data derived from personal healthcare information via some methodology for pseudonymous identification

— statistical and research data, including anonymised data derived from personal healthcare information by removing personally identifying data

— clinical/medical knowledge not related to a specific patient or patients, including clinical decision support data (e.g., data on adverse drug reactions)

— data on health professionals and staff

— information related to public health surveillance

— audit trail data produced by healthcare information systems and containing personal healthcare information or pseudonymous data derived from personal healthcare information, or data about the actions of users in regard to personal health information, and

— system security data, including access control data and other system- related configuration data, for healthcare information systems.

Such healthcare information will be used in networks for a variety of healthcare/hygiene services, including online claims for medical fees for medical treatment, online maintenance of medical devices, remote medical care such as teleradiology and telepathology, and healthcare information services for regional healthcare cooperation. Ensuring the security of healthcare information with respect to the privacy of patients' personal information requires a more secure network.

5.3. Network requirements in the healthcare field

The following are the key features for a network used in the healthcare field.

— patients' sensitive personal information is handled

— large-volume data such as image data is handled

— medical institutions exchange information in a local area

© ISO 2008 – All rights reserved

— medical devices, network devices, and users must be authenticated as the number of parties to communication increases

— network construction expenses will increase

In view of these features, the requirements for a network in the healthcare field are as follows:

— secure communication

— high-speed communication of large-volume data

— implementation and extension of the network to support N-to-N connection

— authentication of members (users, organizations, and devices)

— cost deduction related to secure network connection

6. Concept of network construction in the healthcare field

A typical situation of healthcare information exchange with external institutions involves networks connecting a regional core hospital, clinics, pharmacies, and examination centers as part of regional healthcare cooperation efforts, together with online maintenance companies for medical devices. Another situation involves online claims for medical fees to a medical fee payment fund by using ASP-type services.

If medical institutions use networks to exchange healthcare information with other institutions, the information must be sent to the intended organization in a secure way that never allows others to have access. This network security must be guaranteed on the communication path from the sender's device to the recipient's device. Transmitted data must be protected from threats like wiretapping, tampering, intrusion, spoofing, and interference.

This chapter assumes certain situations inherent to healthcare information exchange via networks, focusing on the network connection methods to be used.

6.1. Responsibility to manage security of healthcare information exchange including personal information between independent institutions

6.1.1 Clear demarcation of responsibility

By contract, the sender and the recipient must agree on demarcation of responsibility for data transmission on the communication path, such as handling of communications failure and other accidents. Then, they must decide how to share managerial responsibility among themselves, the OSP, and the telecommunication carrier. They must also clarify the scope of managerial responsibility to be assigned to another organization and define which organization should take the initiative in dealing with possible service failures.

6.1.2 Precautionary measures taken within a medical institution

The medical institution sending healthcare information has managerial responsibility for the information during the whole process in which the information is transmitted via networks (provided by the telecommunication carrier) and then received by the intended recipient in an appropriate manner.

Note here that “managerial responsibility” means responsibility for the information in electronic form; in other words, it means responsibility for ensuring the authenticity of both the content and the persons referred to. For example, encryption here means encrypting healthcare information to prevent outsiders from determining what the information means, even if they have wiretapped the communication path. Digital signatures are helpful for detecting tampering.

© ISO 2008 – All rights reserved

From these viewpoints, medical institutions that are going to transmit information are responsible for suitably protecting the information and must therefore be aware of the following:

a) Protection against wiretapping

When information is exchanged over networks, it can be stolen by way of, for example, a virtual bypass built on the communication path or a physical device attached to a network device. Medical institutions should take proper measures to protect healthcare information even if it is stolen during transmission or an unexpected information leakage or incorrect transmission occurs. One possible measure is to encrypt the healthcare information itself. The timing and strength level of the encryption vary depending on the confidentiality level of the information and the usage of the information system in a medical institution. If healthcare information is transmitted through networks from medical institutions, it is preferable that the information be encrypted.

b) Protection against tampering

When information is transmitted over networks, the risk of tampering is reduced if it is encrypted. The information can still, however, be altered intentionally or unintentionally because of a failure on the communication path or other possible causes. Since information can be transmitted without encryption, the sender must take precautions against tampering. One tampering detection method is the use of digital signatures.

c) Protection against spoofing

Since networking is not a face-to-face communication method, medical institutions must ensure that the recipient medical institution is correct when sending information over networks. Also, medical institutions must verify the identities of both the medical institution sending the information and the transmitted information itself. For this purpose, some mutual authentication method should be used to identify the recipient/sender properly at the start/end point of communication, particularly by using proven authentication systems such as public key and symmetric-key cryptography. In addition to its application for tampering prevention, the use of digital signatures for healthcare information is also helpful in identifying the medical institution sending the information.

6.2. Security concepts in network systems for medical institutions

Networks with appropriate costs and operation must be selected according to analysis of information security. Then, the parties responsible for network security must be defined by contract: the telecommunication carrier, the medical institution, or both. This situation roughly divides into the following two cases:

— a protected network path provided by the telecommunication carrier and an OSP, and

— a dubious network path provided by the telecommunication carrier and an OSP.

As stated above, medical institutions planning to exchange healthcare information via networks should select an appropriate type of network, considering how responsibilities should be shared according to the form of services that they use. They should also understand the characteristics of their security technologies, identify allowable risks, and, if necessary, explain the risks to their patients in order to demonstrate their accountability.

Among a wide variety of network services, the following sections assume several cases and list some key points.

6.2.1 Communication via closed networks

A "closed network" here means a dedicated network for business use and is defined as a network not connected to the Internet. There are three connection forms that offer closed networks: a common carrier leased line, a public network, and a closed IP communication network.

© ISO 2008 – All rights reserved

Since these networks are not connected to the Internet, they are basically at lower risk of wiretapping, spoofing, and tampering. The risk of wiretapping by a physical method cannot be eliminated, however, and it might be necessary to encrypt the information to be transmitted.

The different features of the three forms of closed networks are described below.

a) Connection over a telecommunication carrier leased line

While network quality is good, extensibility as a form of network connection is low, and the cost is generally high. Still, it is worthwhile to implement this line if a large amount of significant information needs to be constantly transmitted.

b) Connection over a public network

Omitting a mechanism for phone number confirmation can result in connection and information transmission to a wrong number. As with a telecommunication carrier leased line, this public network system has low extensibility. The transmission speed is lower than that of currently popular broadband connections. This system is not suitable for sending large amounts of information and large files such as those containing image data.

c) Connection over a closed IP communication network

This form of connection can be implemented at lower cost than connection over a telecommunication carrier leased line. Appropriate selection of the contract type and the category of network service can ensure enough bandwidth to transmit large amounts of information and large files.

These three forms of communication via closed networks have no risk of intrusion from outsiders, and in that sense, they are safe. Connection services generally do not, however, offer encryption of the data to be transmitted. There can be cases where different networks supported by different telecommunication carriers are interconnected via connection points. When networks are interconnected in this way, the recipient's address can sometimes be interpreted, or additional data can be added to the sender information's to be transmitted. This might cause accidental information leaks.

For these reasons, even with a closed network, medical institutions should take security measures, such as encryption of healthcare information to make their data harder to discern and introduction of a tampering detection system, as described in 6.1.2.

6.2.2 Communication via open networks

Considering the wide spread of the broadband network environment, its applications are likely to expand—for example, by reducing implementation costs by using open networks or building extensive mechanisms for regional healthcare cooperation. Since there are various threats on the communication path, such as wiretapping, tampering, intrusion, spoofing, and interference, sufficient security measures must be taken. Encryption of healthcare information is also necessary.

a) Connection over a protected network path by telecommunication carriers and OSP

Note that even with an open network connection, the telecommunication carrier and OSP might provide their services via a protected network path with security measures against threats. Medical institutions that use such services can transfer most of their responsibility for communication path management to these businesses by defining demarcation points of responsibility by contract.

b) Connection over a medical institution's own open networks

If medical institutions use their own open networks to exchange personal information and other healthcare information with other institutions, most of the managerial responsibility falls on the medical

© ISO 2008 – All rights reserved

institutions themselves. Hence, they must take full responsibility for implementing such networks, and be aware of their responsibility for guaranteeing technical safety.

With an open network connection, the necessary level of security on the network path depends on the layer at which the security is guaranteed, among the seven layers of the OSI hierarchical model. (Refer to Annex C)

For example, when communication is made using the SSL protocol, the communication path is encrypted at the fifth layer, the Session Layer. While the path may be encrypted appropriately, there is a possible risk of wiretapping in the course of encryption and an inappropriate path being established, since the negotiations before starting communications are not encrypted. When IPsec is used, a path is encrypted in a layer below the second or third layer, the Network Layer, and thus the risk of wiretapping is lower than for communication encrypted by the SSL protocol. Exchange of an encryption key for the path uses IKE to encrypt the details of the negotiations (SA parameter of IPsec). This eliminates the risk of wiretapping, and the combination of IPsec + IKE ensures safety.

Regarding SSL/TLS (a modified version of SSLv3), RFC3552 specifies that TLS shall depend on a reliable protocol, such as the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP). SSL using TCP in the Transport Layer does not support applications using the User Datagram Protocol (UDP). TLS is influenced by attacks on the IP Layer without IPsec. Research has pointed out the possible risk of a security hole in this approach, such as session hijacking or ARP spoofing at a LAN access point. Cases of financial damage have been reported, including data pilferage and data tampering in financial applications or the like.

7. Threat analysis and measures

To satisfy the requirements of networks in the healthcare field according to the concept of implementation, it is necessary to perform threat analysis and take corresponding measures technically or by way of operation.

A network for healthcare information, including patients' personal information, is composed of multiple elements, such as the players, technology and operation of medical institutions and network devices. To assure the security of the entire network, the safety of each element should be established. It is necessary to examine the technical and operational specifications related to security and considered by medical institutions throughout the network before designing the network and defining its requirements.

The security of each element is provided by adhering to definite standards, rules, and guidelines so as to maintain a certain level of security. The details are given in Annex A. Threat models are assumed on the basis of threats to the network or assets to be protected, in terms of RFCs. Guidelines and reference documents such as RFCs related to security are referenced to examine various security measures and evaluate their effectiveness. Currently, the protocol of IPsec + IKE as the basis of a VPN system has been concluded to be effective as a channel security measure using a combination of available technical elements.

© ISO 2008 – All rights reserved

8. Network construction in the healthcare field

8.1. Minimum guidelines for security management of healthcare information exchange including personal information between external institutions

From the viewpoint of ensuring channel security, the following measures[1] are required against network threats, including wiretapping, tampering, and spoofing:

a) Protected path

— Protection against message insertion and virus injection into the network path

— Protection against wiretapping by crackers who try to steal passwords or message texts on the path between facilities

— Protection against spoofing such as session hijacking and IP address spoofing

For example, the use of IPsec＋IKE meets the above requirements to ensure network path security.

b) Other party authentication specified by the user at the gateways of the sender and recipient institutions and in the network devices

Useful measures include:

— PKI-based authentication, and

— Use of a pre-shared key.

c) Prevention of spoofing as an authorized user or device

d) Use of network devices that are confirmed as secure and proper routing to prevent communication with different institutions via a VPN device in the institution.

e) Security measures, including encryption of information to be transmitted, taken by both the sender and the recipient:

— Use of SSL/TLS

— Use of Secure / Multipurpose Internet Mail Extensions (S/MIME)

— Encryption of files

— Use of encryption keys conforming to the e-government recommended cipher list

f) Assignment of responsibilities and clarification of demarcation points of responsibility by contracts among medical institutions, telecommunication carriers, SIs, system operation companies, and device maintenance companies offering remote maintenance services

g) Avoidance of unnecessary logins if remote maintenance is conducted

---

[1] The details of these guidelines are given in section 6.10 of Annex B: “Guidelines for the Security Management of the Medical Information System” (second version), issued by Japan’s Ministry of Health, Labor and Welfare.

© ISO 2008 – All rights reserved

h) Confirmation of the scope of responsibility for threat control and communication line quality, including line availability, before signing a contract with a telecommunication carrier or OSP

8.2. Technical and operational checklists for evaluation of network security

Services using a network in the healthcare field include the following: online claims for medical fees, online maintenance of medical devices, remote medical care, and healthcare information services for regional healthcare cooperation. From the viewpoint of a particular medical institution, the connecting parties are not fixed and connections will be switched as required between multiple destinations. In such a case, to ensure the reliability of the healthcare information handled, SIs and SPs that are compliant with the “Guidelines for the Security Management of the Medical Information System, second version" (refer to Annex B of this technical report) should be preferentially selected. The medical institution should selects a product by considering both its specifications and its operating conditions and related costs, so that the nonconforming portion of the product specifications will be covered by operation for the purpose of satisfying all the specifications described in the Guidelines. The items involved in handling healthcare information as defined in the Guidelines and observed by a medical institution have been exhaustively compiled into checklists (refer to Annex C for details).

These checklists cover all the requirements specified in the Guidelines for medical institutions to meet when they deal with healthcare information. The checklists range from operational requirements to technical and system requirements. For ease of reference, the checklists classify medical institutions according to their functions. For medical institutions to observe the Guidelines, SIs and SPs must provide services and carry out their functions in accordance with the Guidelines. Therefore, each checklist comprises three different sub-checklists—for managers of medical institutions, for SIs, and for SPs—with different items to be examined by different providers of service functions. The medical installation managers, Sis, and SPs should each evaluate the network security of the medical institution and select products by considering both the product specifications and the operating conditions and related costs.

8.3. Application of an on-demand VPN

Now, sophisticated medical devices have penetrated into medical institutions, including medium- to small-sized institutions. Greater diagnostic capability is required as devices become more sophisticated. The problem is that the absolute number of specialists for sophisticated medical devices is limited. What is expected is utilization of remote diagnosis support through IT. Remote diagnosis eliminates the need for a specialist to take precious time to travel to a requesting hospital, enabling quick, simple support. Utilization of IT does not lead to a decrease in the absolute number of specialists, as the demand for diagnosis is increasing. If it was possible to send images promptly, the number of requests or requesting medical institutions might grow. The system cooperation between the requesting hospital and a hospital offering remote diagnosis will become closer. With the expansion of available facilities, the combinations of on-demand communication will become more complicated. It is desirable that a network of facilities maintains high security while appropriately controlling N-to-N connections. Furthermore, easy, low-cost utilization of remote diagnosis is necessary even in medical institutions where network technicians are not resident and reduced responsibility of the medical institution in terms of a demarcation point is desirable. These contradictory needs can be satisfied by using a dynamic on-demand VPN for the facility network infrastructure on an Internet line, as an example satisfying the Guidelines under section 8.1.

A dynamic on-demand VPN assures the validity of devices connecting sites to each other. Moreover, the demarcation of responsibilities between a medical institution and an SP is made clear, and staff configuring or using the service is reliably authenticated, thus assuring high security in terms of operation. Multiple combinations of connections can be preset, and secure communication is possible with a particular distant party alone as required. An outline of the specifications of a dynamic on-demand VPN is shown in Annex D.

A dynamic on-demand VPN is a kind of managed VPN in which the responsibilities for line connection belong to an SP, although the medical institution must observe its own obligations. In particular, in a healthcare network that handles sensitive personal information, it is necessary to monitor the security of such information, as well as observance of obligations by the SP.

© ISO 2008 – All rights reserved

9. Cases of security measures in a dynamic on-demand VPN for exchange of healthcare information with external institutions

The case study described here shows examples of security measures for the exchange of healthcare information with external institutions via a dynamic on-demand VPN.

The dynamic on-demand VPN is applicable as an example of a network providing security of communication paths, which are guaranteed against network threats, by the telecommunication carrier and OSP as described in section 6.2.2, thus satisfying the network requirements described in section 5.3 and the guidelines mentioned in section 8.1.

The dynamic on-demand VPN is initially used for regional healthcare cooperation, remote medical care, online maintenance, and so forth. The following demonstrates various application models.

9.1. Regional healthcare cooperation model with a healthcare portal

Figure 1 shows a regional healthcare cooperation model, in which healthcare information is exchanged as necessary among medical institutions (regional core hospitals, clinics, etc.), an examination center, and pharmacies over a network in a community. In this model, each patient can check his or her consultation appointment status and medical examination results from home through the healthcare portal. Through the network, the regional core hospitals receive referrals and medical examination data for patients from clinics, diagnose the patients, receive medical examination results from the examination center, and send prescription information to pharmacies. In this model, the network connections are not fixed, and switching of N-to-N connections among a number of medical institutions must be supported. Because healthcare information is exchanged over the network, the network requires adequate security, through the use of a dynamic on-demand VPN via the Internet.

To this end, network devices for the dynamic on-demand VPN are installed in the various medical institutions, and secure communication is provided via the Internet under the management of an SP, by way of the dynamic on-demand VPN.

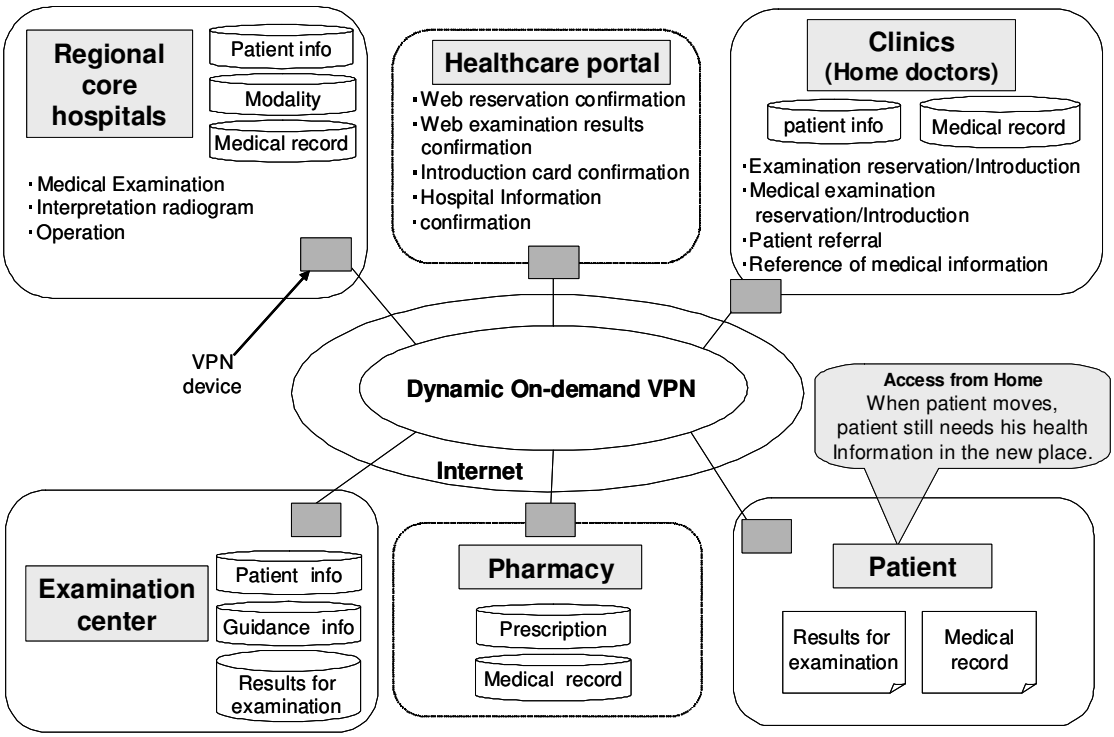

Figure 1 — Regional healthcare cooperation model with a healthcare portal, using a dynamic on-demand VPN

© ISO 2008 – All rights reserved

9.2. Online maintenance model

Figure 2 shows an online maintenance model, in which medical device providers and SIs maintain the medical devices and systems installed in institutions over a network. During maintenance work, they can use actual healthcare information stored in the medical devices for device-status and problem-reproduction checks; furthermore, they can transfer this information over the network. Therefore, the network must allow each provider to connect to various medical institutions and allow each institution to connect to various providers. Moreover, the network must prevent connection to anyone other than contract-signers and must support switching of N-to-N connections at both the source and the destination. The network must also provide IP-level security. To satisfy such requirements, network devices for a dynamic on-demand VPN are installed in the medical institutions and in facilities providing remote services, and secure communication is performed via the Internet to provide remote maintenance. In this model, a policy related to protection of personal information must be exchanged in advance between the medical institutions and the maintenance vendor.

