Provisional Translation

The 1st-edition established in December 2011

# Manufacturer Disclosure Statement for Medical Information Security

Japan Medical Imaging and Radiological Systems Industries Association
Medical Imaging System Division
Security Committee

* This English version of the disclosure document is provided for reference purposes only. In the case of any discrepancy between the Japanese original and the English translation, the former shall prevail.

## Preface

### Introduction

In recent years, information technology has advanced remarkably. The need for computerization is further increasing in our information-based society. Also in the field of medical information, regarding the medical information systems and the resultant external preservation of data, Ministry of Health, Labour and Welfare published a comprehensive guideline entitled, "Guideline for the Security Management of Medicalcare Information Systems" (henceforth, Security Management Guideline) for medial institutions being asked to comply properly with Personal Information Protection Law and Utilization of Information and Communication Technology for Document Storage by Private Business Entities Act ( e-Document Law).

Manufacturers publish various explanatory documents for security functions of their medical information systems in their own way because of lack of standard methods of description and standard levels of details. This situation, difficulty to harmonize different systems, is problematical and troubles those people who build a total system in a medical institution. On the other hand, it also troubles manufacturers to meet different formats of description that are specified by each medical institution.

Accordingly, Security Committee (JIRA, Medical Imaging System Division) have attempted to standardize the security statement of product by manufacturers, and have drafted "Manufacturer Disclosure Statement for Medical Information Security (henceforth, Disclosure Statement)." The use of this standard format is intended to enable both medical institutions and manufacturers to efficiently build a better system.

Performing risk assessment and risk management about medical information that is transmitted and maintained through medical information systems, medical institutions will surely be helped by this document. Manufactures are able to quickly respond to medical institutions that enquire about security functions of their products. On the other hand, medical institutions are able to easily review the security information described by manufacturers in the standardized formats.

This document consists of a disclosure statement based on Security Management Guideline Edition 4.1 (issued in February 2010) and explanatory notes about how to fill in this format. Readers are requested to have prior knowledge of Security Management Guideline (especially, Chapter 6).

December 2011, Japan Medical Imaging and Radiological Systems Industries Association

Medical Imaging System Division, Security Committee
"Manufacturer Disclosure Statement for Medical Information Security" Working Group

Contents

## 1 Scope

The format specified in this document is expected to be used as follows. The format is filled in by manufacturers as a part of product explanation and disclose to medical institutions to help them implement the security management.

(1) The format should concern the security function of medical information system provided by manufacturers, show the technical conformity to Security Management Guideline Chapter 6, and help medical institutions to understand the necessary operative measures.

(2) The format should provide helpful information to medical institutions that must follow with Security Management Guideline.
Introducing the system and implement the security management, medical institutions can use the information disclosed by manufacturers for risk assessment.

(3) The format can be used by manufacturers to self-check their conformity with Security Management Guideline.

(4) The format can be used by medical institutions as a basis, when they request manufacturers to explain the security functions.

The description unit in this format is the medical information system provided as a product unit. For example, it is a package of functions provided as a product and options under a certain model name. If it includes any other manufacturer's product (for example, OS or middleware),the function realized by such a product shall be included in the description.

Furthermore, the format in this document enables manufacturers to additionally describe technical security-related functions in each medical information system.

The use of this format is not mandatory. However, JIRA intends that the format should be used widely enough to be recognized as a de-fact standard, and expects that it will be posted by manufactures to their homepages etc.

Although JIRA created this format, it does not certify, test or inspect the design, installation, maintenance etc. of a product. It does not guarantee fulfillment of specific purpose and needs in a specific medical institution, and does not guarantee performance of individual product or service. The manufacturer who filled in this format shall take full responsibility for the description.

## 2 References

Ministry of Health, Labour and Welfare. Guidelines for the Security Management of Health information Systems. Edition 4.1
http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html

SPC Manufacturer Disclosure Statement for Medical Device Security- ver2 (2008)
http://www.jira-net.or.jp/commission/system/04_information/information. html#02-05
HIMSS/NEMA Standard HN 1-2008 Manufacturer Disclosure Statement for Medical Device Security
http://www.jira-net.or.jp/commission/system/04_information/information.html#02-05
HIMSS/NEMA Standard HN 1-2008 Manufacturer Disclosure Statement for Medical Device Security
http://www.jira-net.or.jp/commission/system/04_information/information.html#02-05

MEDIS-DC. Program of Rating Evaluation for Medical Information Systems Safety Control (PREMISs). Self-evaluation file (Form 6)
http://premiss.medis.or.jp/download.html

## 3 Terms and Definitions

e-Document Law
The generic name of "Utilization of Information and Communications Technology for Document Storage by Private Business Entities Act "

Biometric authentication
The authentication identified by the body characteristics of the user.

