厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

Guidelines on Safety Management of Healthcare Information Systems Ver. 6.0 -- Outline and Major Points Amended

Specific Drug Development Support/Healthcare Information Councilor Office, Health Policy Bureau, Ministry of Health, Labour and Welfare

Ministry of Health, Labour and Welfare of Japan

Background for Devising the Guidelines on Safety Management of Healthcare Information Systems and History of Revision

- The Guidelines on Safety Management of Healthcare Information Systems, Version 1, were prepared in March 2005 as a set of guidelines on information security management to comply with the e-Document Act (Act on Utilization of Telecommunications Technology in Document Preservation, etc. Conducted by Private Business Operators, etc.), protection of personal information and so on.
- It subsequently underwent revisions corresponding to trends in various related systems, advances in information system technology, etc. Recently, **Version 6.0 was prepared in May 2023.**

Time of preparation/revision

Version 1	Version 2	Version 3	Version 4	Version 4.1	Version 4.2	Version 4.3	Version 5	Version 5.1	Version 5.2	Version 6.0
2005 March	2007 March	2008 March	2009 March	2010 February	2013 October	2016 March	2017 May	2021 January	2022 March	2023 May

Version

Preparing/revision outlined

Version 1
- Prepared for the purpose of healthcare information system security management.

Version 2
- Revised from the viewpoint of healthcare information systems as critical infrastructure.

Version 3
- Revised corresponding to discussions over personal information-related measures and spread of mobile terminals.

Version 4
- Revised corresponding to discussions over personal information protection and spread of mobile terminals.

Version 4.1
- Revised about external storage of information at private sector data centers.

Version 4.2
- Revised corresponding external storage of dispensed prescriptions, dispensing records, etc.

Version 4.3
- Revised corresponding to "Guidelines on Operation Related to Electronic Prescriptions."

Version 5
- Clearer definition of the scope of medical facilities, etc.
- Corresponding to amended Act on the Protection of Personal Information,
- Corresponding to trends in cyber-attacks.

Version 5.1
- Corresponding to cloud services
- Corresponding to authentication and password
- Corresponding to cyber-attacks, etc.
- Corresponding to external storage contractor selection criteria

Version 5.2
- Securing coherence with guidelines, etc., of two other ministries (MIC and METI).
- Corresponding to amended Act on the Protection of Personal Information, etc.
- Coping with diversification/sophistication of cyber-attacks on medical facilities.
- Corresponding to "Regulatory Reform Implementation Plan," etc.
- Electronic signature
- External network, etc.

Version 6.0

Review of overall design
- Reconstituted into 4 chapters (Overview, Governance, Management, Control).
- Improvement in Q&A

and so on

Technical trends
- Adjustments about the utilization of outside contractors and services
- Adjustments of views about information security
- Corresponding to new technologies and changes in systems/specifications,

etc.

Policies for revising Version 5.2 into Version 6.0

Because online qualification check is mandatory, as a rule, at NHI-covered medical facilities and pharmacies from April 2023, almost all medical facilities, etc., are required to take the network-related security measures described in this set of guidelines. For this reason, revision into Version 6.0 focused on the points of issue related to the plan of mid- and long-term continuation of discussions declared in Version 5.2, accompanied by review of the overall design.

○ Adjustments about the utilization of external contractors and services

- Views about risks and countermeasures based on the characteristics of cloud services
- Adjustments of responsibilities, etc., tailored to system types at medical facilities, etc.