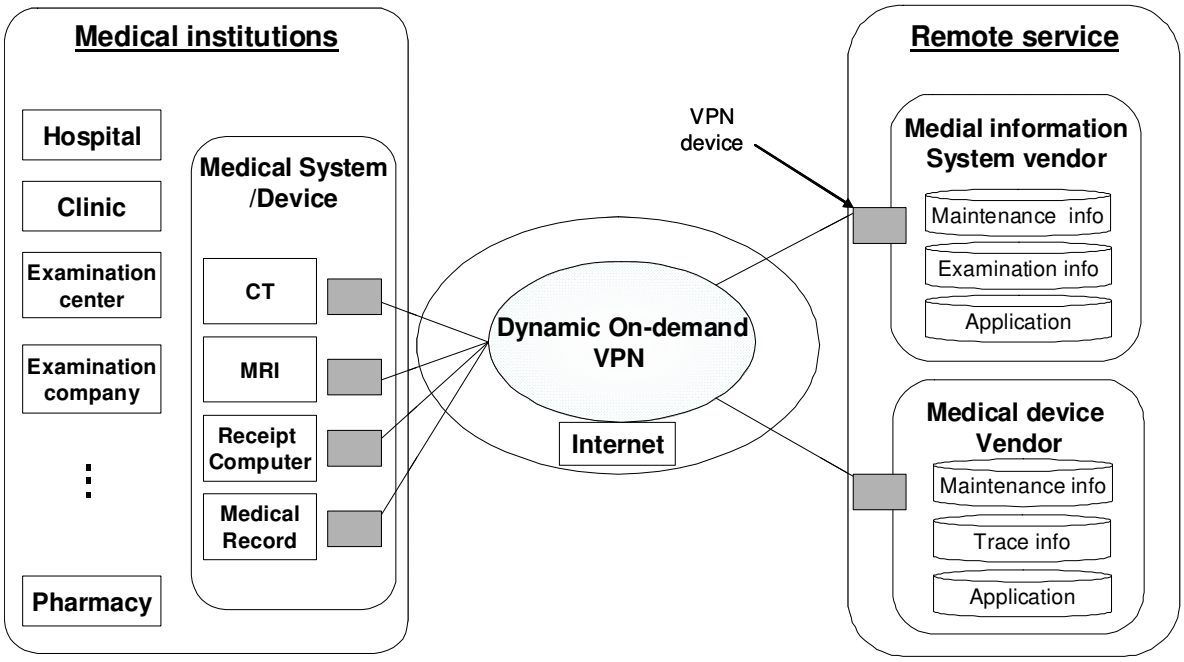

Figure 2 — Online maintenance model, using a dynamic on-demand VPN

9.3. Regional cooperation model with the lead taken by a regional core hospital

A secure network for regional healthcare cooperation can be implemented using a dynamic on-demand VPN, as shown in Figure 3. In this example, a regional core hospital and clinics cooperate with each other by sharing examination data, introducing patients according to their conditions, and providing and sharing necessary information. In the network, the purpose of the service is to provide functions such as creating patient referrals, making consultation appointments, sending secret e-mails including healthcare information, and sharing information. In the network, the regional core hospital and clinics are authenticated over the network connections by using IKE, before being connected through the VPN by using IPsec/AES so that threats to the network paths are eliminated. In the regional core hospital, the external network, which is an SZ, and the internal network, which is an HSZ, are separated from each other by a firewall for access control. The personal computers (PCs) at the clinics access the server in the SZ for external connection using the dynamic on-demand VPN. After introduction to medical institutions, this model can be characterized as follows:

— Making appointments is easier.

— Work for making appointments etc can be done irrespective of the opening hours of the core hospital.

© ISO 2008 – All rights reserved

— Since encryption is used, this model has the advantage of providing an excellent system in terms of security, with investment in only a single VPN device.

To exchange healthcare information for coordination with acute-phase hospitals for post-operation, long-recovery-type situations and coordination with chronic-phase hospitals, the network devices for a dynamic on-demand VPN are installed in the different facilities to provide secure communications.

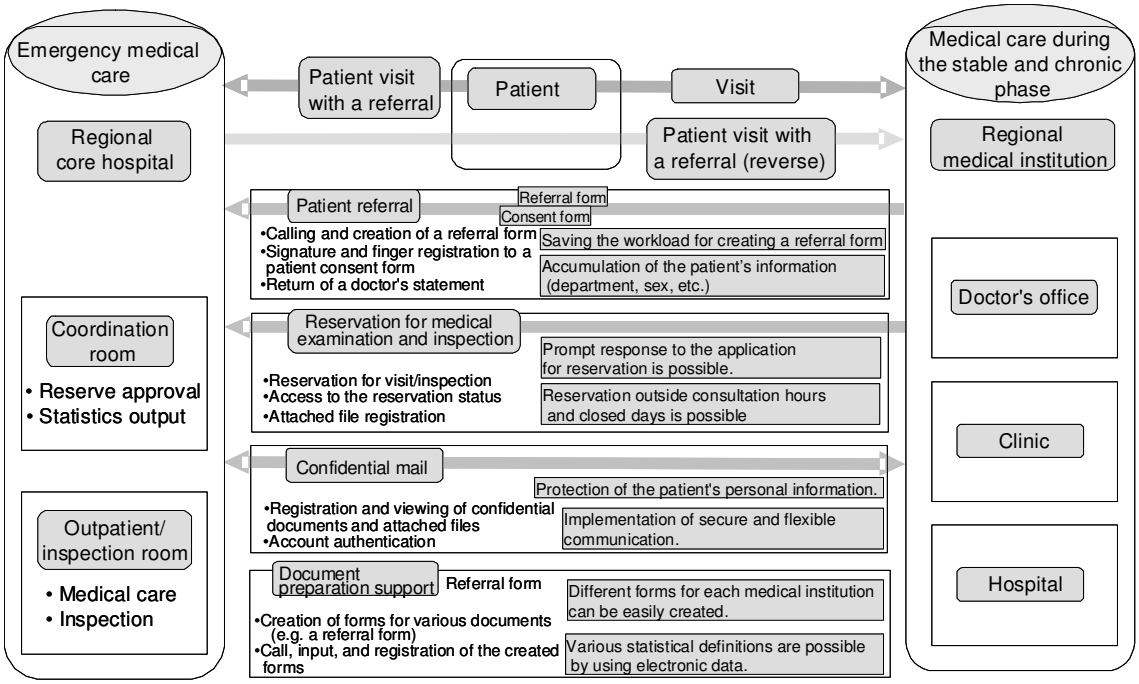

Figure 3 — Regional healthcare cooperation with the lead taken by a regional core hospital, using a dynamic on-demand VPN

9.4. Model for teleradiology, remote maintenance, and network conferencing with the cooperation of university hospitals, research institutions, and regional hospitals

Large volumes of data for diagnostic imaging are transmitted between medical institutions. Furthermore, actual healthcare information is transmitted over networks for remote maintenance of medical devices. Therefore, personal information can be transmitted over such networks, resulting in a threat of wiretapping. For this reason, a dynamic on-demand VPN can be applied with the purpose of enhancing security through medical device authentication and enabling multiple connections.

As shown in Figure 4, a remote maintenance network was built, with a university hospital, a research institution, and a medical device provider cooperating with each other to provide services such as diagnostic imaging, remote maintenance of medical devices, and network conferencing. This network includes a diagnostic imaging support network for teleradiology, which was built to connect the image servers of the university hospital and research institutions to universities, local hospitals, and regional core hospitals by using the dynamic on-demand VPN. The diagnostic imaging support network provides services such as transferring images for diagnosis, holding network conferences, and sharing pathology-related documents. It also provides services for remote maintenance of medical devices, such as computed tomography (CT) and magnetic resonance imaging (MRI) scanners, by connecting the equipment to the remote maintenance terminals of medical device providers via the VPN. Since this network uses L2TP tunneling for LAN connection inside the university, IKE/PKI authentication is applied to each session and established at the start

© ISO 2008 – All rights reserved

and end points of the tunnel, before the VPN connection is made using IPsec/AES. To verify the security with the external connection to the internal hospital LAN, the university configures the network in such a way that the internal network and the SZ for external connection are switched over properly with a physical change-over switch.

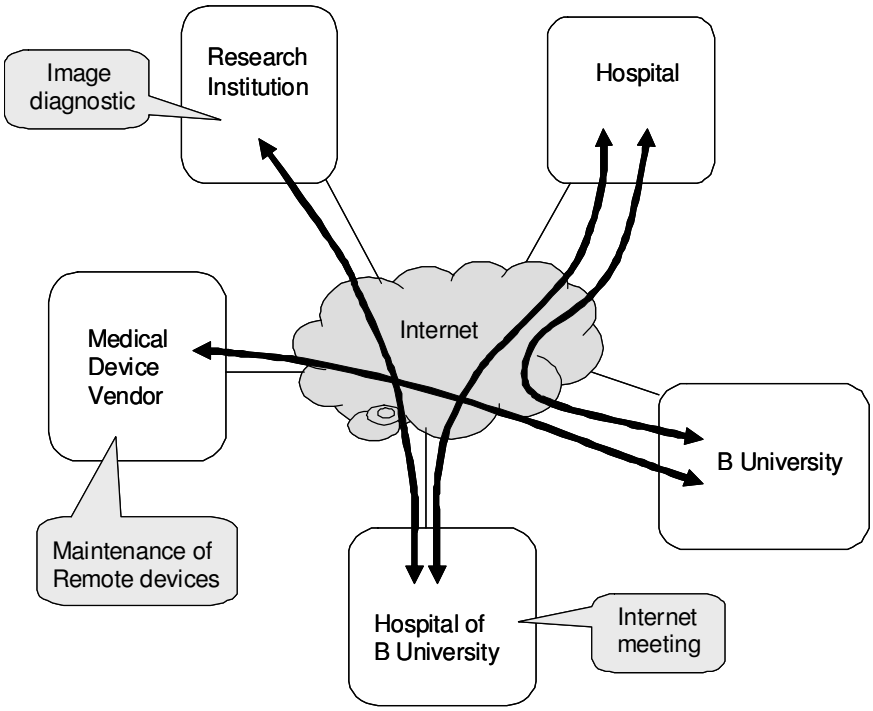

Figure 4 — Teleradiology, remote maintenance, and network conferences, using a dynamic on-demand VPN

9.5. University hospital model centered around teleradiology, telepathology, and network conferences conducted between a university hospital and regional hospitals

Figure 5 shows a model of a university with a network connecting hospitals to provide services such as transferring images for diagnosis, sharing pathology-related documents, and conducting network conferences. To overcome the insufficient number of pathologists, the university can build a pathological diagnosis network by using a dynamic on-demand VPN. This network connects the image server installed in the hospital and the pathology sample capture servers installed in the hospitals where pathological diagnosis doctors are sent within the same region. The network provides services such as telepathology sample capture, diagnosis image transfer, and sharing of network conference and pathology-related documents. The image server for the pathological diagnosis network is located in the university's SZ and linked to other pathology sample-capture servers located in the SZs of hospitals within the prefecture. In the university hospital and each regional hospital, access is controlled and viruses are checked through routers and firewalls when communication is made from a PC connected to the LAN inside a hospital to a host on the Internet in the SZ. For each of the paths -- a path within the LAN between the image server and connection routers, or a path on the Internet between the bases -- in the pathological diagnosis network, IKE/PKI authentication is applied to each session established before the VPN connection is made using IPsec/AES, so that threats to the paths can be eliminated from both inside and outside the hospitals. The communication logs of the network devices of the servers and the VPN devices of the bases can be stored in the administrative server for the dynamic on-demand VPN, once time synchronization has been established with the NTP (Network Time Protocol)

© ISO 2008 – All rights reserved

Server. Therefore, repudiation regarding access can be prevented, and traceability during system audits can be ensured. In addition, a secure channel of the dynamic on-demand VPN is used for remote diagnosis of radiological images and for network conferences via the Internet.

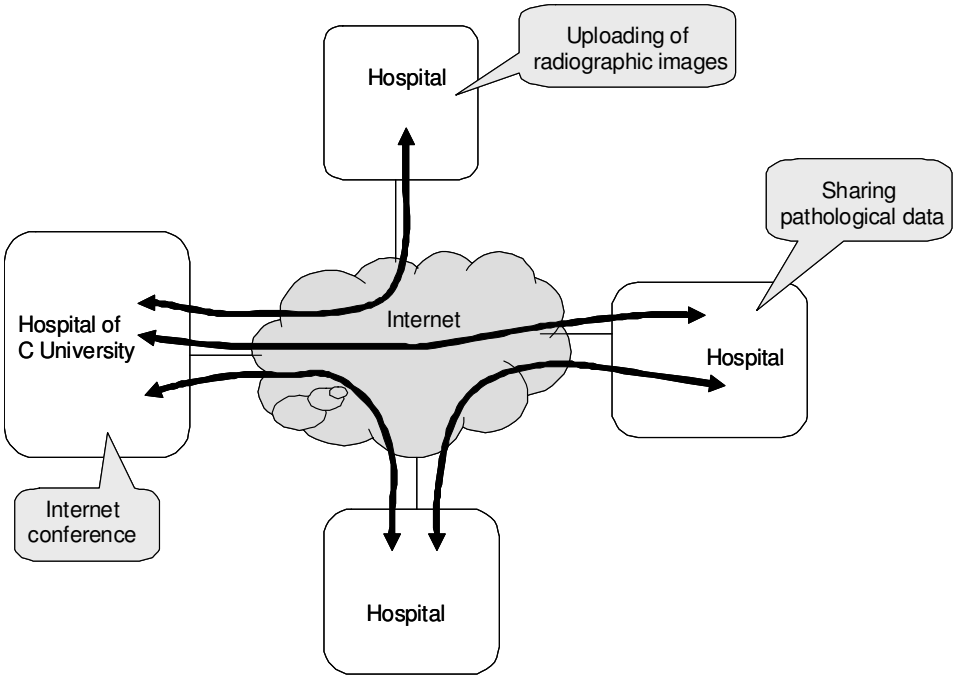

Figure 5 — Teleradiology, telepathology diagnosis, and network conferences, using a dynamic on-demand VPN

© ISO 2008 – All rights reserved

Annex A
(informative)

Threat analysis and measures

A.1 Extraction of network-related security requirements

To examine security requirements, they have been extracted in reference to guidelines and requirements issued so far and to RFCs related to security.

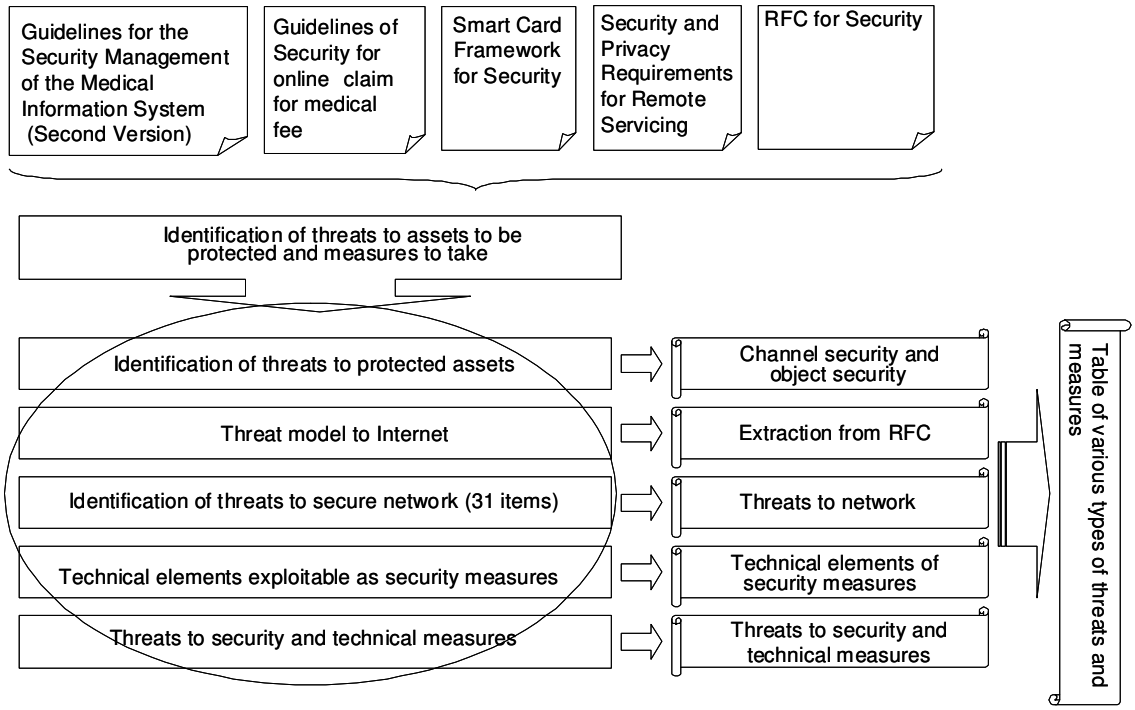

Figure A.1 — Threat analysis of network security

Among the related guidelines, portions of the "Guidelines for the Security Management of the Medical Information System" (second version) and "Guidelines for the Security of Online Claims for Medical Fees", from Japan's Ministry of Health, Labor and Welfare, are referred to for technical examination and described below. Also described is guideline "Security and Privacy Requirements for Remote Servicing", examined by NEMA/COCIR/JIRA Security and Privacy Committee (SPC) in order to comply with regulations related to privacy protection.

a) Guidelines for the Security Management of the Medical Information System, second version (refer to Annex B of this Technical Report)

   Technical information from the following sections of these Guidelines has been referenced:

   Section 6.9 Emergency measures for disasters

   Section 8 Standard for external storage of medical care history and medical care records

   Section 8.1 External storage on electronic media via network

© ISO 2008 – All rights reserved

Section 8.1.1 Observance of three standards for electronic storage

Section 8.1.2 Limitation of institutions entrusted with external storage

Section 8.1.3 Protection of personal information

Section 8.1.4 Specification of responsibilities

b) Guidelines for the Security of Online Claims for Medical Fees

Technical information from the following sections of these Guidelines has been referenced.