Controlled area
The area which requires a more careful control defined by a HDO in order to protect information asset.

Routing
The structure to select the optimized route for transfer an IP packets to destination, using the collected information of route information.

Protocol control
The structure incorporated by the information of implementing the protocol-based procedure, when using a device and a software which implements a various protocols (set of the predefined arrangement mutually decided when computers communicate through the network) defined by a standards.

Specific authorization certificate authority
PKI certificate authority operated by the accredited certifying body specified in the Electronic Signatures and Authentication Services Act.

Authenticity
It is an action shall be taken to enable the identification of alteration or erasure about an electromagnetic record in the due period of storage, including its contents, and to clarify the location of responsibility for the creation of the electromagnetic record. (Quoted from Security Management Guideline)

Clear screen
The concept in a security control of a personal computer. The measures are intended to prevent leakage of confidential information, unauthorized access to information etc. For example, logging off the terminal from display, while operator leaving a terminal.

Confidentiality
Term used to prevent the disclosure of information to unauthorized individuals or systems.

Object security

The safety measure for information. For example, signing for an encryption of a file or to detect a tampering.

Channel security
The safety measure for a securing a communication channel. Example of channel security will be VPN and IPSec.

Security target
The concept used by "the ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation". It is a specification of the security design, describing a security target which should be provided by the information system.

Time stamp
The digital signed date and time issued by a third party, in order to prove that the existence of information and not have been tampered.

## 4 Symbols and abbreviation

This disclosure document uses the following symbols, abbreviation and notation.

CAdES:CMS Advanced Electronic Signatures

COCIR:the European Coordination Committee of the Radiological and Electromedical Industry

JIRA: Japan Medical Imaging and Radiological Systems Industries Association

NEMA:National Electrical Manufacturers Association

SPC:Joint NEMA/COCIR/JIRA Security & Privacy Committee (the joint committee of NEMA, COCIR, and JIRA about security and privacy)

XAdES:XML Advanced Electronic Signatures

# 5 Checklist
## 5.1 How to fill in the checklist

The checklist has two parts. The first part is the checklist itself and the second part is the Note column that complements the checklist. The checklist is a question-and-answer format. The Note column is a free text. The number in the parenthesis at the end of check item corresponds to the chapter number of Security Management Guideline.

The items of the checklist are as follows.

(1) Basic information

| | |
|---|---|
| manufacture's Name: | Describe the name of the manufacturer of a product. |
| Product Name: | Describe the name and model name of a product. |
| Version: | Describe the version of a product. |
| Release date: | Describe the release date of a checklist. |

(2) Question items
The number in the parenthesis of the question item corresponds to the chapter number of Security Management Guideline, version 4.1.

Yes: Select this when the system meet the question. If it is an option, describe it in Note.

No: Select this when the system does not meet the question.

NA (Not Applicable) : Select this when a required function is not relevant to a product.

Note: Describe the number you write in Note Column (Note _____) .Describe the details in "Note Column".

(3) Note Column
In the left column, describe the number indicated in a Note of the checklist. In the right column, describe the details. If the latest revision of Security Management Guideline should make this format obsolete, describe a non-conforming part in this Note Column until JIRA revises this format.

## 5.2 Checklist

| | |
|---|---|
| Manufacture's Name ： | Release date ： |
| Product Name ： | Version ： |

Implementation of Information Security Management System (ISMS) at a Medical Institution (6.2)

1 Is the list of PHI presented? (6.2. C1) Yes. No NA (Not Applicable) Note__

Physical Security Measures (6.4)

2 Does the system have a function to prevent prying? (6.4. C5) Yes. No NA Note__

Technical Security Measures (6.5)