○ Adjustments of views about information security

- Network perimeter defense type thought/zero trust network type thought
- Actions upon/against urgency such as disasters, cyber-attacks, and system disorders

○ Coping with new technologies and changes in systems/specifications

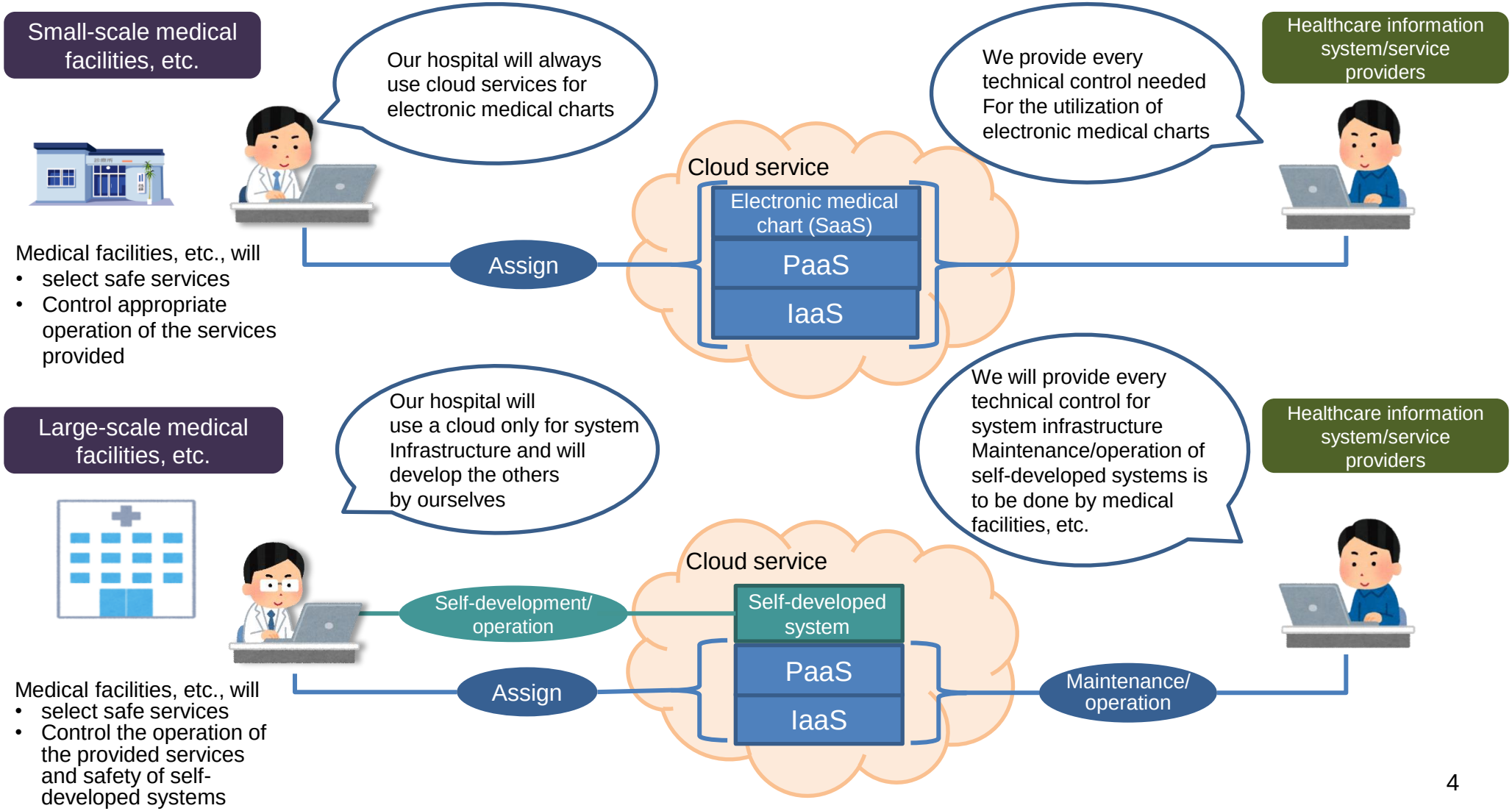
- Application to scenes requiring user authentication (eKYC utilization)
- Safety management measured for network apparatus, etc., needed for online qualification check introduction
- Possibility for new network technology (local 5G) utilization and scenes of its utilizations
- Trends in regulations (statutes, etc.) and technologies/specifications related to sharing/provision of healthcare information