Section 5. Technical security: Necessity of filtering between networks

The following figure shows filtering between networks that are separated.

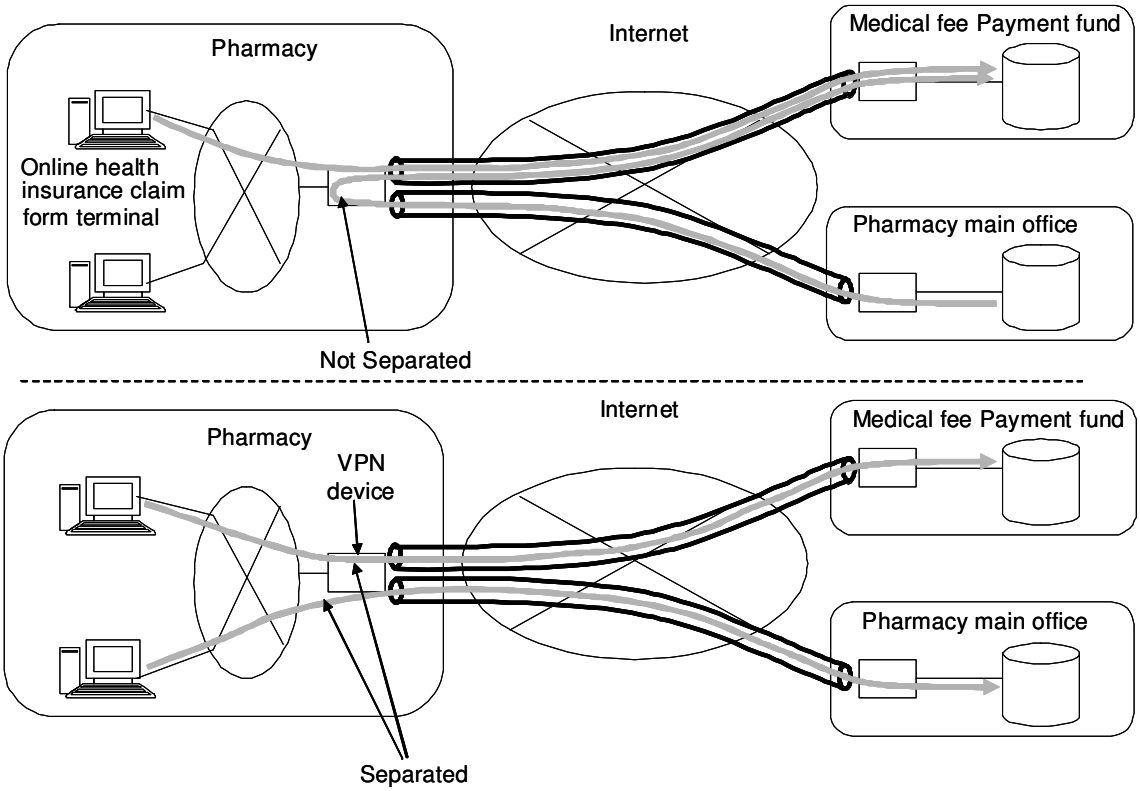

Figure A.2 — Necessity of filtering between networks

c) Security and Privacy Requirements for Remote Servicing

The guideline "Security and Privacy Requirements for Remote Servicing", examined by NEMA/COCIR/JIRA Security and Privacy Committee (SPC) in order to comply with regulations related to privacy protection, is described below as a reference for practices in foreign countries proceeding with the globalization of medical care and communication of insurance information.

— Only one access point shall be provided for the sites of medical institutions and medical-related institutions.

— Authentication is performed at a site's access point. While it is desirable to authenticate who has attempted access, it suffices to authenticate which institution is the source of communication if the association is made at the source.

© ISO 2008 – All rights reserved

— A medical institution must always monitor the access state and block illegal communication, if detected.

— Encryption is necessary to protect the privacy of communication. If possible, encryption using PKI is desirable. Communication logs, including information on who accessed the network, where, and when, must be recorded at three points: the source, the access point for the medical institution, and the accessed location. If necessary, matching between the three logs must be available for system audit.

— A medical institution must establish a security policy and require other medical institutions or medical-related institutions establishing access via a network to adhere to the security policy.

A.2 Channel security and object security as protected assets

RFC3552 defines the requirements for channel security and object security. These two sets of requirements complement each other to define the provision of security related to a single data object. Object security means security applied to the entire data object, while channel security provides a secure channel for transparently conveying objects.

Clear definition of the scope of examination across the entire network (terminal-network-terminal) leads to classification of network devices into “channel security” and “object security”. The following items must be examined as assets to be protected in the scope of examination.

Channel security between terminals ⇨ Transmit/Receive data

Object security of network device ⇨ Configuration file of network device and private key

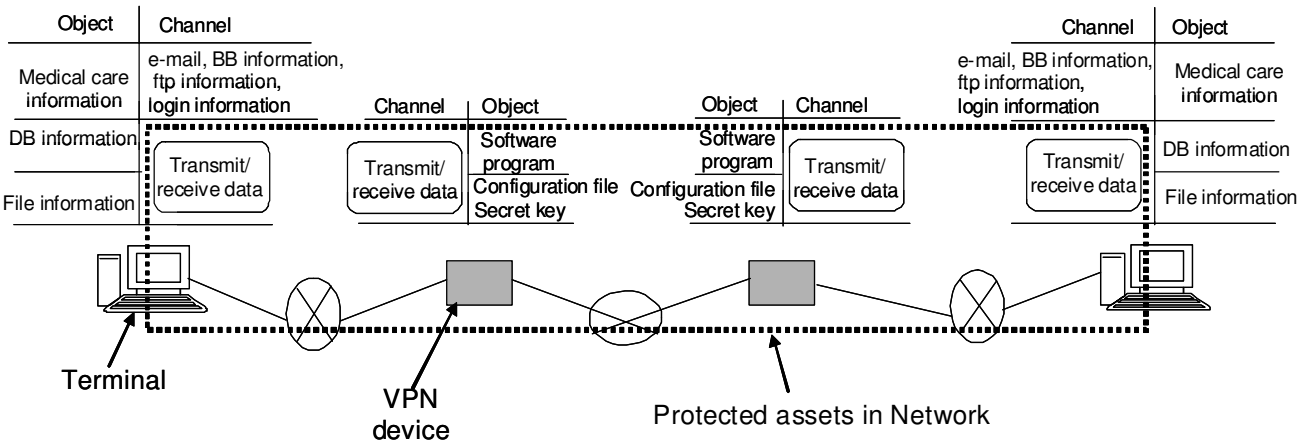

Figure A.3 — Channel security and object security

© ISO 2008 – All rights reserved

A.3 Component features related to object security of network devices

Table A.1 — Functional elements of set information for network devices

Major class	Minor class	Feature outline
VPN management features		
	Key exchange feature (IKE)	Automatically exchanges encryption keys used for VPN connection.
	Encryption feature (IPsec)	Encrypts data in order to provide confidentiality of communication data.
	Authentication feature (IPsec)	Authenticates the source of communication data.
	VPN control feature	Acquires from the connection management center the parameters necessary for VPN connection.
	VPN connection feature	Performs connection/disconnection requests for VPN connection or data transmission/reception.
	Initial registration feature	Registers initial information (device information with manufacturer's signature) in the secure storage area.
	Device information reference feature	Reads out device information stored in the secure storage area.
Key management features		
	Tamper resistance feature	Logically/Physically controls access to the storage area.
	Encryption processing feature	Encrypts/Decodes a key to be stored.
	AP management feature	Controls writing/deletion of AP or operation of downloaded AP of PKI chip.
	Storage area management feature	Performs access control of an area into which a key pair or certificate is to be stored.

A.4 Location of threats and problems

— About 80 percent of the threats related to information leakage from companies using LANs or WANs exist within the organization (on a LAN). Measures against threats to WANs using a closed network, ISDN, or IP-VPN are not sufficient as security measures on the communication path connecting terminals with each other.

— An open network performs encryption to mitigate threats to the WAN, through means such as Internet VPN (IPsec) and encrypted communication by SSL protocol or the LAN. Currently, the authenticity of a person or device cannot be assured, so there is a threat of attacks by crackers through "spoofing". Moreover, communication encrypted by the SSL protocol has vulnerability to attacks from the lower IP layer, which it cannot handle by itself.

— Internet VPN currently provides the most secure network environment by implementing an authentication environment in which spoofing is difficult, through use of the PKI technique and the like. By precluding spoofing, it is possible to provide secure communication between devices, by detecting hacking operations, including data tapping and tampering by another party, and by releasing the communication path while utilizing the features inherent to the protocol in use.

— In any system, it is impossible to prevent illegal operations from an authorized terminal. The user authentication feature must be reinforced by login authentication using a smart card for personal identification or by other methods.

© ISO 2008 – All rights reserved

A.5 Summary of threats to the network and security measures (channel security)

A.5.1 Definition of threats to the network

A total of 31 threats related to the Internet have been identified in reference to security-related RFCs, as listed below.

— Plain text transmission

— Shared password

— Dictionary attack

— Guess attack

— Network Information Service (NIS)

— Existence of cryptanalytic tools

— Topology destruction

— Determination of being on the same link

— Attack using regular protocol

— Internal threat

— Illegal copying of information

— Session hijacking

— ARP spoofing (IP address spoofing)

— Access certification

— TCP SYN packet insertion

— TLS RST impersonation

— Sequence number guess attack

— Unused Media Access Control (MAC) check

— Host-to-host SA

— Transfer after virus contamination

— Information destruction/overwriting

— Retransmission after message tapping

— Retransmission through auto-dialling

— TCP SYN flood attack

— Denial of service (DoS)

© ISO 2008 – All rights reserved

— Disaster/physical destruction

— Illegal usage

— Inappropriate usage

— Spoofing

— Illegal processing due to service interruption

— Tampering

— Negligence/theft/loss

A.5.2 Examination of measures against threats

The technical elements available in measures against channel security have been identified as follows, in association with the threats outlined in RFCs.

Table A.2 — Security-related RFCs indicating direct measures against network threats

Definition of threat	Security-related RFC indicating direct measure
Passive attack <RFC1704>	RFC2406
	RFC3552
Active attack <RFC1704>	RFC2406
	RFC2828
Replay attack <RFC1704>	RFC3631
	RFC4107
Topology destruction <RFC3552>	RFC2196
Determination of being on the same link<RFC3552>	RFC3552
Non-repudiation <RFC3552>	RFC3227
Denial of service attack <RFC3552>	RFC2827

In these RFCs, threat models are assumed based on threats to the network or protected assets. Guidelines and reference documents such as RFCs related to security are referenced to examine various security measures and evaluate their effectiveness. Currently, the following measure models are considered effective as channel security measures combining available technical elements.

© ISO 2008 – All rights reserved

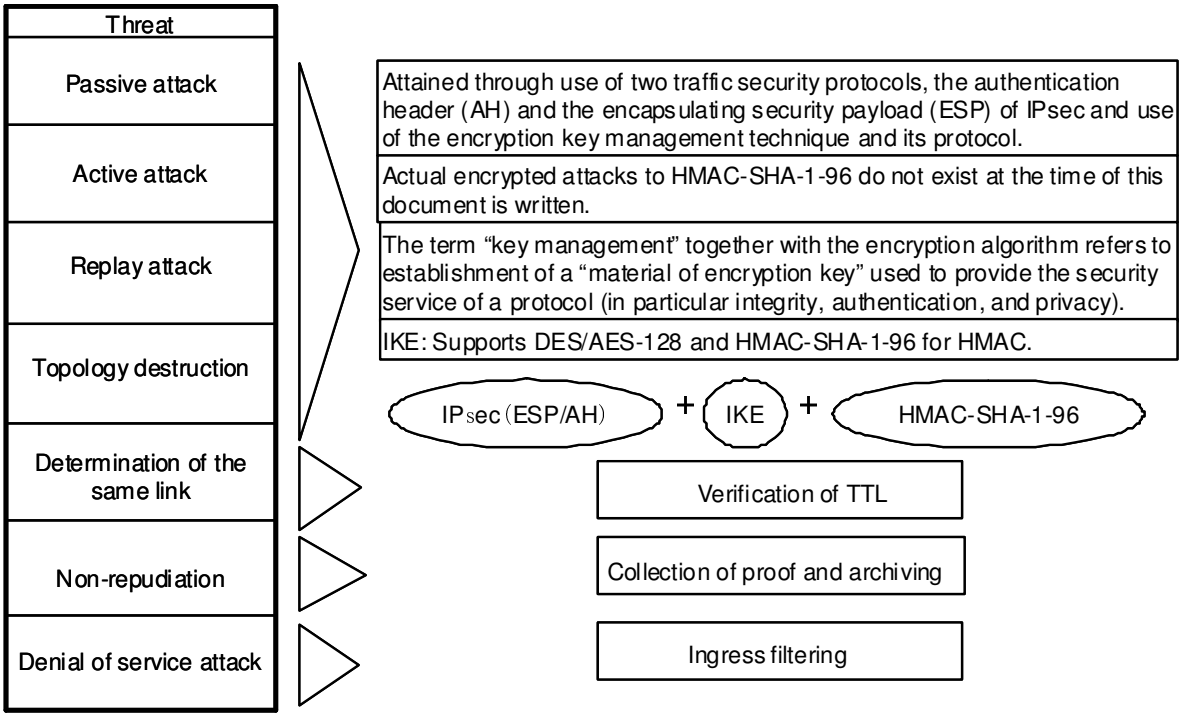

Figure A.4 — Threat model assuming specific attack methods

Bibliography

Annex B Section 6.10 of "Guidelines for the Security Management of the Medical Information System" (second version), issued by Japan's Ministry of Health, Labor and Welfare of Japan, March 2007 (informative)

© ISO 2008 – All rights reserved

Annex B
(informative)

Security management of medical information exchange including personal data between independent institutions

B.1 Basic concepts

This section describes some important concepts to remember regarding personal information protection and network security when medical institutions share information with other institutions. A possible situation of such information sharing is medical record exchange via computer networks with local medical institutions, pharmacies, and examination centers as part of regional healthcare cooperation. Other situations include online claims for medical fee bills to a medical fee payment fund and online access to ASP-type services.

If medical institutions use external networks to exchange healthcare information with other institutions, the intended data must be sent to the intended organization in a secure way that never allows the others to have access. This network security must be guaranteed on the communication path from the sender's device to the recipient's device. Transmitted data must be protected from threats like wiretapping, tampering, network intrusion, and interference.

Note that this Guideline does not cover all possible situations but assumes only some of them, focusing on the network connection methods used for healthcare information exchange. Also, note that protection of personal information during network-based data exchange will be discussed separately from network security, because they should be considered from different viewpoints.

If medical institutions subcontract storage of personal and other healthcare information, special attention must be paid to information protection against improper secondary use or other risks, whether mandatory by law. This topic will be detailed in chapter 8.

B.2 Clear demarcation of responsibility

According to Japan's Act on Personal Information Protection, there are two types of healthcare information provision to other institutions: subcontracting, and provision to third parties. Different regulations must be followed in each situation.

In the case of subcontracting, the information source (medical institution) assumes managerial responsibility. It must create a contract and supervise the subcontractor, ensure accountability, and take responsibility for consequences. The subcontracted organization is responsible for abiding by the contract and reporting on its operation.

In the case of provision to third parties, with a few exceptions stipulated in Article 23 of the Act on Personal Information Protection, the information provider must obtain implied or express consent from the people in question. If the provision fits one of the descriptions from (a) through (d) of III-5-(3)-1) in the "Guidelines for Personal Information Management by Medical Treatment and Nursing Care Organizations," implied consent is sufficient, as stipulated in these guidelines. Otherwise, express consent is necessary. The information provider is also responsible for identifying its intended purpose, as stipulated in Articles 15 and 16 of the above-mentioned act, and for ensuring personal information protection in accordance with the above-mentioned guidelines and act. The information provider is not responsible for the information provided in accordance with these requirements.

When delivered online, patient information leaves the control of the patients themselves. So, at least one of the involved organizations must be responsible for the delivery, and where the responsibility lies must be clear and beyond misapprehension. Patients must be informed of the organization against which they can make a complaint and from which they can request an explanation.

© ISO 2008 – All rights reserved

Involved organizations can include the information sender (medical institution), the OSP, the telecommunication carrier, the recipient, and possible secondary recipients. The demarcation points of responsibility must be defined based on the following principles.

By contract, the sender and recipient must agree on demarcation points of responsibility for data transmission on the communication path, such as handling of communication failures and other accidents. Then, they must decide how to share managerial responsibility among themselves, the OSP, and the telecommunication carrier and define the demarcation points accordingly. They must clarify the scope of managerial responsibility to be assigned to another organization and specify which organization should take the initiative in dealing with possible service failure. As described above, however, accountability and responsibility for the consequences lie with the sender in the case of subcontracting and with the sender or recipient in the case of provision to third parties. Note that the OSP and the telecommunication carrier accept only part of the managerial responsibility.

The telecommunication carrier is not responsible for protecting personal information against wiretapping: as long as transmitted data is encrypted in a suitable manner by the sender and decrypted by the recipient, both functions are outside the carrier's scope of managerial responsibility. The carrier must clarify by contract the scope of its managerial responsibility for threats like tampering, intrusion, and interference, and for the communication quality that it guarantees, such as line availability.

The OSP is not responsible for protecting personal information against wiretapping: as long as transmitted data is encrypted in a suitable manner by the sender and decrypted by the recipient, both functions are outside the OSP's scope of managerial responsibility. The OSP must clarify by contract the scope of its managerial responsibility for threats like tampering, intrusion, and interference, and for the communication quality that it guarantees, such as service availability.

In statutory or other special cases, unencrypted healthcare information might be sent to an OSP or a network provider. To take necessary measures against wiretapping during online service provision and on the communication line, the medical institution with managerial responsibility for the information on the communication path must negotiate with the OSP or the network provider to agree upon each party's managerial responsibility for the information. If all or part of the managerial responsibility is assigned to the OSP or network provider, the information source must establish a suitable contract with each of the involved parties and oversee the subcontracted work.