3 Does the system have a function to prevent unauthorized input? (6.5. C3) Yes. No NA Note__

4 Does the system have a function of access control? (6.5. C1, 6.5. C5) Yes No NA Note__

4.1 What kind of authentication method for access control? (6.5. C1).

- Passwords Yes No NA Note__
- Biometrics Yes No NA Note__
- Physical media Yes No NA Note__
- Two-factor Yes No NA Note__
- Others (please write down a abstract method in a note) Yes No NA Note__

4.1.1 Using a password authentication , does the system have a function of password management? (6.5. C10-1 to-6.5.C10-3). Yes No NA Note__

4.2 Does the system have function of logging the audit trail? (6.5. C6) Yes No NA Note__

4.2.1 Does the system have a function of presenting the audit trail for users. Can user check an access log? (6.5. C6) Yes No NA Note__

4.2.2 Can the system restrict an access to the audit trail? (6.5. C7) Yes No NA Note__

5 Does the system have a mechanism to assure an accuracy of time information? (6.5. C8) Yes No NA Note__

6 Does the system have a capability to control malware effectively? (6.5. C9) Yes No NA Note__

7 Does the system have a function of security measure for wireless LAN? (6.5. C.11) Yes No NA Note__

Taking out Information and Information Equipment (6.9)

8 Does the system have a function to restrict installation of software? (6.9. C9) Yes No NA Note__

9 Can the system disable the function to import/export? (6.9) Yes No NA Note__

10 Does the system have a function to limit an access such as using a boot password, when information is carried out from the controlled area? (6.9. C6, 6.9.C7) Yes No NA Note__

Emergency Action in Disasters or Other Incidents (6.10)

11 Does the system have any function or account in case of an emergency situation? (6.10. C1) Yes No NA Note__

Security Management at External Exchange of Health information Including Personal Information (6.11)

12 Does the system have a function of transmitting/receiving a medical information (including personal information) between exterior, or a function of remote maintenance ? (6.11. C1) Yes No NA Note__

12.1 Does the system have a function to prevent a spoofing? (6.11. C3) Yes No NA Note__

12.2 Does the system have a function to encrypt data (SSL, S/MIME, file encryption, etc.)? (6.11. C5)
Yes No NA Note__

12.3 Does the system have a function of routing and protocol control of network? (6.11. C4)
Yes No NA Note__

12.3.1 Can the system be configured to satisfy the Security Management Guideline for routing and protocol control of network?(6.11. C4). Yes No NA Note__

12.3.2 Is there any document that can clarify an adequacy of function for routing and protocol control? (6.11. C4)
Yes No NA Note__

12.4 Does the system have a remote maintenance function? (6.11. C7) Yes No NA Note__

12.4.1 Does the system have a function to limit an unnecessary remote login? (6.11. C7)
Yes No NA Note__

Electronic Signature for Compulsory Signing and Sealing (6.12).

13 Does the system support any document that requires digital signature or sealing? (6.12. C. (1))
Yes No NA Note__

13.1 Does the system have digital signature function supporting a certificate issued by HPKI authority or specific acknowledged certificate authority? (6.12. C. (1)) Yes No NA Note__

13.2 Does the system have a verification function using a certificate issued by HPKI authority or specific acknowledged certificate authority? (6.12. C. (1)) Yes No NA Note__

13.3 Does the system have a function to provide the time stamp acknowledged by Japan Data Communications Association? (6.12. C. (2)) Yes No NA Note__

13.4 Does the system have a function to verify the time stamp acknowledged by Japan Data Communications Association? (6.12. C. (2)) Yes No NA Note__

13.5 Does the system have a mechanism to ensure an authenticity of document during a storage period? (6.12. C. (2)) Yes No NA Note__

| Note Column | |
|---|---|
| | |

## 6 Explanation of checklist.

6.1 " 1 Is the list of PHI presented? (6.2. C1)"

This item is to check whether all the information handled is listed in order to perform the risk analysis in system based on Security Management Guideline "6.2.2 the grasp of handled information".

Answer "Yes" when all the information handled in information system is listed. If not, answer "No." For the reason of question is not relevant (NA), or some lists are insufficient etc., when the supplementary explanation is needed, then describe it in Note.

6.2 "2 Does the system have a function to prevent prying? (6.4. C5)"

This item is to check whether the system has a function to prevent prying based on Security Management Guideline "6.4 Physical safety measures".

Answer "Yes" when the system has a function to prevent prying. If not, answer "No". Answer "NA" when this item is not relevant to the applicable equipment. When you have supplementary explanation, describe it in Note.