○ Review of overall design

- Reconstituted into four chapters (Overview, Governance, Management, and Control; each consisting of tens of pages, overall review of the sentences, etc., of Version 5.2).
  *Chapter 6.12 (electronic signature) of Version 5.2 is kept unchanged from the current version, as a rule, because detailed discussions and adjustments had been made during its preparation.
- Adjustment of supportive documents such as overview, Q&S, terminology, and featured articles (for small-scale medical facilities, etc., cyber-security)

Adjustments about the utilization of outside contractors and services

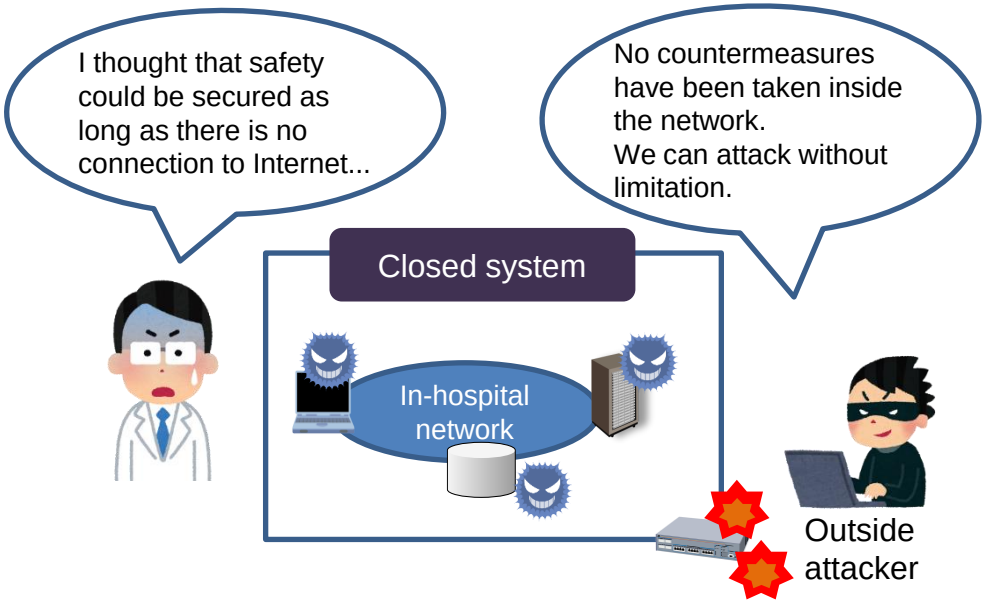
- Adjustments have been made on the responsibilities, etc., tailored to system types at medical facilities, etc., and on views about the risks and countermeasures based on the characteristics of cloud services.



Adjustments of views about information security -Network perimeter defense type thought/zero trust network type thought-

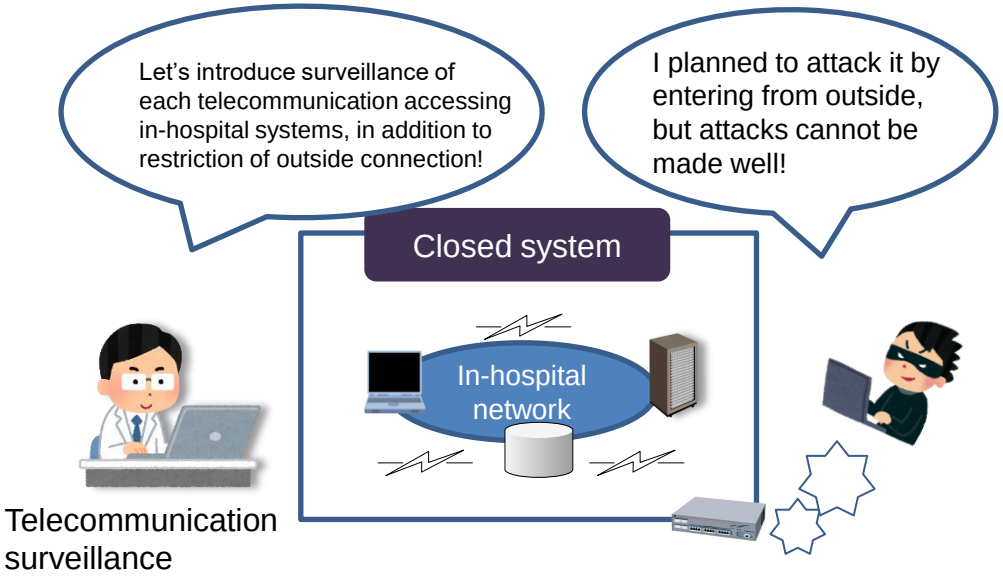
- Network-related adjustments were made and the usefulness of adopting zero trust network type thought was demonstrated.
- Taking measures by skillfully combining the perimeter defense type thought with the zero-trust thought was shown.