If a medical institution transmits data to a single organization or to multiple organizations specified in advance, the sender and recipient(s) must fulfill their obligations in accordance with the requirements for subcontracting or provision to third parties.

If a medical institution transmits data to multiple organizations and there is a possibility that someone not specified in advance will receive the data, healthcare information must not be transmitted in principle, except as stipulated by law or with some other exceptions.

Typical applications of data access by remote login include remote system maintenance. Such remote maintenance is convenient, but loosely restricted access can lead to unauthorized reading or tampering of personal or other healthcare information temporarily stored on a computer disk.

Total prohibition of remote login, however, makes remote maintenance impossible, resulting in higher costs and longer time of maintenance. Remote login should thus be enabled only when it is appropriately controlled.

B.3 Precautionary measures taken within a medical institution

Regarding the responsibilities listed in section B.2 "Clear demarcation of responsibility", this section describes the precautionary measures a medical institution should take within its own organization when sending medical records or other healthcare information via networks.

The most important concept to remember is that a medical institution sending healthcare information has managerial responsibility for the information during the whole process in which data is transmitted via networks (provided by the carrier) and then received by the intended recipient in an appropriate manner.

© ISO 2008 – All rights reserved

To avoid misunderstanding, note here that managerial responsibility means responsibility for the information in electronic form: in other words, responsibility for ensuring the authenticity of both the content and the persons referred to. The necessary actions differ from the situations described later in section B.4, "Concepts of appropriate network security". For example, encryption in this section means encrypting healthcare information to prevent outsiders from viewing data even if they have wiretapped the communication path. Digital signatures are helpful for tampering detection. In contrast, encryption as described in section B.4 means encrypting the communication path to prevent information theft during transmission.

From these viewpoints, medical institutions that are going to transmit data are responsible for suitably protecting the data and must be aware of the following.

a) Protection against wiretapping

Wiretapping is one of the most important threats to be dealt with in sending data via networks. Stealing information is a criminal activity, which can be done in various situations, such as by building a virtual bypass on the communication path or attaching a physical device to a networking device. There might be cases in which the fault cannot be directly attributed to the medical institution. Failure to appropriately configure networking devices can cause unintended data leaks or transmission to incorrect recipients, and the sender might be responsible.

Taking such risks into consideration, medical institutions must take appropriate actions to protect healthcare information even if it is stolen on the communication path, accidentally leaked out, or transmitted to a wrong recipient. One possible action is encryption of healthcare information. As explained above, encryption here means encrypting the information itself.

A guideline cannot simply specify when and to what extent information should be encrypted. That depends on how sensitive the information is and how the medical institution's information system is operated. At minimum, it is preferable to encrypt data before it is sent from the sender's networking device.

These measures against wiretapping should also be taken during system maintenance tasks through ID- and password-based remote login. The medical institution that owns the computer system is responsible for informing the maintenance company of the above-mentioned considerations and supervising the maintenance tasks.

b) Protection against tampering

When sending information over networks, the sender should also ensure that it is transmitted “as is” to the recipient. Though data encryption reduces the risk of tampering, transmitted data could still be tampered with because of a failure on the communication path or other possible causes, whether intended or not.

Depending on the networking configuration, as described later in section B.4, data might be transmitted without encryption. In this case, the sender must take precautions against tampering. One tampering detection method is the use of electronic signatures.

c) Protection against spoofing

When sending information over networks, medical institutions must ensure that the recipient is correct. When receiving information over networks, medical institutions must confirm the identity of both the sender and the transmitted data. This is because networking is not a face-to-face communication method.

One way to identify the recipient/sender at the start/end point of communication is mutual authentication by using proven authentication systems, such as public-key and symmetric-key cryptography, at the entry into and exit from the network. The use of digital signatures for tampering prevention is also helpful in identifying the sender.

© ISO 2008 – All rights reserved

For counteractions against cyber attacks that pose such risks, refer to section 6.9, "Emergency measures for disasters", in the Guideline.

B.4 Concepts of appropriate network security

B.4.1 Overview

When considering network security for healthcare information exchange with other institutions via networks, medical institutions must define demarcation points of responsibility and then identify important considerations from a viewpoint different from that expressed in section B.3, "Precautionary measures taken within a medical institution", which referred to measures taken within the organization. This section focuses on the outside world: networks connecting the sender's external network connection point to the recipient's. Note that LANs within medical institutions are not taken into account. As stated in section B.2, "Clear demarcation of responsibility", medical institutions are responsible for being aware of the risk of unintended data leaks due to inappropriate network configuration or communication path design, and for taking necessary measures against this risk.

To configure networks for exchanging healthcare information with other institutions, medical institutions should first identify the confidentiality of the information to be exchanged. From the same viewpoint as for data encryption described in section B.3, the network type must be selected according to the confidentiality of the data. High-level network security is basically essential to healthcare information exchange, but excessive security measures for not-so-sensitive data result in unnecessarily high costs and impractical operation. Networks with appropriate costs and operation must be selected through analysis of information security. Then, who should be responsible for network security must be defined by contract: the telecommunication carrier, the medical institution, or both. There are roughly two cases: network security is guaranteed by the telecommunication carrier and the OSP, or it is not guaranteed by these businesses.

a) Guarantee of secure network path provided by the telecommunication carrier and OSP

Among the network services offered by telecommunication carriers and OSPs, there is a form of network connection whose security is guaranteed by these businesses, mostly in the form of a closed network connection (described later). Even in the form of an open network connection, there exist network services in which telecommunication carriers provide an encrypted communication path, like Internet VPN service. With this type of network, a medical institution can delegate a large portion of its managerial responsibility to these businesses, though it assumes responsibility for the final consequences of security on the communication path. As a matter of course, a medical institution must exercise due care and ensure security management of its in-house system according to organizational, physical, technical, and human security management rules.

b) No guarantee of secure network path provided by the telecommunication carrier and OSP

As an example, there might be a case in which two medical institutions install network devices to communicate with each other via the Internet, based on a mutual agreement. In this case, the telecommunication carrier and the OSP do not take responsibility for network security. Therefore, besides the above-mentioned security management, these medical institutions must appropriately manage their network devices and encrypt the communication path. All possible measures should be taken to prevent personnel without sufficient knowledge of networking from setting up a network.

Otherwise, healthcare information will be exposed to threats. For this purpose, medical institutions must develop measures to identify the sender's and recipient's network devices, the data transmission terminals installed in the medical institution, the features of these terminals, and their users. Medical institutions must also consider signing contracts for information handling with each other, assigning exclusive staff members, and developing operational management rules in anticipation of threats. These rules should be stricter than those a telecommunication carrier would develop to guarantee security on the network path.

As stated above, medical institutions planning to exchange healthcare information via networks should select an appropriate type of network, by considering how responsibilities should be shared according to the form of services that the institutions use. They should also understand the characteristics of the security technologies

© ISO 2008 – All rights reserved

that they use, identify allowable risks, and, if necessary, explain the risks to their patients to fulfill their accountability.

From among a wide variety of network services, the following sub-sections assume several cases and list some key concepts to remember.

B.4.2 Communication via closed networks

A "closed network" here means a dedicated network for business use and is defined as a network not connected to the Internet. There are three connection forms that offer closed networks: a telecommunication carrier leased line, a public network, and a closed IP communication network.

Since these networks are not connected to the Internet, they are basically at lower risk of wiretapping, intrusion, tampering, and interference. The risk of wiretapping by a physical method (described in section B.3) cannot be eliminated, and it might be necessary to encrypt the information to be transmitted. Moreover, the antivirus software's virus definition files and the operating system's security patches should be applied on a timely basis to maintain secure computer systems.

The following subsections describe the different features of the three forms of closed network.

a) Connection over a telecommunication carrier leased line

This is an always-on network connection used only for subscribing machines between two points with constant network quality. Because the network quality and transmission speed, or bandwidth, are guaranteed by the telecommunication carrier, this form of connection is used for constantly connecting two sites and sending large amounts of data and large files.

While the network quality is good, the extensibility is low and the cost is generally high. Still, it is worthwhile to implement this line if a large amount of significant data needs to be constantly transmitted.

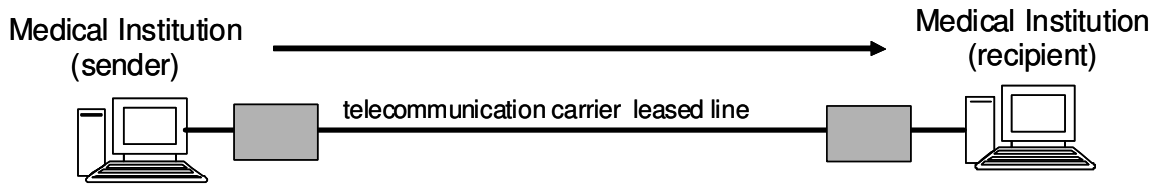

Figure B.1 — Connection over a telecommunication carrier leased line

b) Connection over a public network

This is a form of connection that uses a public network via switches, and it includes ISDN and dial-up connections.

Note that connection over a public network here means direct connection to the recipient's phone number, not to the Internet service provider (ISP). The latter should meet the requirements described later in section B.4.3, “Communication via open networks", because the data enter the Internet at the ISP.

This public network system dials directly to the recipient's phone number to establish network connection. A mechanism to confirm the phone number before network connection establishment ensures communication with the recipient.

Omitting this mechanism can result in connection and data transmission to an incorrect number. As with a telecommunication carrier leased line, this public network system has poor extensibility. The transmission speed is lower than that of currently popular broadband connections. This system is not suitable for sending large amounts of data or large files such as those containing image data.

© ISO 2008 – All rights reserved

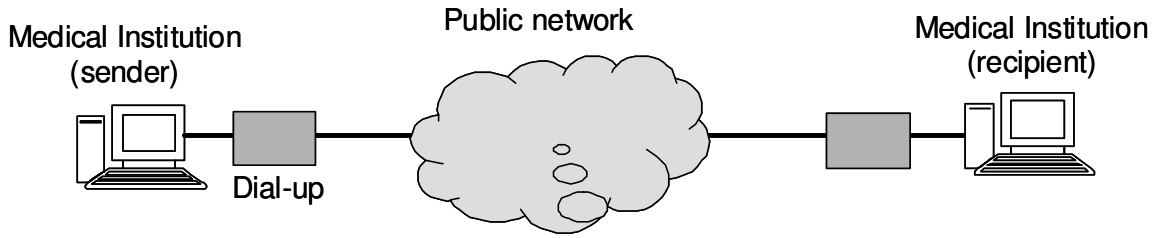

Figure B.2 — Connection over a public network

c) Connection over a closed IP communication network

This connection uses a communication line that connects a telecommunications carrier's WAN to a user's (i.e., a medical institution's) network device. This line is shared with no other network services. The Guidelines refer to this connection service as IP-VPN and define it as a closed network. Other forms of connection are considered as open network connections. IP-VPN is mainly used as a kind of corporate LAN to share information between a company's headquarters and its branch offices in remote locations, and generally, a single entity is responsible for its operation.

This form of connection can be implemented at lower cost than connection over a telecommunication carrier leased line. Appropriate selection of the subscription type and network service can be sufficient to transmit large amounts of data and large files.

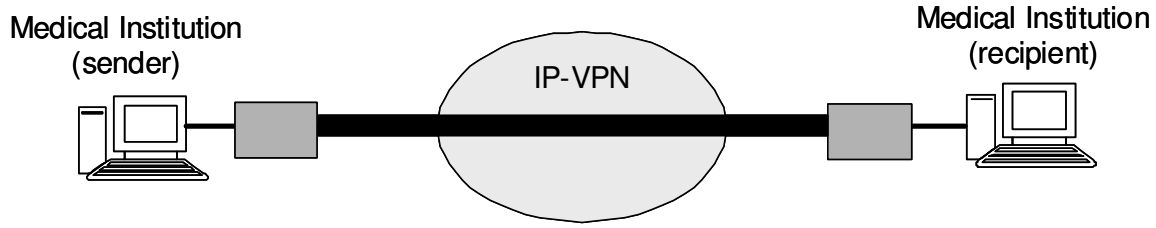

Figure B.3 — Closed network provided by a telecommunication carrier

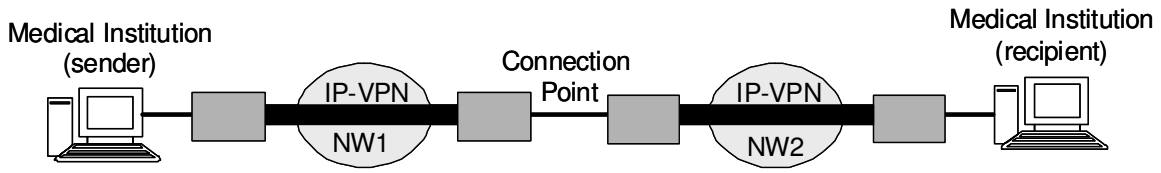

Figure B.4 — Interconnected closed networks

These three forms of communication via closed networks have no risk of intrusion from outsiders, and in that sense, they are safe. Connection services, however, generally do not offer encryption of data to be transmitted. There might be a case in which different networks offered by different telecommunication carriers are interconnected via connection points. When networks are interconnected via connection points, sometimes the recipient's address is interpreted or additional data are added to the transmitted sender information.

This might cause accidental data leaks. The Telecommunication Business Law prohibits further spread of the leaked data, but accidental leaks should be avoided from the viewpoint of healthcare professionals' confidentiality obligation. Particular attention should be paid to the necessary level of security management,

© ISO 2008 – All rights reserved

because it generally changes at the demarcation points of responsibility, such as a connection point from a medical institution to a closed IP communication network.

For these reasons, even with a closed network, medical institutions should take security measures, such as encryption of healthcare information to make the information hard to access and introduction of a tampering detection system, as described in section B.3.

B.4.3 Communication via open networks

This is a form of connection using the Internet. Considering the wide spread of broadband network environments, its applications are likely to expand, thus enabling, for example, reduced implementation costs by using open networks or building an extensive mechanism of cooperation for regional healthcare. Since there are various threats on the communication path, such as wiretapping, intrusion, tampering, and interference, sufficient security measures must be taken. Encryption of healthcare information is also necessary.

Note that, as stated in section B.4.1, even with an open network connection, telecommunication carriers and OSPs might provide their services by guaranteeing secure network paths as security measures against threats. Medical institutions that use such services can transfer most of their responsibility for communication path management to those businesses by defining demarcation points of responsibility by contract.

If medical institutions use their own open networks to exchange personal information and other healthcare information with other institutions, most of the managerial responsibility falls on the medical institutions themselves. Therefore, they must take full responsibility for implementing such networks and be aware of their responsibility for guaranteeing technical safety.

With an open network connection, the necessary level of security on the network path depends on the layer at which security is guaranteed, among the seven layers of the OSI hierarchical model[2]. For network path security based on the OSI model, refer to "A Case Study Report on ‘Guidelines for the Security Management of the Healthcare Information System’", published by HEASNET in February, 2007.

Table B.1 — OSI model:

Layer 7	Application	Provides FTP, e-mail, and other services
Layer 6	Presentation	Converts data into a human-readable form suitable for communication
Layer 5	Session	Related to establishment and release of a data path
Layer 4	Transport	Stipulated for secure data transmission
Layer 3	Network	Provides address control and path selection
Layer 2	Data link	Stipulated for establishment of a physical communication path
Layer 1	Physical	Converts bit data electrically and physically and specifies device shapes and characteristics

For example, with encrypted communication by the SSL protocol, the communication path is encrypted at the fifth layer, called the Session Layer, and during the process there is a risk of wiretapping and inappropriate path building. With IPsec, the communication path is encrypted at the third layer, called the Network Layer, or

[2] The OSI hierarchical model is an international standard protocol for communication between heterogeneous systems.

© ISO 2008 – All rights reserved

at lower layers. The risk of wiretapping is lower than with encrypted communication by the SSL protocol, but still, a standard process of IKE should be combined with encryption key exchange for path encryption to ensure safety.

As described above, medical institutions that are planning to use open network connections should carefully review different security technologies and their inherent risks to ensure that the possible risks are acceptable. If medical institutions subcontract network implementation, as is often the case, they should request an explanation of such risks and understand them.

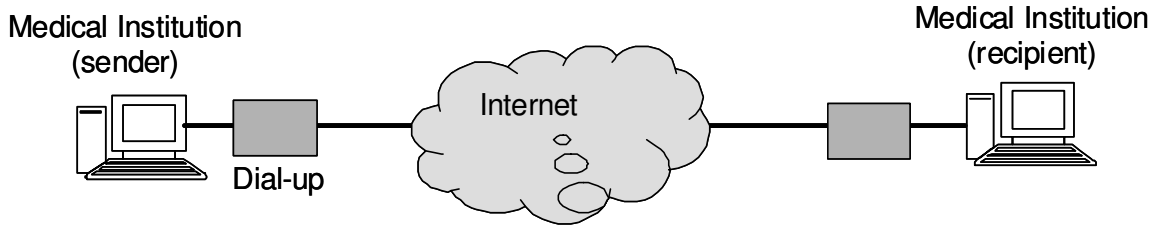

Figure B.5 — Communication via open networks

B.4.4 Provision of medical records to patients

As disclosure of medical records is becoming more and more popular, some medical institutions will perhaps give their patients (or their family members) online or onsite access to their own medical records. This is very likely to occur, though these Guidelines mainly assume information exchange between medical institutions. The following paragraphs describe the basic ideas of direct provision of medical records to patients. Note that we do not discuss the provision of medical and treatment records stored by other organizations (refer to Chapter 8 of the Guideline) here. These records are given to the patients by the subcontracted organizations.

The most important thing to remember when providing patients with medical records via networks is that different patients have different knowledge levels and different network security environments. Once information is revealed to patients, they are also responsible for handling it. Considering the patients' knowledge of network security, medical institutions must give sufficient explanation of the purpose of online information provision and the possible risks, until patients fully understand these concepts. Medical institutions must also be aware that they cannot avoid their responsibility if data leaks occur without much prior explanation.

Connection via closed networks, such as over a telecommunication carrier leased line, is not suitable for communication with patients, because installation of network systems in patients' houses is not realistic. Open networks should be used instead, but the risk of wiretapping is extremely high and it is very difficult for medical institutions to tell their patients how to avoid such risk.

Considering both usability and protection against threats, medical institutions must take security measures based on the considerations described in sections B.2 and B.3. In particular, computer systems and applications that are used to give healthcare information to patients must be separated from other systems and applications owned by the medical institutions, in order to avoid unauthorized intrusion into them. Such technologies as firewalls, access monitoring, encrypted communication by SSL, and PKI-based personal authentication are necessary.