6.3 "3 Does the system have a function to prevent unauthorized input? (6.5. C3)"

This item is to check whether the system has a function to prevent unauthorized input.

Answer "Yes" when the system has a countermeasure (e. g. clear screen) against unauthorized input while an operator leaves a terminal for a long time. If not, answer "No". Answer "NA" when this item is not relevant to the applicable equipment. When you have supplementary explanation, describe it in Note.

6.4 " 4 Dose the system have a function of access control? (6.5.C1, 6.5.C5)"

Answer "Yes" when the system has a function of user identification and user authentication. If not, answer "No". Answer "NA" when the access control is out of scope of function.
In addition, for better answer, understanding "B. Concept" of Security Management Guideline "6.5 Technical Security Measures" is needed.

6.4.1 "4.1 What kind of authentication method for access control? (-)"

Answer from the following items what can be used as an authentication of an access control. (Multiple answers are available.)

Passwords, biometrics, physical media, two factor and others (please write down an abstract method in a note.)

6.4.1.1 " 4.1.1 Using a password authentication, does the system have a function of password management? (6.5. C10-1 to 6.5.C10-3)"

Answer "Yes", when a password is used for user authentication and the password control is possible. If not, answer "No". This item requires the password control where the password is both enciphered and protected against easy guess.

6.4.2 "4.2 Does the system have a function of logging the audit trail? (6.5. C6)"

Answer "Yes" when the system has a function that outputs the access log.

6.4.2.1 "4.2.1 Does the system have a function of presenting the audit trail for users. Can user check an access log? (6.5. C6)

Answer "Yes" when the access log can identify and confirm user, an access time (user login time, operation time) and accessed personal information.

6.4.2.2 "4.2.2 Can the system restrict an access to the audit trail? (6.5. C7)"

Answer "Yes" when it is possible to restrict a user who access the access log including personal information, and when it is possible to prevent unauthorized deletion, tampering, or addition of access log.

6.5 "5 Does the system have a mechanism to assure an accuracy of time information? (6.5. C8)"

Answer "Yes" when the health information system has any time synchronization method with the standard time for time information to be used for access log.

6.6 " 6 Does the system have a capability to control malware effectively? (6.5. C9)"

Answer "Yes" when the system has a measure for malware (e.g. the detection and removal functions of a computer virus). When using anti-virus software, up date of the pattern file periodically is needed. If the system has any concrete measures, restrictions, etc. indicate in the notes section.

6.7 " 7 Does the system have a function of security measure for wireless LAN? (6.5.C.11) "

Answer "Yes" when the system has a security measure for the use of wireless LAN. Answer "NA" when the use of wireless LAN is not allowed. Indicate a concrete available security function in the notes section.

6.8 "8 Does the system have a function to restrict installation of software? (6.9.C9)"

This item is to check whether the system have a function to restrict installation of software. The measure against leakage of information such as restricting installation of inadequate software is necessary inappropriate.

Answer "Yes" when a system has a function to restrict installation of software. Answer "No" when a system does not have the function. Answer "NA" when installation of software is not possible.

6.9 " 9 Can the system disable the function to import/export? (6.9)"

This item is to check whether it is possible to disable the external import/export device (a DVD drive, USB memory, etc.). Disabling the external import/export device makes it possible to prevent intrusion of a computer virus or leakage of information etc.

Answer "Yes" when the system has a function to disable an external import/export device. Answer "No" when the system does not have the function. Answer NA when the system has no external import/export device.

6.10 "10 Does the system have a function to limit an access such as using a boot password, when information is carried out from the controlled area? (6.9. C6, 6.9.C7)"

This item is to check whether usage can be restricted by access limit such as the start-up password when portable device (e.g. ECG, laptop PC) is carried outside of the controlled area. An information terminal or a portable device has a risk of theft, loss, or misplacing. There for information leakage preventive measures are needed to these risks.

Answer "Yes" when an information terminal and a portable device have function to put a restriction on the access to the system. Answer "No" when an information terminal and a portable device do not have the function to put a restriction on the access to the system. Answer NA when it is not possible physically to carry outside the control area, or when information is not retained.

6.11 "11 Does the system have any function or account in case of an emergency situation? (6.10. C1)"

This item is to check whether the system has a function to provide medical services at the time of a natural disaster and IT faults. In an emergency, measures in case of normal user authentication being impossible (function to access the patient data with an emergency account) or a function responding to a procedure for emergency such as without registering a patient at reception at the time of disaster is required.