Following sophistication and other changes of cyber-attacks, the risk for invasion from outside has been elevated also for closed healthcare information systems.



If countermeasures relying only on perimeter defense are taken

Adoption of zero-trust thought will enable appropriate countermeasures also against individual invasion from outside.



If countermeasures adopting zero-trust thought are taken

Adjustments of views about information security -Actions upon/against urgency such as disasters, cyber-attacks, and system disorders-

- Actions upon/against urgency such as disasters, cyber-attacks, and system disorders have been adjusted and described.
- Concrete measures such as compliance with BCP and backup will be discussed and adjusted depending on the scenario.

Differences in views about backup depending on the scenario of urgency (examples)

When we say “actions upon disasters,” we should bear in mind that the details of actions upon disasters differ from those upon cyber-attacks or system disorders!

The view about service continuity at medical facilities, etc., also needs to be discussed for each scenario of urgency...

Backup in preparation of large-scale disasters need to be stored at multiple places in a dispersive manner...

Multiple non-rewritable backups are needed to deal with ransomware or the like...

When taking actions for disorders, actions enabling rapid recovery without system stoppage are needed.

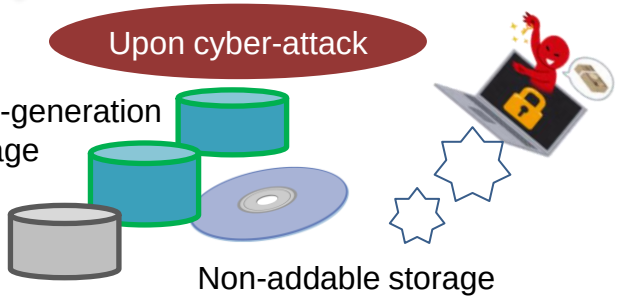
Necessity of measures corresponding to the scenario of urgency