As just described, medical institutions that are planning to provide patients with information must take comprehensive action-security management of not only networks but also their internal information systems, give convincing explanations of possible risks and provision purposes to patients, and account for various legal bases. Before implementation, they must also clarify who is responsible for each activity, and to what extent.

© ISO 2008 – All rights reserved

B.5 Minimum guidelines

a) Protection against tampering, such as message insertion and virus injection into the network path. Protection against wiretapping by crackers who try to steal passwords or message texts on the path between institutions. Protection against spoofing, such as session hijacking and IP address spoofing. A possible way to obtain such protections is to use IPsec and IKE to ensure communication path security.

b) Authentication of the sender/recipient at the gateways of their institutions, at their networking devices, at the functional units of these devices, and at other units that the user wants to use. Authentication methods must be selected according to the communication system and operation rules. Secure methods are recommended, such as PKI-based authentication, key distribution like Kerberos authentication, and use of a pre-shared key or one-time password.

c) Protection against spoofing as authorized users or devices in the institution. For information on spoofing, refer to section 6.5, "Technical safety measures", of this Guideline.

d) Routers and other network devices must be confirmed safe, and routing must be properly configured, so that routers cannot be used for communication with different facilities via a VPN. Devices that are confirmed safe meet, for example, ISO15408's security targets or the requirements of other, similar documents stipulating that the security measures of the devices are confirmed to be in conformance to this Guideline.

e) Security measures, including encryption of data to be transmitted, must be taken by both the sender and the recipient. Possible options are SSL/TLS, S/MIME, and file encryption. Encryption keys must conform to the e-government recommended cipher list.

f) Many other organizations are involved in telecommunication between medical institutions: telecommunication carriers, SIs, system operation companies, device maintenance companies that offer remote maintenance services, and others. The following responsibilities must be assigned to relevant organizations, and demarcation points of responsibility among these organizations must be clarified by contract:

— Decision on the timing of sending healthcare information including medical records and on the action of starting a series of information exchange operations.

— Handling of the sender's failure in connecting to a network.

— Handling of the recipient's failure in connecting to a network.

— Handling of connection failure or considerable communication delay in the middle of the network path.

— Handling of the recipient's failure in recognizing the information that it receives.

— Handling of failure in encrypting transmission data.

— Handling of failure in authenticating the sender or the recipient.

— Isolation of a failed part in the case of failure.

— Handling of the sender's/recipient's termination of information exchange. Medical institutions must stipulate the following by contract or through operational management rules:

— Clarification of responsibility for managing communication, encryption, and authentication devices. If such management is subcontracted, the demarcation points of responsibility must be defined and a contract must be signed.

© ISO 2008 – All rights reserved

— Clarification of accountability to patients.

— Designation of an exclusive manager who is responsible for fault restoration and coordination with other facilities and vendors.

— Clarification of responsibility for the consequences to the other party of information exchange. Notification of patients' inquiries about personal information handling to both the sender and the recipient of the information, and confidential matters regarding such personal information handling.

g) Prevention of unnecessary login during remote maintenance by setting appropriate access points, limiting the protocols to be used, and controlling access privileges, if necessary. For maintenance activities, refer to section 6.8, "Adaptation and maintenance of the information system", of the Guideline.

h) When signing a contract with a telecommunication carrier or an OSP, institutions must make sure that there is nothing wrong with the scope of managerial responsibility for threats and telecommunication quality, including line availability, and that the above minimum guidelines 1 and 4 are followed.

© ISO 2008 – All rights reserved

Annex C
(informative)

Technical and Operational Checklists for the Guideline

C.1 Introduction

These checklists cover all the requirements, specified in the "Guidelines for the Security Management of the Medical Information System" (second version), to be met by medical institutions when they deal with healthcare information. These checklists range from operational requirements to technical and system requirements. For ease of reference, the checklists classify medical institutions according to their functions. For medical institutions to observe the Guideline, SIs and SPs must provide services and carry out their functions in accordance with the Guideline. Therefore, a checklist comprises three kinds of sub-checklists—for managers of medical institutions, for SIs, and for SPs—with each item to be examined by the different providers of service functions.

First, stakeholders should identify the type of checklist their organization should use, according to the following definitions:

a) Large hospitals

In large hospitals, multiple staff members share personal and other sensitive information, including healthcare information and accounting data, through the LAN in the hospital. Large hospitals have facilities for users to exchange or provide information, some of which is exchanged with different institutions by using the network configuration shown in Figure C.1. This figure illustrates a network composition example for a large hospital.

b) Small hospitals

In small hospitals, multiple staff members share personal and other sensitive information, including healthcare information and accounting data, through the LAN in the hospital. Small hospitals utilize services provided by SPs, including Internet access, information exchange by e-mail, information provision, and external storage. Small hospitals exchange information with different institutions by using the network configuration shown in Figure C.2.

c) SPs

SPs have facilities for externally storing personal and other sensitive information generated in medical institutions, or for exchanging information with or giving information to other organizations. Such information is exchanged with medical institutions by using the network composition shown in Figure C.3. SPs also provide common services, including time stamps, Internet access, and content screening.

Table C.1 lists the differences among large hospitals, small hospitals, and SPs, with the corresponding checklists to be used.

© ISO 2008 – All rights reserved

Table C.1 — Major differences among the three types of organization

	Medical institutions		SP
	Large hospitals	Small hospitals	
Functions and facilities	Have equipment for providing information to differnet institutions	Do not have equipment for providing information to different institutions	Telecommunication carriers and OSPs
Example figure	Figure C.1	Figure C.2	Figure C.3
Corresponding checklist	Checklist for Large Hospitals	Checklist for Small Hospitals	Checklist for SPs

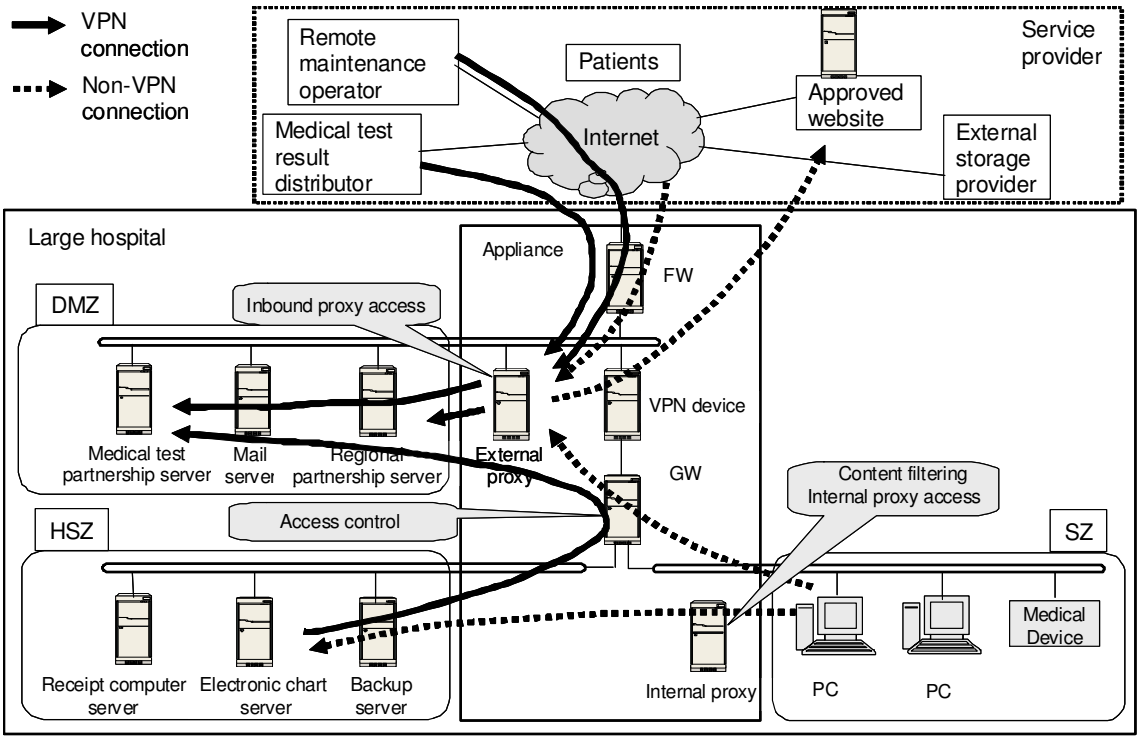

Figure C.1 — Network composition example for large hospitals

© ISO 2008 – All rights reserved

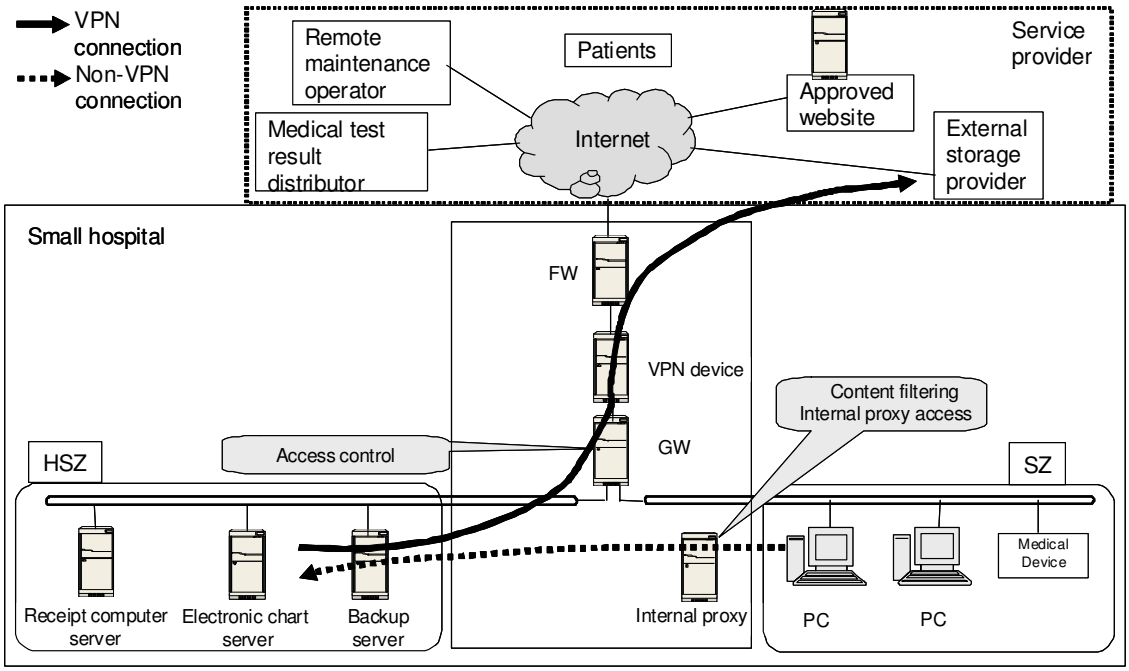

Figure C.2 — Network composition example for small hospitals

© ISO 2008 – All rights reserved

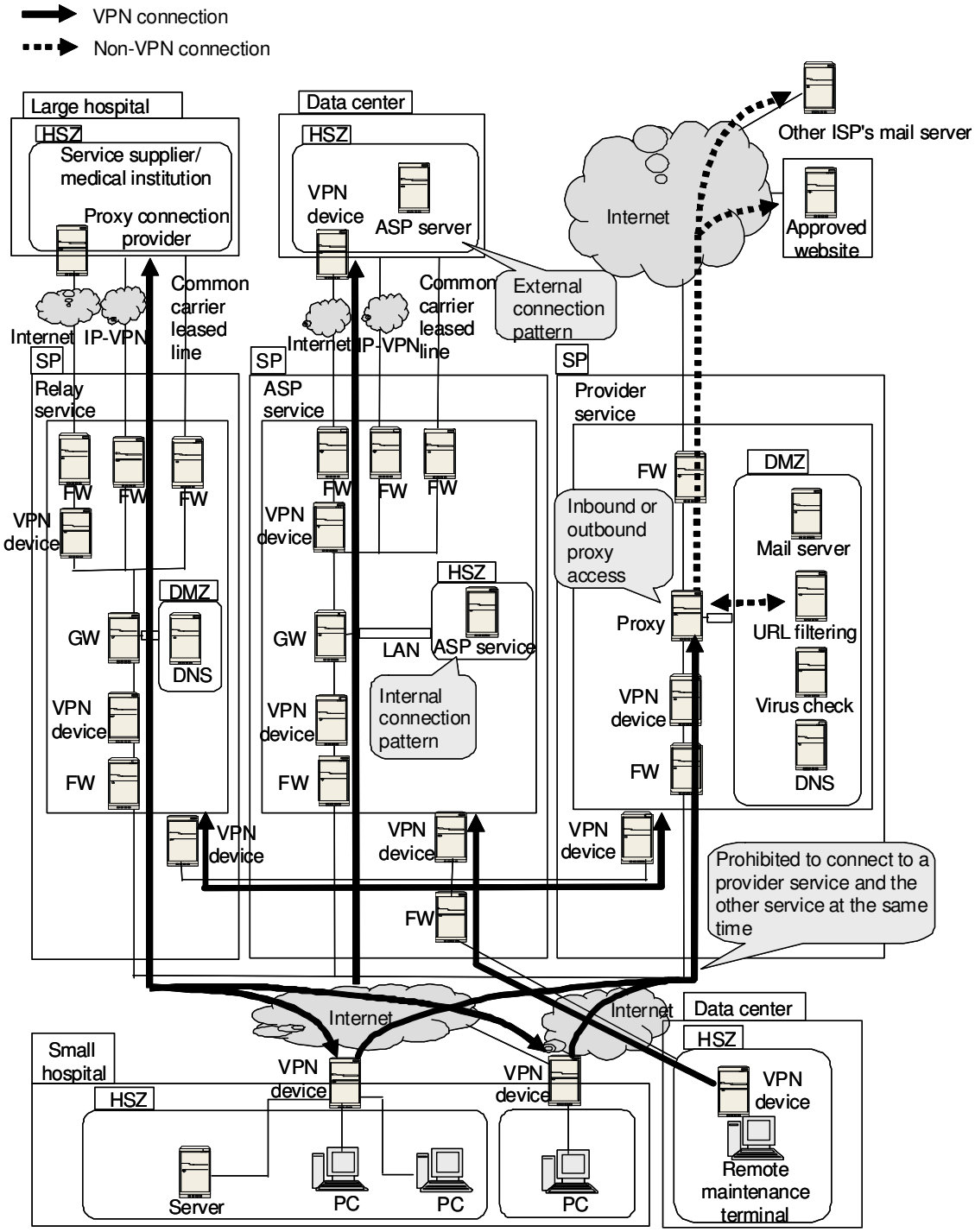

Figure C.3 — Network composition example for SPs

© ISO 2008 – All rights reserved

C.2 Instructions for the checklist for large hospitals

This checklist is intended for medical institutions having equipment for providing information to different institutions (i.e., medical institutions that can provide SP services to different institutions). Medical institutions that do not have such equipment should use the checklist for small hospitals instead.

(1) Checklist components

The checklist for large hospitals consists of three sub-checklists for three different organization types: the sub-checklist for medical institutions, the sub-checklist for SIs, and the sub-checklist for SPs.

Table C.2 — Checklist components for large hospitals

Organization type	Definition	Large hospitals			Remarks
		Sub-checklist for medical institutions	Sub-checklist for SIs	Sub-checklist for SPs	
Medical institution	The organization or manager that manages the hospital	X *	-	-	* If the medical institution finds certain items difficult to handle, it should consult the SI or the person in charge of network/system design.
SI	The SI that designs and builds the network and system for the hospital	-	X	-	
SP	The SP or its manager (when the hospital outsources service provision to an SP)	-	-	X *	

(2) Items in the sub-checklists

The table below shows the relationships between the organization types and the items in the sub-checklists. The items marked with ‘M’ are mandatory. Only the applicable items (services that the hospital provides or uses) need be considered for the items marked with ‘A’.

© ISO 2008 – All rights reserved

Table C.3 — Items in the sub-checklists for large hospitals

Service items		"Guidelines for the Security Management of the Medical Information System": Technical and Operational Checklists		
		Large hospitals		
		Sub-checklist for medical institutions	Sub-checklist for SIs	Sub-checklist for SPs
1. Form of communication		M		
2. Communication policy		M	M	M
3. Technical security on the premises		M	M	M
4. Service type				
	4-1 Deployment of ASP information provision services targeted at medical institutions	A	A	
	4-2 Use of ASP information provision services targeted at medical institutions			
	4-3 Use of ASP information provision services (external storage type) targeted at medical institutions	A	A	A
	4-4 Deployment of ASP information provision services targeted at organizations other than medical institutions	A	A	
	4-5 Use of ASP information provision services targeted at organizations other than medical institutions			
	4-6 Use of ASP information provision services (external storage type) targeted at organizations other than medical institutions	A	A	A
	4-7 E-mail service (provider service)	A	A	
	4-8 Internet access service (provider service)	A	A	
	4-9 Use of remote maintenance service	A	A	
	4-10 Access to external service suppliers / large hospitals (relay service)	A	A	A
5. Physical security on the premises		M	M	

Note: A hospital providing or using an individual service must examine all the individual items that are applicable.

© ISO 2008 – All rights reserved

Figure C.4 illustrates the checking steps to follow. For this checklist, conformance to the Guidelines must be checked through the steps below.

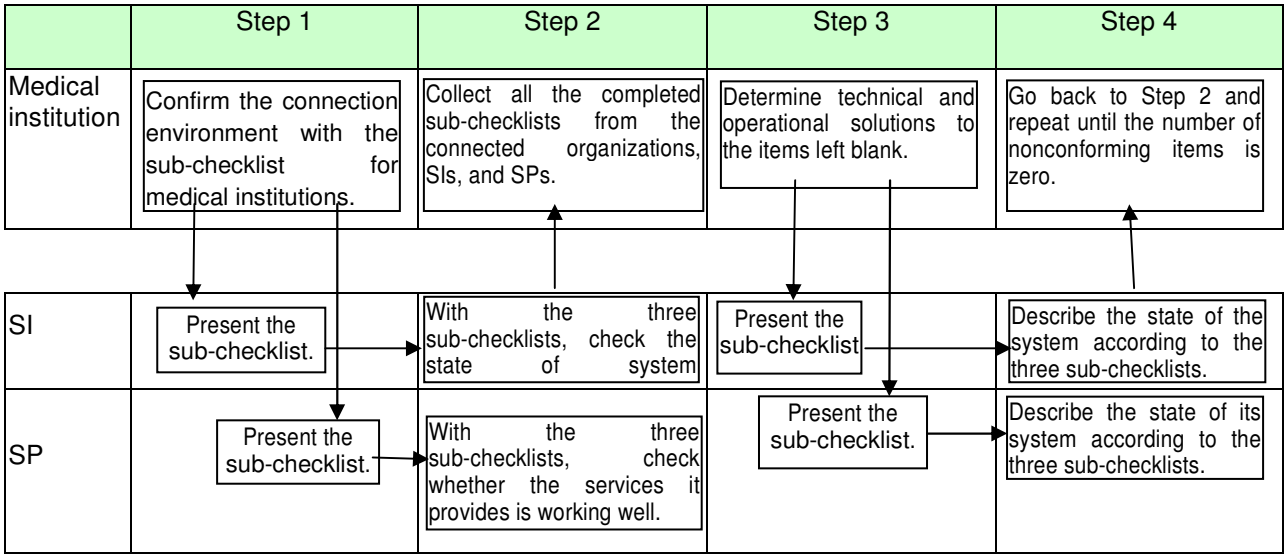

Figure C.4 — Checking steps for large hospitals

Managers of medical institutions must apply this checklist to consider the content and functions of services that SIs and SPs supply, determine solutions to any failure to follow the standards, and clarify each party's responsibility before establishing contracts with SIs and SPs prior to introduction of a network. Each party's responsibility must be defined in writing.