Answer "Yes" when a system has emergency functions or emergency account mentioned above. Answer "No" when a system does not have emergency functions or emergency account mentioned above. Answer NA when a system has no account management function.

6.12 "12 Does the system have a function of transmitting/receiving medical information (including personal information) between exterior, or a function of remote maintenance? (6.11. C1)"

This item is to check whether the system have a function of exchange a medical information (including personal information) with external systems, or have a function of remote maintenance. It includes one-way connection. "The exchange of a medical information (including personal information) with external systems" includes the following cases: A medical institution, a pharmacy, and a clinical laboratory exchange a medical e information; A medical staff accesses an information system in a institution from external systems using mobile computer; and a patient accesses an information system from external systems.

Answer "Yes" when the system has a function to exchange medical information. . If not, answer "No." If you answer "Yes", answer to questions 12.1 to 12.4.

6.12.1 "12.1 Does the system have a function to prevent a spoofing? (6.11. C3) "

When information is exchanged with external systems, it is necessary to assure authenticity of a sender and a receiver in order to keep confidentiality. Answer whether the system has a function of authentication to protect against spoofing.

Answer "Yes" when the system has an authentication function. If not, answer "No." If an additional explanation is needed, describe specifications of an authentication function in Note.

6.12.2 "12.2 Does the system have a function to encrypt data (SSL, S/MIME, file encryption, etc.)? (6.11. C5)"

"Encryption data" means encryption for layer four or more of OSI reference model. This question is to ask whether the system has an encryption (object security) function of the data itself to keep confidentiality for information exchange with external systems. Note that this is not encryption (channel security) for layer three or less of OSI reference model, such as IPSec.

Answer "Yes" when encryption of data is possible.. If not, answer "No". If additional information is needed, describe the specification of encryption in Note.

6.12.3 "12.3 Does the system have a function of routing and protocol control of network? (6.11. C4) "

This item is to check whether the route is set up to prevent communication between VPNs connecting different facilities via a router within the facility. "Network route control and protocol control" refers to having network equipment (router, switch, firewall, etc.) or equivalent function. It refers to limiting the connection route or prohibiting a bypass in order to minimize information security risk.

Answer "Yes", when there is such a function. If not, answer "No." If your answer is "Yes", reply to questions in 12.3.1 and 12.3.2.

6.12.3.1 "12.3.1 Can the system be configured to satisfy the Security Management Guideline for routing and protocol control of network? (6.11.C4)

Answer "Yes" when it is possible. If not, answer "No."

6.12.3.2 "12.3.2 Is there any document that can clarify an adequacy of function for routing and protocol control? (6.11. C4)

This item is to check whether the network equipment to exchange information with external facilities is accompanied with a document that can prove its conformity to Security Management Guideline requirement. For example, it refers to a document that specifies the security target specified by ISO15408 or the similar security countermeasures.

Answer "Yes" when equipment is accompanied with a document. If not, answer "No."

6.12.4 "12.4 Does the system have a remote maintenance function? (6.11. C7)"

This item is to check whether a maintenance company provides the remote maintenance service to the equipment. When a company provides the remote maintenance service, reply also to questions in 12.4.1.

Answer "Yes" when a maintenance company provides the remote maintenance service. If not, answer "No".

6.12.4.1 "12.4.1 Does the system have a function to limit an unnecessary remote login? (6.11. C7) "

This item is to check whether the system user can set up an access point, limit protocol, access management, in order to prevent unnecessary login about remote maintenance service.

Answer "Yes" when they have a function. If not, answer "No."

6.13 "13 Does the system support any document that requires digital signature or sealing? (6.12. C. (1))"

This item is to check whether the software creates, refers, and retains a document that requires signature and sealing. Examples that require signature and sealing are a diagnosis, a REFFERAL, radiation exposure record, etc.

When you answer "Yes", reply to 5 items after 13.1. To create these documents in electronic format, you need the electronic signature that suits the e-Signature Act. Moreover, when referring to the document that has electronic signature and the time stamp, you may need to verify the electronic signature and the time stamp. Furthermore, when you save the electronic document over a long period of time exceeding the term of validity (generally about ten years) of the time stamp, you need to perform the long-term signature technique for reservation of authenticity, or the equivalent measures.