Upon disaster

Dispersive storage

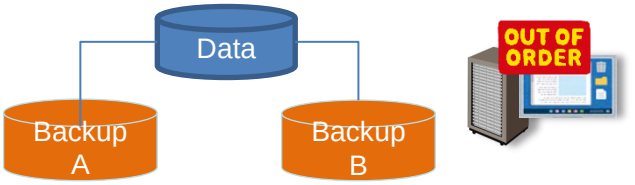
Upon cyber-attack

Multi-generation storage



Non-addable storage

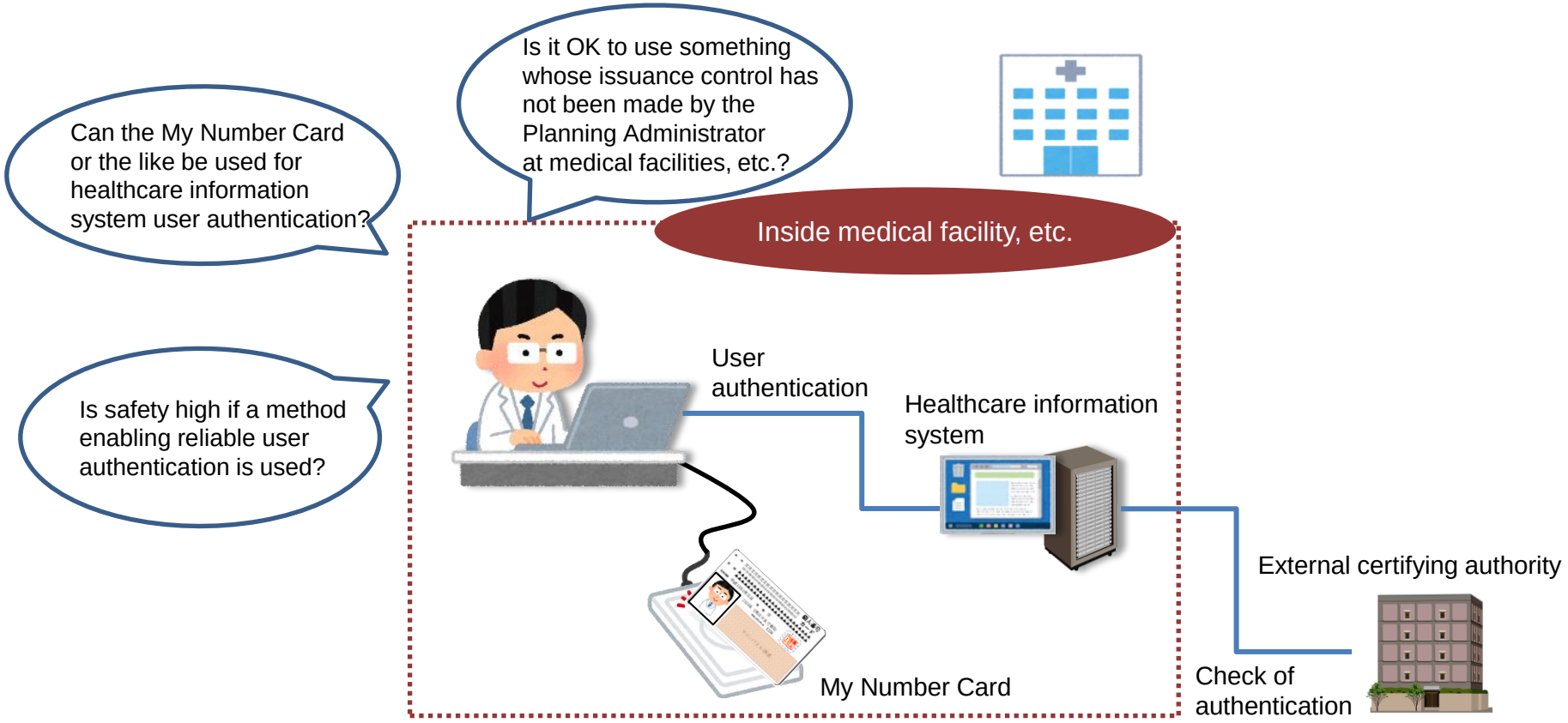
Upon system disorder



Duplicated use of system and storage apparatus

Coping with new technologies and changes in systems/specifications - Application to scenarios requiring user authentication (eKYC utilization) -

- Utilization of eKYC (electronic Know Your Customer), which has recently been used for various services as a means of only authentication, was discussed in scenarios requiring user authentication for healthcare information systems, and precautions or the like have been shown in the form of Q&A.



Precautions upon the utilization of eKYC as a means of authentication for healthcare information systems

eKYC：electronic Know Your Customer

Review of overall design

Bearing in mind the diverse scales, system configurations and service supply forms of medical facilities, etc., and positioning safe information asset management as a base, the overall design was adjusted from 3 viewpoints: i.e., Governance (decision making, policy setting, strategic planning), management (planning management, system operation) and control (methods of management, means of operation).

Overview

The knowledge needed for reading each chapter of the Guidelines and a fundamental overview of each chapter are summarized first of all.

- Objective of the Guidelines
- Applicable information/documents/systems
- Relationship to provisions of relevant statutes, etc., and the background
- Positioning of each chapter, table of contents, outline, etc.

Governance

Setting the organization's management policy and devising computerization strategy
Summarizing the views, relevant legal systems, etc., needed for the management team

- Importance of handled information and relevant statutes
- Responsibility and duties arising from information asset management and information system operation
- Information system utility and its safety management, etc.