Table C.4 gives the checklist for large hospitals.

© ISO 2008 – All rights reserved

Table C.4 — Checklist for large hospitals

Purpose	Item	Functional element	Criterion	Conditions to be met	Tick an applicable box	Corresponding section of the	Remarks
1. Form of communication							
1-1 Identification of the party to be connected to	1-1-1 Confirmation of security standards followed by the party to be connected to	-	Connecting to a large hospital that belongs to a different legal entity: The large hospital to be connected to has completed the check process with the "Checklist for Large Hospitals" and meets the requirements.	If the party to be connected to belongs to a different legal entity, the party's security policies must be confirmed and the responsibility of each party must be clarified. All the facilities to be connected to must be operated so that the requirements listed in the corresponding checklists are met.	□	6.11 B-1 6.11 B-3	
		-	Connecting to a small hospital that belongs to a different legal entity: The small hospital to be connected to has completed the check process with the "Checklist for Small Hospitals" and meets the requirements.		□		
		-	Connecting to a service provider: The service provider to be connected to has completed the check process with the "Checklist for Service Providers" and meets the requirements.		□		
2. Communication policy							
2-2 Connection between facilities via open networks	2-2-1 Unauthorized relay in the case of connection to multiple facilities that belong to a different legal entity: In the case of multiple connections between different legal entities, each entity is responsible for preventing unauthorized relay.	VPN function	In the case of connection between facilities via a network, a medical institution must check whether unauthorized relay from the institution itself to two or more other facilities or vice versa is prohibited.				
			In the case of connection between facilities via a network, a medical institution must check whether unauthorized relay from the institution itself to other two or more other facilities or vice versa is prohibited.	Measures against such unauthorized relay are taken.	□	6.11 C 4	
2-3 Handling of connection to/from other facilities	2-3-1 Agreement on communication with the facilities to be connected to	VPN function	The facilities to be connected to/from must ensure the following:				
			The contents of services and the form of their operation are confirmed and agreed on.	Measures against such unauthorized relay are taken.	□	6.5 B (5)	
			Agreement on VPN communication has been made.				
3. Technical security on the premises							
3-3 High securlity zone	3-3-4 Connection from a large hospital's HSZ to a different facility	Proxy function /VPN function /firewall function	Check whether the following security measures are taken to protect important data and devices in the SP's HSZ from tampering and intrusion during connection to a large hospital.				
			Measures against DoS attacks and other service interference are taken.	Connection to a large size hospital from the HSZ must be forbidden unless these measures are taken.	□	6.5 B (1) 6.5 B (2) 6.5 B (3) 6.5 B (4) 6.5 B (5)	
			Measures to detect, prevent, and block data tampering and illegal intrusion are taken.				
			Secure access to the Internet is assured.				
			Measures against virus infection are taken.				
			Authentication is performed at the time of connection.				
			Measures to ensure the security of the communication path are taken.				
			Access monitoring is performed.				

© ISO 2008 – All rights reserved

3-5 Security of DMZ	3-5-1 Virus check of each host	Each host	Check whether the virus check is performed properly.				
				The virus definition file is kept up-to-date.	The latest definition file must be used to prevent infection and spread of a virus when stored data contains a virus.	□	6.5 B (4)
3-6 Internal security service	3-6-1 Implementation of security patches and other update functions in the facility	Gateway function /proxy function	Check whether the security patches are up-to-date.				
				The patch files are kept up-to-date.	When downloading security patches via the Internet, hospitals must take measures against security hole attacks by downloading security patches to the host zone where Internet access is not allowed and distributing the patches to the applicable hosts.	□	6.5 B (4) 6.5 B (5) 6.11 B-3 I
4. Service type							
4-1 Deployment of ASP information provision services targeted at medical institutions 【Examples of service provision items】 ・Information provision service ・E-mail service ・Regional partnership service ・Medical test data distribution service ・External storage service ・Time stamp service ・VA service	4-1-1 Information provision or disclosure for medical institutions	Firewall function	Check whether the following security measure is taken to prevent illegal use.				
				Access control is performed to prevent illegal use.	Security measures such as firewall installation must be taken and illegal access to/from unauthorized facilities must be prevented by permitting only destination souce IP addresses that are agreed on with the facilities to be connected to/from.	□	6.10 C (9) 6.11 B2
	4-1-2 Authentication of service-providing users	Server function	Check whether the users providing ASP service are authenticated.				
				Authentication methods			
				Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.5 B (1)
				IC/smart card authentication is performed.		□	6.5 C (7)
				Biometric authentication is performed.		□	6.10 C (9)
	4-1-3 Security measures for using external ASP services via open networks	Proxy function /VPN function /firewall function	Identify the current security measures.				
				Security measures			
				Protection measures against viruses and DoS attacks are taken.	For information provision or disclosure for medical institutions, these security functions must be implemented to protect important data and devices in the HSZ from tampering and intrusion.	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)
				Measures to detect and block illegal packets are taken to prevent tampering and intrusion.			
				Access monitoring is performed.			
				Communication paths are encrypted to prevent spoofing.			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1
	4-1-4 Data storage or device installation in the HSZ	Zone	For information provision for medical institutions, the following security measures must be taken to protect important data and devices from tampering and intrusion.				
				Zone type			
				Located in the HSZ.	The host must be located in the HSZ from the viewpoints of the security level of the data and what services are provided and how they are used.	□	6.10 C (9) 7.3 B 7.4 C

© ISO 2008 – All rights reserved

4-2 Use of ASP information provision services targeted at medical institutions 【Examples of service provision items】 ・Information provision service ・e-mail service ・Regional partnership service ・Medical test data distribution service ・External storage service ・Time stamp service ・VA service							
	4-2-1 Authentication of ASP service users	Server function	Check the method of authenticating ASP service users before use.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		
	4-2-2 Security measures for the use of information provision ASP services	Proxy function /VPN function /firewall function	Identify the security measures currently taken in small hospitals.				
			Security measures				
			Protection measures against viruses and DoS attacks are taken.	For the use of ASP services, these security requirements must be met to protect medical information and other important data and devices in the HSZ from tampering and intrusion.	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			Measures to detect and block illegal packets are taken to prevent tampering and intrusion.				
			Access monitoring is performed.				
			Communication paths are encrypted to prevent spoofing.			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-2-3 Prohibition against combined use of ASP service with relay or provider service	-	Check whether combined use with other services is prohibited.				
			Combined use with provider service is prohibited.	Combined use with relay, provider, or remote maintenance service must be prohibited to prevent threats from spreading when an incident occurs.	□	6.10 C (9) 6.11 B-3	
			Combined use with relay service is prohibited.				
	4-2-4 Installation and storage of hosts in the HSZ	Zone	Check whether the medical information gained through ASP services is stored in the HSZ.				
			Zone type				
			Located in the HSZ.	The host must be located in the HSZ from the viewpoints of the security level of the data and what services are provided and how they are used.	□	6.10 C (9) 7.3 B 7.4 C	
4-3 Use of ASP information provision services (external storage type) targeted at medical institutions 【Examples of service provision items】 ・Outsourcing	4-3-1 Installation of hosts and devices that use ASP services (external storage type)	Zone	Check whether the hosts and devices to be used is located in the HSZ.				
			Zone type				
			Located in the HSZ.	To prevent tampering and information leakage through illegal access, access to the devices that provide external storage service must be allowed only to the host terminals located in the HSZ.	□	6.4 B③ 6.10 C (9)	
4-4 Deployment of ASP information provision services targeted at organizations other than medical institutions 【Examples of service provision items】 ・Information provision service ・E-mail service ・Regional partnership service ・External storage service ・Time stamp service	4-4-1 Information provision or disclosure	Firewall function	Check whether the following security measure is taken to prevent illegal use.				
			Access control is performed to prevent illegal use.	Security measures such as firewall installation must be taken and illegal access to/from unauthorized facilities must be prevented by permitting the destination or souce IP addresses that are agreed on with the facilities to be connected to/from.	□	6.10 C (9) 6.11 B2	
	4-4-2 Authentication of service-providing users	Server function	Check whether the users providing ASP service are authenticated.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		

© ISO 2008 – All rights reserved

	4-4-3 Security measures for using external ASP services via open networks	Proxy function /VPN function /firewall function	Identify the current security measures.				
			Security measures				
			Protection measures against viruses and DoS attacks are taken.	If a hospital provides or discloses important information, it must implement these security functions to protect important data and devices in the HSZ from tampering and intrusion.	□	6.5 B (1) 6.5 B (4) 6.5 B (5)	
			Measures to detect and block illegal packets are taken to prevent tampering and intrusion.				
			Access monitoring is performed.				
			Communication paths are encrypted to prevent spoofing.			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-4-4 Storage of important data or storage of devices into the HSZ	Zone	For information provision for medical institutions, the following security measures must be taken to protect important data and devices from tampering and intrusion.				
			Zone type				
			Located in the HSZ.	The host must be located in the HSZ from the viewpoints of the security level of the data and what services are provided and how they are used.	□	6.10 C (9) 7.3 B 7.4 C	
4-5 Use of ASP information provision services targeted at organizations other than medical institutions 【Examples of service provision items】 ・Information provision service ・e-mail service ・Regional partnership service ・External storage service ・Time stamp service ・VA service	4-5-1 Authentication of ASP service users	Server function	Check the method of authenticating ASP service users before use.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		
	4-5-2 Security measures for the use of information provision ASP services	Proxy function /VPN function /firewall function	Identify the security measures currently taken in small hospitals.				
			Security measures				
			Protection measures against viruses and DoS attacks are taken.	For the use of ASP services, these security requirements must be met to protect important data and devices in the HSZ from tampering and intrusion.	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			Measures to detect and block illegal packets are taken to prevent tampering and intrusion.				
			Access monitoring is performed.				
			Communication paths are encrypted to prevent spoofing.			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-5-3 Prohibition against combined use with relay or provider service	-	Check whether combined use with other services is prohibited.				
			Combined use with provider service is	Combined use with relay, provider, or remote maintenance service must be prohibited to prevent threats from spreading in the case where some incident occurs.	□	6.10 C (9) 6.11 B-3	
			Combined use with relay service is prohibited.				
	4-5-4 Installation and storage of hosts in the HSZ	Zone	Check whether the important information gained through ASP services is stored in the HSZ.				
			Zone type				
			Located in the HSZ.	The host must be located in the HSZ from the viewpoints of the security level of the data and what services are provided and how they are used.	□	6.10 C (9) 7.3 B 7.4 C	
4-6 Use of ASP information provision services (external storage type) targeted at organizations other than medical institutions 【Examples of service provision items】 ・Outsourcing	4-6-1 Installation of hosts and devices that use ASP services (external storage type)	Zone	Check whether the hosts and devices to be used are located in the HSZ.				
			Zone type				
			Located in the HSZ.	To prevent tampering and information leakage through illegal access, access to the devices that provide external storage service must be allowed only to the host terminals located in the HSZ.	□	6.4 B③ 6.10 C (9)	

© ISO 2008 – All rights reserved

4-7 e-mail service (provider service) 【Examples of service provision items】 ・e-mail service	4-7-1 e-mail screening	Gateway function	Check whether protection from spam mail and e-mail with viruses attached is ensured.				
			e-mail senders and recipients are restricted.	These security measures must be taken to protect important data and devices in the HSZ from tampering and intrusion. Otherwise the service must not be used.	□	6.5 B (4) 6.5 B (5)	
			Spam mail is blocked.				
			Virus checking is performed on outgoing and incoming e-mail and suspicious messages are deleted or isolated.				
	4-7-2 Prohibition of the transfer of illegal e-mail	e-mail function	Check whether e-mail is properly transferred.				
			e-mail is properly transferred.	The e-mail function must be protected from being used as a stepping-stone by illegal e-mail.	□	6.5 B (4) 6.5 B (5)	
	4-7-3 Authentication of e-mail service-providing users	Gateway function /server function	Check the authentication method used for e-mail service.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.5 B (1) 6.5 C (7)	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		
	4-7-4 Use of other ISP mail servers (webmail) by the users	Gateway function /proxy function	If webmail is used by request of the users, Check whether the relevant risk has been explained and agreed on.				
			The webmail used is a part of the Internet access service provided by the service provider.	The use of webmail as part of the Internet access service should not be permitted unless the relevant risk has been explained to the users and agreed on.	□	8.1.3 C (1)②	
	4-7-5 Prohibition against combined use of e-mail service (provider service) with relay or ASP service	-	Check whether combined use with other service is prohibited.				
			Combined use with ASP service is	Combined use with relay, ASP, or remote maintenance service must be prohibited to prevent threats from spreading in the case where some incident occurs.	□	6.11 B-3	
			Combined use with relay service is prohibited.				
4-8 Internet access service (provider service) 【Examples of service provision items】 ・Internet access service	4-8-1 Restriction on website browsing	Gateway function	Check whether website browsing unrelated to the users' jobs or use of services is prohibited.				
			Screening with URL whitelisting is	These functions must be working to forbid website browsing unrelated to the users' jobs and to prevent virus infection and information leakage through illegal websites.	□	6.5 B (4) 6.5 B (5)	
			Screening is performed to prevent the users from browsing inappropriate websites.				
			Content filtering is performed to prevent unwanted programs from running.				
	4-8-2 Authentication of Internet access service users	Gateway function /server function	Identify the technology used for authenticating Internet access service users.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.11 B-1 6.11 C-7 8.1.1 C③	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		
	4-8-3 Prohibition against combined use of Internet website browsing with relay service of relay to external service suppliers or ASP service	-	Check whether combined use with other service is prohibited.				
			Combined use with ASP service is	Combined use with relay service or ASP service must be prohibited to prevent threats from spreading in the case where some incident occurs.	□	6.11 B-3	
			Combined use with relay service is prohibited.				

© ISO 2008 – All rights reserved

4-9 Use of remote maintenance service 【Examples of service provision items】 ・Remote maintenance service	4-9-1 Installation of a remote maintenance terminal	Zone	Check whether the hosts and devices to be used are located in the HSZ.					
				Zone type				
				Located in the HSZ.	The remote maintenance and remote monitoring terminal must be located in the HSZ to protect system devices and data.	□	8.1	
	4-9-2 Authentication of remote maintenance operators	Gateway function /server function	Identify the current method of user authentication of a remote maintenance operator.					
				Authentication technology to be implemented				
				Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.11 B-1 6.11 C-7 8.1.1 C③	
				IC/smart card authentication is performed.		□		
				Biometric authentication is performed.		□		

© ISO 2008 – All rights reserved

	4-9-3 Measures against unauthorized operation or manipulation by a remote maintenance operator	-	Check the current rules for remote maintenance.				
			Requirements to be stipulated				
			Rules for managing remote maintenance operators have been established.	These operational rules have been established for protection of personal information and secure system management.	□	8.1.1 C③	
			Rules for managing remote terminals and networks have been established.				
			Measures against unauthorized operation by personnel who do not have an authorized remote terminal have been stipulated.				
			Rules on remote maintenance recording and handling of data delivery/receipt have been established.				
			Rules on addition and relocation of remote terminals have been established.				
4-10 Access to external service supplier/large hospitals (relay service) 【Examples of service provision items】 ・VPN service ・IX service ・ASP service	4-10-1 Installation of data or devices that connect to external service suppliers	Zone	Check whether the devices that connect to external service suppliers are located in the HSZ.				
			The zone where the devices that connect to external service suppliers are located				
			Located in the HSZ.	Such devices must be located in the HSZ to protect system devices and important information	□	6.5 B (5) 6.10 C (9)	
	4-10-2 Authentication of users who use services from external service suppliers	Gateway function /server function	Identify the method of authenticating users who use services from external service suppliers.				
			Authentication methods				
			Accounts are managed with IDs/passwords.	Service-providing users must be authenticated with one of these authentication methods to prevent intrusion of unauthorized users and information leakage. (Only one of these methods will do.)	□	6.10 C (9) 6.11 B-1 6.11 C-7 8.1.1 C③	
			IC/smart card authentication is performed.		□		
			Biometric authentication is performed.		□		
	4-10-3 Security measures for connection to external service suppliers	-	Identify the current security measures.				
			Protection measures against viruses and DoS attacks are taken.	Appropriate security requirements must be met to protect important data and devices in the HSZ from tampering and intrusion.	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			Measures to detect and block illegal packets are taken to prevent tampering and intrusion.				
			Users are authenticated.				
			Access monitoring is performed.				
	4-10-4 Prohibition against combined use of relay service to external service suppliers with provider service or ASP service	-	Check whether combined use with other services is prohibited.				
			Combined use with ASP service is	Combined use with provider service or ASP service must be prohibited to prevent threats from spreading in the case where some incident occurs.	□	6.10 C (9) 6.11 B-3	
			Combined use with provider service is prohibited.				
	4-10-5 Written agreement with external service suppliers and connection admission	-	Check the following for connection to external service suppliers.				
			Service contents and the form of operation are confirmed in writing.	For connection to external service suppliers, written agreement and connection admission are required.	□	6.10 C (9) 6.5 B (5)	
			Agreement with external service suppliers has been made and connection admission has been gained.				