6.13.1 "13.1 Does the system have digital signature function supporting a certificate issued by HPKI authority or specific acknowledged certificate authority? (6.12. C. (1))

This item is to check whether there is a function to create the document that requires signature and sealing. Security Management Guideline demands the use of a HPKI certificate or a certificate issued by a certificate authority. It is an essential function to give electronic signature.

Answer NA when there is no creation function. Answer "Yes" when there is creation function and describe the corresponding certificate in Note. If you answer "No", you need to provide an alternative means to give electronic signature. If possible, describe how to offer signature function co-works with the system, in Note.

6.13.2 "13.2 Does the system have a verification function using a certificate issued by HPKI authority or specific acknowledged certificate authority? (6.12. C. (1))"

This item is to check whether there is a function to verify a document that requires signature and sealing. Security Management Guideline demands the verification of a HPKI certificate or a certificate issued by a certificate authority. It is an essential function to give electronic signature.

Answer NA when there is no verification function. Answer "Yes" when there is verification function and describe the corresponding certificate in Note. If you answer "No", you need to provide an alternative means to verify electronic signature. If possible, describe how to offer signature verification function co-works with the system, in Note.

6.13.3 " Does the system have a function to provide the time stamp acknowledged by Japan Data Communications Association? (6.12. C. (2))"

This item is to check whether it is possible time stamping. This is because Security Management Guideline demands the use of the time stamp accredited by the Japan Data Communication Association. In electronic document creation, it is necessary timestamp after signing electronically.

Answer NA when there is no creation function of the document that requires signature and sealing. When there is creation function, answer "Yes" and describe the corresponding time stamp service. When you answer "No", you need to offer an alternative means time stamping. If possible, describe how to stamp the time that is cooperate with the system, in Note.

6.13.4 "13.4 Does the system have a function to verify the time stamp acknowledged by Japan Data Communications Association? (6.12. C. (2)) "

This item is to confirm the time stamp verification. Security Management Guideline demands the use of time stamp accredited by the Japan Data Communication Association. At the time of reference of the document, verification may be needed.

Answer NA when there is no reference function of the document that requires signature and sealing. When there is reference function, the verification function of time stamp is needed. When you answer "Yes", describe the available time stamp service.

6.13.5 "13.5 Does the system have a mechanism to ensure an authenticity of document during a storage period? (6.12. C. (2)) "

The item is to confirm the storage function. The legal storage period exceeds 10 years for some documents. Some documents are stored for a period of more than 10 years beyond the legal storage period. Their authenticity cannot be assured by a time stamp alone. When documents are stored beyond the valid period of time stamp, this item confirms the functions specified by JIS CAdES , XAdES or similar functions to assure the equivalent authenticity.

Answer NA when there is no function to store a document that requires signature and sealing. When you answer "Yes", describe a specific method in Note. When you answer "No", you need to offer an alternative means to assure authenticity. If possible, describe how to assure authenticity incorporate with the system in Note.

Annex　WG about Manufacturer Disclosure Statement for Medical Information Security, List of authors

Takashi Igarashi (KONICA MINOLTA MEDICAL & GRAPHIC, INC.)
Kaneki Shimono (Goodman Co., LTD)
Shinichiro Nishida (Shimadzu Corporation)
Tsutomu Nozu (Research Institute of Systems Planning, Inc.)
Isao Haga (KONICA MINOLTA MEDICAL & GRAPHIC, INC.)
Taizo Hirata (Siemens Japan K.K.) (Convener)
Hideyuki Miyohara (MITSUBISHI ELECTRIC CORPORATION)

List of translators

Takashi Igarashi (KONICA MINOLTA MEDICAL & GRAPHIC, INC.)
Kaneki Shimono (Goodman Co., LTD)
Shinichiro Nishida (Shimadzu Corporation)
Tsutomu Nozu (Research Institute of Systems Planning, Inc.)
Isao Haga (KONICA MINOLTA MEDICAL & GRAPHIC, INC.)
Taizo Hirata (Siemens Japan K.K.) (Convener)
Hideyuki Miyohara (MITSUBISHI ELECTRIC CORPORATION)
Masao Murata (FUJIFILM Corporation)
Yasushi Okada (Toshiba Medical Information Systems Corporation)