© ISO 2008 – All rights reserved

6. Wireless LAN, mobile terminals, and remote access							
6-1 Security of wireless connection and mobile terminals	6-1-1 Security of wireless LAN	Wireless function	Check whether measures to prevent the use of wireless LAN from being identified are taken.				
			Measures				
			Stealth mode	Stealth mode is selected.	☐	6.5 C-8	
			ANY connection refusal	ANY connection refusal is selected.	☐		
			Check whether measures against illegal access are taken.				
			Measures				
			SSID-based access restriction	SSID-based access restriction is performed.	☐	6.5 C-8	
			MAC address-based access restriction	MAC address-based access restriction is performed.	☐		
			Electronic certificates	Electronic certificates are used for access checking.	☐		
			Check whether measures against illegal acquisition of information are taken.				
			Measures				
			WPA/TKIP-based encryption	WPA/TKIP-based encryption is performed.	☐	6.5 C-8	
			WPA2/AES-based encryption	WPA2/AES-based encryption is performed.	☐		
			Check whether the measures are taken against difficulty in using the wireless LAN because of radio interference in areas where the wireless				
			Measures				
			Prohibition of setting PCs to ad hoc mode	Setting PCs to ad hoc mode is prohibited.	☐	6.5 C-8	
			Restriction of the use of devices that emit radio waves (such as game consoles)	Use of devices that emit radio waves (such as game consoles) is restricted.	☐		
	6-1-2 Control of taking information and IT equipment outside an authorized area	Wireless function	Check the content of the operational rules for managing information and IT equipment.				
			Measures				
			Operational rules for management of taking information and IT equipment outside an authorized area	Operational rules for management of taking information and IT equipment outside an authorized area have been established.	☐	6.9 C-1 to C-4 6.9 C-10	
			Way of management	The way of managing information and IT equipment has been established.	☐		
			Response to theft or loss	The response to theft or loss has been stipulated in the operational rules.	☐		
			Education	The operational rules have been explained and are well understood.	☐		
			Privately owned terminals	The same measures are taken with privately owned terminals.	☐		
			Check whether the locations of information-storing IT equipment and portable media are recognized.				
			Measures				
			Recognition of locations	Types of information and equipment are managed with registers.	☐	6.9 C-5	
			Check the instructions on password setting for IT equipment protection.				
			Measures				
			Password protection	Login password is specified.	☐	6.9 C-6	
			Measures against spoofing	Avoidance of easy-to-guess passwords	☐		
				Change of passwords on a regular basis	☐		

© ISO 2008 – All rights reserved

			Check the instructions on response to theft or loss.				
			Measures				
			Encryption	Data in disks and files is encrypted.	☐	6.9 C-7	
			Password protection	Access password is specified.	☐		
			Check the instructions on measures against data leakage and tampering during connection of IT equipment to a network.				
			Measures				
			Measures against computer viruses	Antivirus software is installed.	☐	6.9 C-8	
			Firewall	A personal firewall is installed.	☐		
			Check whether the access environment is illegally utilized.				
			Measures				
			Restriction of the access environment	Access from a terminal with file-sharing software (such as Winny) installed is not allowed.	☐	6.9 C-9	
	6-1-3 Environment management in the case where medical information and medical institutions are accessed from privately-owned terminals	Wireless function	Check the instructions on password setting for IT equipment protection.				
			Measures				
			Password protection	Login password is specified.	☐	6.9 C-6	
			Measures against spoofing	Avoidance of easy-to-guess passwords	☐		
				Change of passwords on a regular basis	☐		
			Check of instructions on response to theft or loss.				
			Measures				
			Encryption	Data in disks and files is encrypted.	☐	6.9 C-7	
			Password protection	Access password is specified.	☐		
			Check the instructions on measures against data leakage and tampering during connection of IT equipment to a network.				
			Measures				
			Measures against computer viruses	Antivirus software is installed.	☐	6.9 C-8	
			Firewall	A personal firewall is installed.	☐		
			Check whether the access environment is illegally utilized.				
			Measures				
			Restriction of the access environment	Access from a terminal with file-sharing software (such as Winny) installed is not allowed.	☐	6.9 C-8	
	6-1-4 Attitudes to the use of mobile terminals		Confirm the specifications of the services to select.				
			Measures				
			Contract confirmation	The hospital has confirmed the contract with the relevant business.	☐	6.10 C-6 6.10 C-8	
			Check whether a mechanism to prevent wiretapping and tampering is implemented.				
			Measures				
			Content encryption	Use of SSL communication	☐	6.10 C-5	
				Contents are encrypted.	☐		
				S/MIME is used for e-mail encryption.	☐		
			(Direct dial-up through a public network (telephone network))				
			Check whether the access point is correct.				
			Measures				
			Check of the access point	Check the access settings.	☐	6.10 C-2	
			Check whether access authentication is performed.				

© ISO 2008 – All rights reserved

			Measures				
			Access authentication	ID-based, password-based, or one-time password-based access authentication is performed	☐	6.10 C-3 6.5	
				Connected devices are authenticated by the use of portable phone IDs.	☐		
				The source's phone number is registered for access control.	☐		
			(Access via the Internet)				
			Confirm the specifications of the terminal to use.				
			Measures				
			Communication specifications	The terminal can use SSL communication.	☐	6.10 C-5	
			Confirm the service specifications.				
			Measures				
			Communication specifications	IPSec and IKE are applied to the connection path.	☐	6.10 C-1	
			(Access via a closed network (IP-VPN))				
			Confirm the specifications of the terminal to use.				
			Measures				
			Communication specifications	The terminal can use SSL communication.	☐	6.10 C-5	
	6-1-5 Attitudes to the network used for providing patients with clinical records (These should be consistent with the items for 4-4 Deployment of ASP information provision services targeted at organizations other than medical institutions.")	Wireless function	Check whether the access environment is illegally utilized.				
			Measures				
			Check the system in the hospital.	The computer systems and applications that are used to give medical information to patients are separated from other systems and applications owned by the medical institutions.	☐	6.10 C-9	
			Check whether unauthorized intrusion into the computer system in the hospital through the computer system used for providing information is				
			Measures				
			Firewall	A firewall is installed.	☐	6.10 C-9	
			Access monitoring	Access monitoring is performed.	☐		
			SSL communication-based encryption	SSL communication-based encryption is performed.	☐		
			PKI-based personal authentication	PKI-based personal authentication is performed.	☐		
			Check whether sufficient explanation is given to patients.				
			Measures				
			Explanation to the patients	Convincing explanation of thr possible risks and purposes of information provision is given to the patients.	☐	6.10 C-9	
			Check whether the demarcation points of responsibility are clear.				
			Measures				
			Demarcation points of responsibility	Comprehensive actions, including the establishment of legal bases for non-IT activities, are taken and each party's responsibility is clarified.	☐	6.10 C-9	

© ISO 2008 – All rights reserved

C.3 Instructions for the checklist for small hospitals

This checklist is intended for medical institutions that do not have equipment for providing information to different institutions. Medical institutions that have such equipment (i.e., medical institutions that can provide SP services to different institutions) should use the checklist for large hospitals instead.

a) Checklist components

The checklist for small hospitals consists of two sub-checklists for two different organization types: the sub-checklist for medical institutions, and the sub-checklist for SIs.

Table C.5 — Checklist components for small hospitals

Organization type	Definition	Small hospitals		Remarks
		Sub-checklist for medical institutions	Sub-checklist for SIs	
Medical institution	The organization or manager that manages the hospital	X *	-	* If the hospital manager finds certain items difficult to handle, the manager should consult the SI or the person in charge of network/system design.
SI	The SI that designs and builds the network and system for the hospital	-	X	

b) Items in the sub-checklists

The table below shows the relationships between the organization types and the items in the sub-checklists. The items marked with ‘M’ are mandatory. Only the applicable items (services that the hospital uses) need be considered for the items marked with ‘A’.

© ISO 2008 – All rights reserved

Table C.6 —Items in the sub-checklists for small hospitals

Service items		"Guidelines for the Security Management of the Medical Information System": Technical and Operational Checklists	
		Small hospitals	
		Sub-checklist for medical institutions	Sub-checklist for SIs
1. Form of communication		M	
2. Communication policy		M	M
3. Technical security on the premises		M	M
4. Service type			
	4-1 Deployment of ASP information provision services targeted at medical institutions		
	4-2 Use of ASP information provision services targeted at medical institutions	A	
	4-3 Use of ASP information provision services (external storage type) targeted at medical institutions		
	4-4 Deployment of ASP information provision services targeted at organizations other than medical institutions		
	4-5 Use of ASP information provision services targeted at organizations other than medical institutions	A	
	4-6 Use of ASP information provision services (external storage type) targeted at organizations other than medical institutions		
	4-7 E-mail service (provider service)	A	
	4-8 Internet access service (provider service)	A	A
	4-9 Use of remote maintenance service		
	4-10 Access to external service suppliers / large hospitals (relay service)	A	
5. Physical security on the premises			M

Note: A hospital providing or using an individual service must examine all the individual items that are applicable.

© ISO 2008 – All rights reserved

Figure C.5 illustrates the checking steps to follow. For this checklist, conformance to the Guidelines must be checked through the steps below.

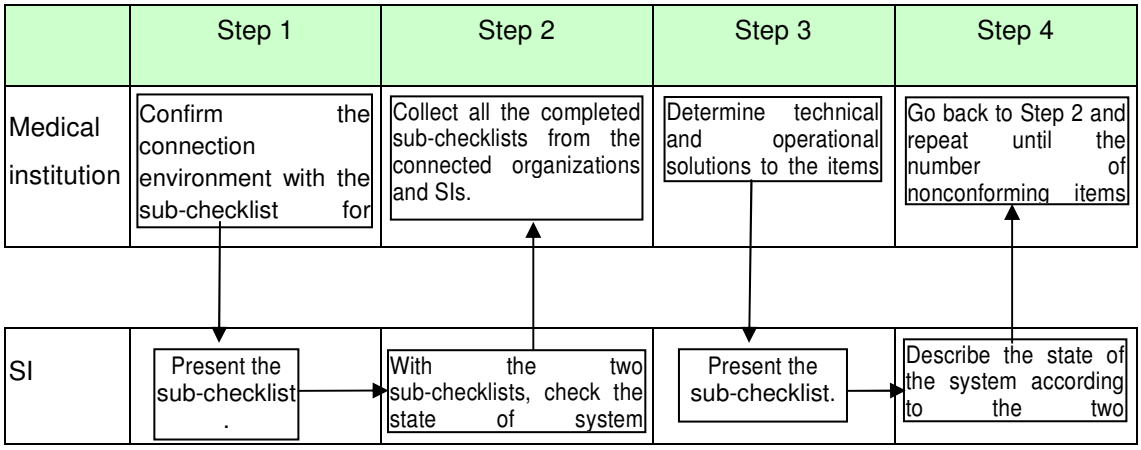

Figure C.5 — Checking steps for small hospitals

Managers of medical institutions must apply this checklist, determine solutions to any failure to follow the standards, and clarify each party's responsibility before establishing a contract with an SI prior to introduction of network. Each party's responsibility must be defined in writing.

C.4 Instructions for the checklist for SPs

a) Checklist components

The checklist for SPs consists of three sub-checklists for three different organization types: the sub-checklist for managers of medical institutions, the sub-checklist for SIs, and the sub-checklist for SPs.

© ISO 2008 – All rights reserved

Table C.7 — Checklist components for SPs

Organization type	Definition	SP			Remarks
		Sub-checklist for medical institutions	Sub-checklist for SIs	Sub-checklist for SPs	
Medical institution	The organization or manager that manages the hospital.	X *	-	-	* If the hospital manager finds certain items difficult to handle, the manager should consult the SI or the person in charge of network/system design.
SI	The SI that designs and builds the network and system for the hospital	-	X	-	
SP	The SP or its manager (when the hospital outsource service provision to an SP)	-	-	X *	

The SP must examine all the items in all of the above three sub-checklists.

b) Items in the sub-checklists

The items vary with the type of service the SP provides for different medical institutions.

— VPN provider service suppliers:

VPN providers that provide VPN services for medical institutions should check the VPN provider requirements listed in the checklist.

— VPN and ASP provider service suppliers:

Providers that provide not only VPN services but also ASP services for medical institutions should check both the VPN and ASP provider requirements listed in the checklist.

— ASP provider service (individual service) suppliers:

Providers that provide individual ASP services such as e-mail, Internet access, and information provision services for medical institutions should check the individual ASP provider requirements listed in the checklist.

Table C.8 shows the relationships between the items in the sub-checklist for SPs and each service supplied by an SP. Depending on the types of service it provides, an SP should check the applicable items (marked with “X”).

© ISO 2008 – All rights reserved

Table C.8 — Relationships between each item in the sub-checklist for SPs and each service supplied by SPs.

Service items		VPN provider requirements		ASP provider requirements	ASP provider (individual service) requirements									
		VPN service	IX service	ASP service	Regional partnership service	Information provision service	Remote maintenance service	E-mail service	Internet access service	External storage service	Medical test result distribution service	Time stamp service	VA service	Outsourcing
1. Form of communication		X	X	X	X	X	X	X	X	X	X	X	X	X
2. Communication policy		X	X	X	X	X	X	X	X	X	X	X	X	X
3. Technical security on the premises				X	X	X	X	X	X	X	X	X	X	X
4. Service type														
	4-1 Deployment of ASP information provision services targeted at medical institutions				X	X		X		X	X	X	X	
	4-2 Use of ASP information provision services targeted at medical institutions													
	4-3 Use of ASP information provision services (external storage type) targeted at medical institutions				X	X		X		X	X	X	X	X
	4-4 Deployment of ASP information provision services targeted at organizations other than medical institutions				X	X		X		X		X	X	
	4-5 Use of ASP information provision services targeted at organizations other than medical institutions													
	4-6 Use of ASP information provision services (external storage type) targeted at organizations other than medical institutions													X
	4-7 E-mail service (provider service)							X						
	4-8 Internet access service (provider service)								X					

© ISO 2008 – All rights reserved

	4-9 Use of remote maintenance service						X							
	4-10 Access to external service suppliers / large hospitals (relay service)	X	X	X										
5. Physical security on the premises		X	X	X	X	X	X	X	X	X	X	X	X	X

Note: If an SP provides two or more of the services listed above, the SP should check all the individual items that are applicable. As for a service not included in the individual ASP service requirements listed above, the SP should identify and check all the applicable items.

An SP must examine the checklist for large hospitals' sub-checklists for managers, for SIs, and for SPs, or the checklist for small hospitals' sub-checklists for managers and for SIs, depending on the type of medical institution the SP provides service for, and it must assure the medical institution of security based on the Guideline. For this purpose, to ensure that the criteria in the checklists for large and small hospitals are met, the SP establish and maintain a contract or memorandum with the medical institution to define the scope of the SP's responsibility regarding the items in these checklists.

© ISO 2008 – All rights reserved

Annex D
(informative)

Technology used: Dynamic on-demand VPN

D.1 VPN security objectives

A VPN is defined in ISO/IEC18028-1,13.2.9.1 as a private network that is implemented by using the infrastructure of existing networks, so that a VPN behaves like a private network from the user perspective and offers similar functionality and services to those of a private network. ISO/IEC18028-1,13.2.9.1 specifies that a VPN can be used in various situations, such as the following:

— Implementing remote access to an organization for mobile or off-site employees

— Linking different locations of an organization together, including redundant links to implement a fall-back infrastructure

— Setting up connections to an organization's network for other organizations/business partners

In addition, ISO/IEC18028-1,13.2.9.2 specifies that the key security risk with communication over an insecure network, more than the risk of unauthorized access, is that sensitive information might be accessible to unauthorized parties, leading to unauthorized disclosure or modification.

ISO/IEC18028-5,6 specifies that the primary security objective of a VPN is protection from unauthorized access. A VPN can therefore be used to fulfill wider network security objectives:

— safeguarding information in networks, systems connected to networks, and the services used by these networks

— protecting the supporting network infrastructure

— protecting network management systems

ISO/IEC18028-5,7 specifies that for the requirements of VPN security to achieve the above objectives, a VPN should be implemented in a way that ensures the following:

— confidentiality of data and code in transit between VPN end points

— integrity of data and code in transit between VPN end points

— authenticity of VPN users and administrators

— authorization of VPN users and administrators

© ISO 2008 – All rights reserved

— availability of VPN end points and network infrastructure

Beyond the above general characteristics, a dynamic on-demand VPN can improve authenticity and authorization of VPN users and administrators, and it features general versatility of access points such as the Internet rather than connection to a specific party.

A dynamic on-demand VPN provides the following functions as measures against network threats:

a) A secure communication path can be ensured by the use of IPsec and IKE. Confidentiality is ensured.

b) Network devices ensuring security can be used, and these can be authenticated at the entry/exit of each base. The validity of connected parties is ensured.

c) The following authentication methods are available: authentication by PKI, and by using a pre-shared key. Authenticity of the VPN users and administrators is ensured.

d) Destination setting is managed by the SP for the dynamic on-demand VPN. N-to-N connection is available, and the responsibilities of the user are reduced.

D.2 The purpose of a dynamic on-demand VPN

As shown in Figure D.1, a dynamic on-demand VPN, which is suitable for a healthcare information network, has the advantages of both good security managed as in IP-VPN and of inexpensive Internet VPN, which ensures security on the Internet for communication. These advantages are guaranteed by the administrative responsibility of the telecommunication carrier. The dynamic on-demand VPN and the Internet VPN are compared in Table D.1. The dynamic on-demand VPN is superior to the Internet VPN in that the authentication level is higher, VPN connection between any bases can be established on demand more easily, and the load for configuring the VPN user environment of users is lighter, among other features. Furthermore, unlike a conventional network, which is built at the initiative of the providers, a dynamic on-demand VPN is a network platform positioned as a user-initiated social infrastructure that allows dynamically changing user connection policies.

© ISO 2008 – All rights reserved

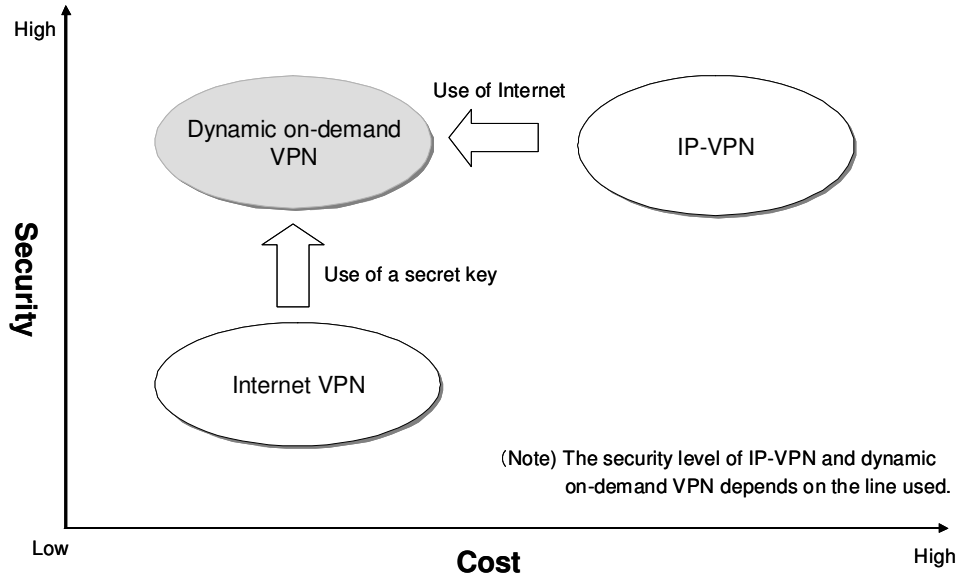

Figure D.1 — Position of the dynamic on-demand VPN

© ISO 2008 – All rights reserved

Item	Dynamic on-demand VPN	Internet VPN
Equipment authentication	• A PKI chip loading an electronic certificate is mounted in a VPN device. • The service provider and a VPN device authenticate the equipment based on the electronic certificate to prevent spoofing of the VPN device	No equipment can be identified due to have no authentication function in existing VPN device.
Environment setting (usability)	• Communication can be started if the VPN device and the dynamic on-demand VPN service are authenticated over the Internet when the VPN device is installed. • To make new connection to another person/party, download a certificate for the service according to the equipment authentication.	Only the VPN connection between the bases is allowed when the VPN device is installed. To allow a new VPN connection with another person/party, the administrator needs to set a key manually.
Target	Since the VPN configuration information is distributed when the connection is started and the identified is made by the ID ensured by a certificate, any internet provider can be applicable.	The target may be limited to specific VPN service providers.

Table D.1 — Comparison of dynamic on-demand VPN and Internet VPN

D.3 Dynamic on-demand VPN connection method

The key feature of a dynamic on-demand VPN is that connection points can easily be changed online to N-to-N connection. To be more precise, the double-layered PKI function incorporated in a PKI chip (IC chip) used in a VPN device (router) allows the dynamic on-demand VPN SP to easily switch the connection online by transmitting a VPN connection service certificate and connection information online over the network. The double-layered PKI function of the PKI chip is an application of the authentication technology of the smart card.

Figure D.2 shows an overview of the dynamic on-demand VPN. A service certificate and connection information are downloaded from the SP of the dynamic on-demand VPN to each VPN device over the network, which organizes group A that includes the regional core hospitals, examination centers, and medical device providers, so that VPN communication is enabled among the members of the group. Likewise, group B is organized to include the regional core hospitals, clinics, pharmacies, and patients, so that VPN communication is enabled among the members of this group. The connection information can be downloaded to each device in response to an application for connection when the conditions for connection to the other end are satisfied. Connection is started according to the information each time connection is required.

The SP of the dynamic on-demand VPN controls the connection information for the members of groups A and B. No connection is enabled unless allowed by the connection information.

© ISO 2008 – All rights reserved

Those devices that are in group C and have no service certificates or connection information cannot connect to devices in groups A or B.

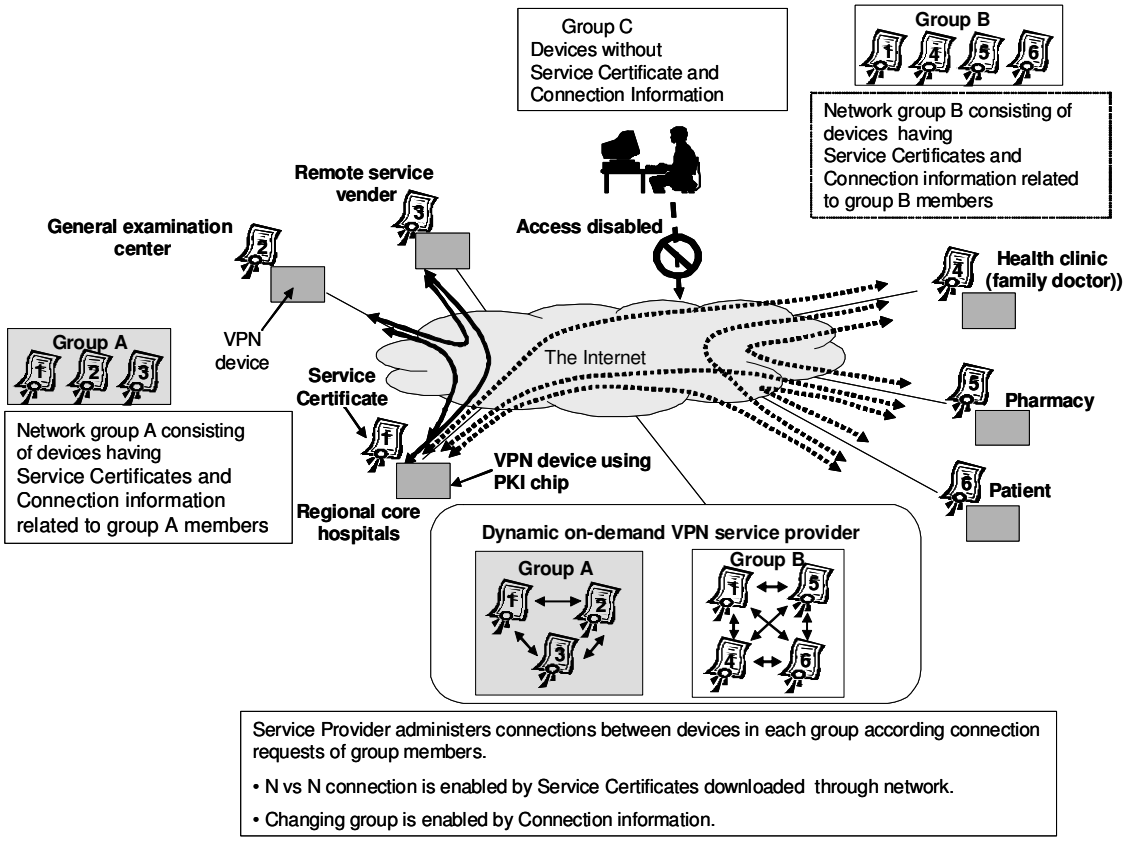

Figure D.2 — Overview of an dynamic on-demand VPN

D.4 Features of the dynamic on-demand VPN

The dynamic on-demand VPN, with the following characteristics, enables mesh-type communication (N-to-N connection) securely and on demand.

a) Authenticates the validity of VPN devices and VPN service users through the double-layered PKI function of the PKI chip.

b) Enables VPN configuration by distributing such parameters and keys online as are necessary for IPsec connection.

c) Prevents spoofing, tampering, and wiretapping by using an IPsec communication channel.

d) Does not require changing application software, since the security is guaranteed at the IP level.

© ISO 2008 – All rights reserved

e) Supports mesh-type communication that allows connection to any medical institution as needed (N-to-N connection, not one-to-one connection)

f) Supports on-demand communication that can be connected when necessary for medical care, such as during a patient visit (connection on demand, not always on).

g) Supports multi-session communication that enables cooperative remote medical care in multiple areas (connection to multiple points with one line).

h) Supports a connection policy that can include individual member policies, in addition to the uniform policy specified by the VPN provider.

D.5 VPN device (router) using a double-layered PKI chip

As shown in Figure D.3, a PKI chip is mounted in a VPN device to enable the dynamic on-demand VPN service. When a VPN device is purchased, it is registered to incorporate a device certified in the first layer of the PKI chip. The owner of the VPN device authenticates its validity by authenticating the certificate to the SP of the dynamic on-demand VPN, using the device certificate of the first layer PKI, and then downloading a service certificate necessary for receiving the VPN service in the second layer of the PKI chip over the network. If a connection is established, the service certificate is authenticated with the SP of the dynamic on-demand VPN using the service certificate of the second layer PKI to download connection information and start the VPN service securely.

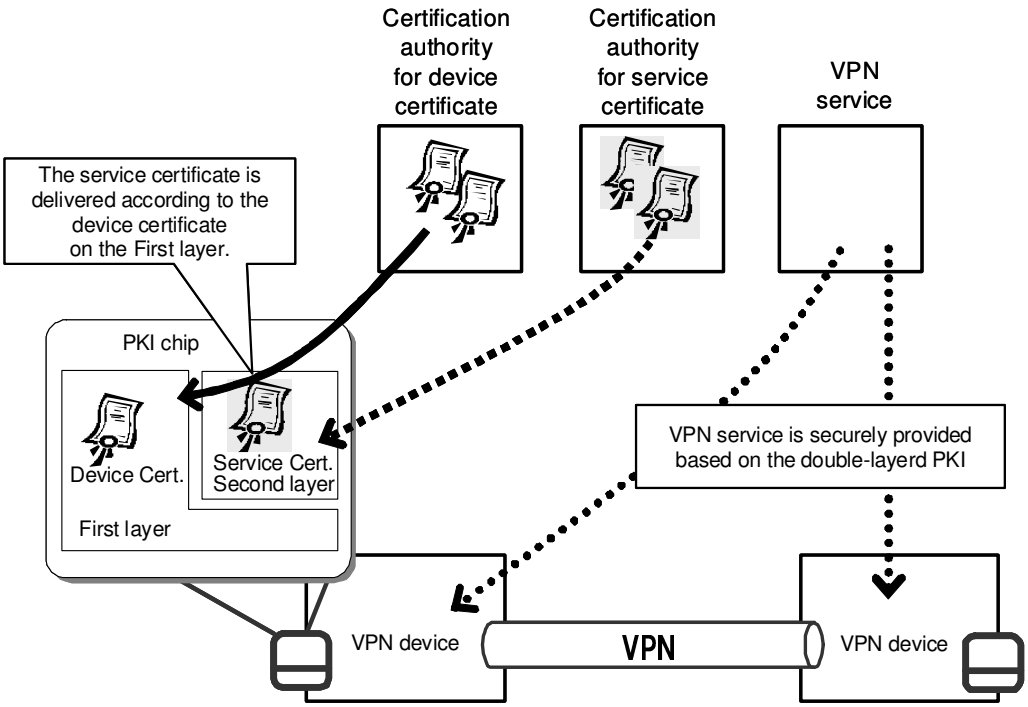

Figure D.3 — Downloading device and service certificates into a PKI chip

© ISO 2008 – All rights reserved

D.6 Registration of VPN device and application of connection

ISO/IEC18028-5 specifies the following. The use of VPN appliances should be considered. While the implementation of VPN functionality through a software solution is adequate in a small-scale VPN (e.g., a single user in a central system), in many situations the use of appliances providing VPN functionalities can have significant advantages, for example, in terms of simplified management and typical operation on a more security-hardened platform. Some form of authentication platform is also likely to be required (e.g., directory, PKI, or RADIUS), which would, for example, allow only authorized users to connect to the central location.

VPN devices should be correctly managed. VPN device management is the generic term for the processes required to set up and monitor VPN devices. Setting up a VPN device consists of configuration to the network configuration and port/application access required, installation of certificates, and continuing network monitoring, as for any other network device.

In the dynamic on-demand VPN, to ensure device security, VPN devices are registered with a certificate-issuing organization and the certificates are incorporated in the VPN devices. Since VPN service certificates are downloaded according to the device certificates, device security is ensured and device spoofing can be prevented. A site and a network device can be authenticated and the validity of the parties connected is ensured, thus strictly satisfying ISO/IEC 18028-5.

Figure D.4 shows an example of the application procedure before a user can start using a dynamic on-demand VPN service.

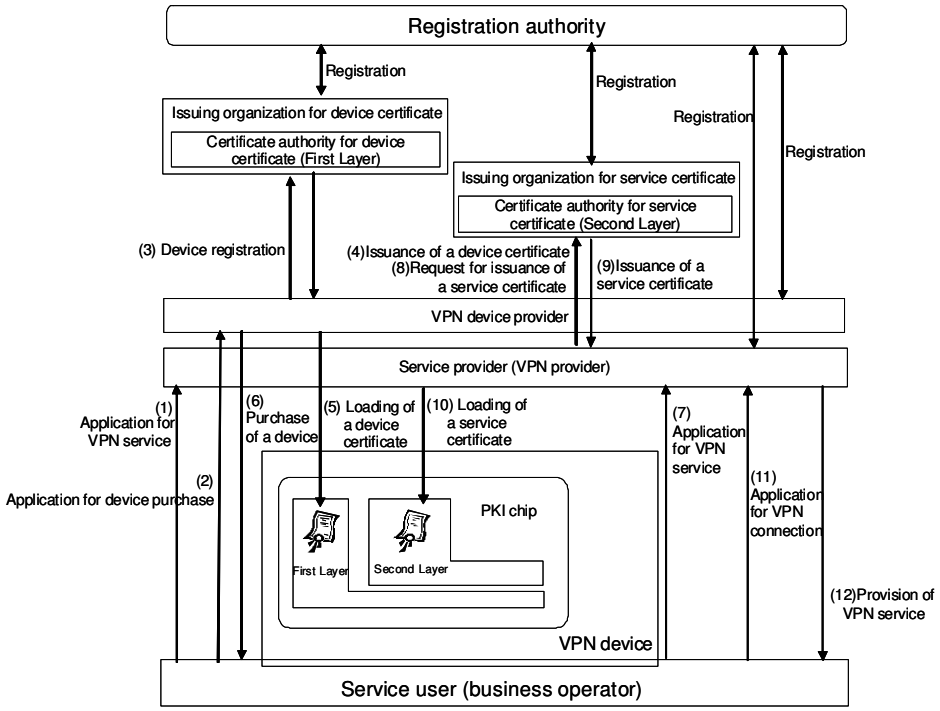

Figure D.4 — Procedure for starting a dynamic on-demand VPN service

© ISO 2008 – All rights reserved

The ASP, the VPN device provider, the issuing organization for the device certificate, and the issuing organization for the service certificate apply for registration as providers and institutions to the registration authority.

a) A (service) user applies to an SP for VPN service.

b) The user applies for purchase of a VPN device from a VPN device provider.
(Applications for VPN service and purchase of a VPN device can be made at the same time. The SP might provide (sell) the VPN device.)

c) The VPN device provider registers the VPN device that the user plans to purchase, with an issuing organization for the device certificate.

d) The issuing organization for the device certificate issues the device certificate for the registered VPN device.

e) The VPN device provider incorporates the device certificate into the first layer of the PKI chip in the registered VPN device.

f) The user purchases (acquires) the VPN device with the device certificate incorporated.

g) The user applies to the SP for VPN service.

h) The SP requests the issuing organization for the service certificate to issue the service certificate for the user.

i) The issuing organization for the service certificate issues the service certificate for the user to the SP.

j) The SP incorporates the service certificate into the second layer of the PKI chip in the user's VPN device.

k) The user applies for VPN connection to the SP.

The SP provides the VPN service to the user. (The connection certificate or pre-shared key is distributed to provide for the VPN service.)

D.7 Precautions on application of a dynamic on-demand VPN

a) Time periods related to configuration to enable a dynamic on-demand VPN

Setup time: A dynamic on-demand VPN takes more time to implement IPsec in terms of setup time than in the case of ordinary communication. The overall time setup time necessary is divided into the time required to use the VPN service and the time required to start IPsec. The time required to start IPsec is the time required to select a destination and implement IPsec. When the handling time for user setup is included, connection is complete in less than 30 seconds.

Overhead: Communication that is based on IPsec (EPS) takes extra time for the called overhead on top of ordinary communication of plain text. The overhead is basically attributable to encryption and decryption. This precaution pertains to setup common to the ordinary IPsec system.

© ISO 2008 – All rights reserved

Real-time traffic: The time of real-time traffic is influenced by the network used by the dynamic on-demand VPN. The Internet currently covers a large number of users and is a best-effort service. A dynamic on-demand VPN influenced by the Internet therefore offers a best-effort service.

b) Communication quality obtained when the dynamic on-demand VPN is used

QoS, packet tagging (Diffserv): The dynamic on-demand VPN applies ESP by way of the IPsec techniques. Techniques to provide QoS (Quality of Service),that correspond to Layer 2 or lower and Diffserv are both applicable. This precaution is similar to that related to the case when ordinary IPsec is applied.

Diffserv uses the Differentiated Service Code in the TOS field of an IP packet. The Differentiated Service Code in an original packet is copied into this field when IPsec is applied, so that the field is not influenced.

c) IP address of the dynamic on-demand VPN

NAT: Protocols such as FTP and SIP cannot be used directly when NAT is performed. This challenge is common to the case when ordinary IPsec is applied.

Firewall: ISAKMP (500/UDP) and ESP (protocol ID: 50) must pass through the firewall. This challenge is common to the case when ordinary IPsec is applied.

Dynamic routing protocol: Under IPsec connection, a routing protocol is encrypted and transferred by ESP. With the dynamic on-demand VPN, connection and disconnection of IPsec is arbitrarily made by the user, so that the network configuration is modified by the user. When the link state type (such as OSPF) is used, recalculation is performed. Because this induces a load on the router, care must be taken depending on the type of routing protocol used.

Influence of existing IP addresses: In case another network with a different SP is connected, racing between IP addresses can occur. The following are possible solutions:

— Matching between addresses is provided in the domain used.

— Racing between addresses is solved by the product design.

— Global addressing is applied.

D.8 Features of double-layered PKI

As shown in Figure D.5, authentication for chip management and authentication for the right to use the service are implemented individually by keys in different layers. With the use of double-layered PKI, various services can be used conveniently and securely.

— First layer: Device authentication → PKI used for authentication and management of the chip, including incorporation of service application

— Second layer: Service authentication → PKI used when the service is provided

© ISO 2008 – All rights reserved

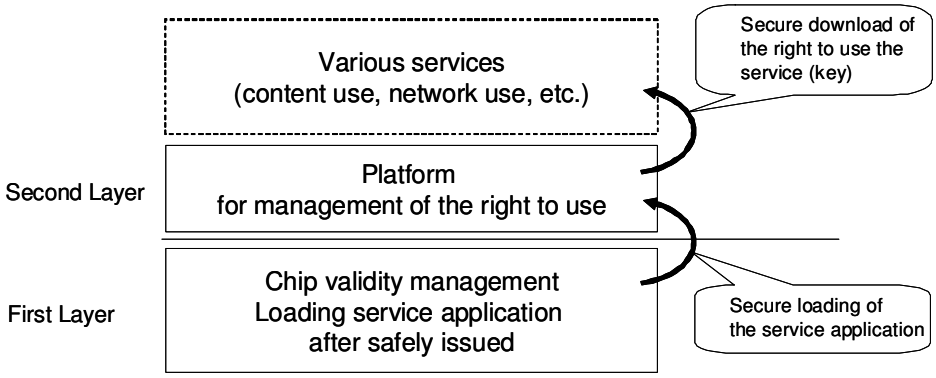

Figure D.5 — Concept of double layered PKI

D.9 Summary

A dynamic on-demand VPN enables secure communication through device authentication and VPN service authentication, using the double-layered PKI function incorporated in the PKI chip used in the VPN device. To change the connection point, a new service certificate simply needs to be downloaded, so that N-to-N VPN connection is possible. With security and flexibility in use, the dynamic on-demand VPN is applicable as a suitable communication scheme to meet the requirements of secure networks in the healthcare field.

© ISO 2008 – All rights reserved