Management

Summarizing the views and methodology for the management of and computerization control of information assets by system users, administrators, and service providers, on the basis of management policy and computerization strategy

- Information asset management system and responsibility boundary
- Risk assessment and countermeasures
- Management and supervision tailored to information type
- Measures upon/against urgency, etc.

Control

Summarizing the concrete views and technology for the realization of safe information asset management and system operation (e.g., views complying with relevant legal systems, their mounting methods, and utilization technologies)

- Technologies required under the Act on the Protection of Personal Information, e-Document Act, Electronic Signature Act, etc.
- Safety management measures, applicable technologies, etc., available for utilization by system users, clients, servers, infrastructure, etc.

Appendix

- Q&A
- Terminology
- Featured articles for small-scale medical facilities, etc. (e.g., clinics and pharmacies)
- Featured articles on cyber-security at medical facilities
- Revision of guidelines and history of changes in relevant statutes
- Relationship between guidelines and relevant statutes and its history of change
- Cross-reference table of each item between Version 5.2 and Version 6.0
- Correlation table of each item of each chapter in Version 6.0
- Checklist for cyber-security measures
- Flow chart of measures upon system disorder outbreak, etc.

Referring-recommended Parts of the Guidelines Tailored to Characteristics of Medical Facilities, etc. (1/2)

◆Referring to the Guidelines has been classified into the following 4 patterns corresponding to the presence/absence of fully-dedicated system operation staff and the form of healthcare information system introduced at medical facilities, etc.

	Healthcare information system owned and operated at medical facilities, etc. (on-premise type)	Healthcare information system operated without ownership at medical facilities, etc. (cloud service type)
Fully-dedicated system operation staff available	Ⅰ	Ⅱ
Fully-dedicated system operation staff unavailable	Ⅲ	Ⅳ

Note) Also at medical facilities, etc., where healthcare information such as medical charts is carried on paper and computerized systems are used only for medical accounting without involving healthcare information, the introduction of online qualification check, etc., system will cause access to the healthcare information because this system is linked to such information via the terminals, through linkage to the medical accounting system and so on.

At these medical facilities, etc., pattern II or IV referring to the Guidelines is recommended.

However, because the recommendable referring pattern can change depending on the entire system configuration, etc., it is advisable to confirm an optimum referring pattern with the healthcare information system/service provider as needed.

Referring-recommended Parts of the Guidelines Tailored to Characteristics of Medical Facilities, etc. (2/2)

<table>
<tr><th>Referring pattern</th><th>Governance</th><th>Management</th><th>Control</th></tr>
<tr><td>I</td><td rowspan="4">Referring to everything</td><td colspan="2">Referring to everything</td></tr>
<tr><td>II

Staff available and Cloud</td><td>Referring to everything, as a rule

*Depending on the healthcare information system configuration, inquiry to the information system service provider is advisable. If covered by the contract with the provider, the following may be simplified.
4.4 Arrangement of manuals or the like and various documents
5. Views about evidence in safety management
15. Management of technical measures
Matters to be complied: Other than 4), 6), 7), 8), and 13)</td><td>The following items should be referred to:
1 through 4, 6 through 8, 11, 12, 3

* Regarding the other items, inquiry should be made to the information system/service provider depending on the healthcare information system configuration.
If covered by the contract with the provider, simplification is possible.</td></tr>
<tr><td>III</td><td colspan="2">Referring to everything

*Referring recommended after replacing the term “staff” with “Planning Administrator” in each chapter.</td></tr>
<tr><td>IV

Staff unavailable and Cloud</td><td>Referring to everything, as a rule.

*Referring recommended after replacing the term “staff” with “Planning Administrator.”
*Depending on the healthcare information system configuration, inquiry to the information system service provider is advisable. If covered by the contract with the provider, the following may be simplified.
4.4 Arrangement of manuals or the like and various documents
5. Views about evidence in safety management
15. Management of technical measures
Matters to be complied: Other than 4), 6), 7), 8), and 13)</td><td>The following items should be referred to:
1 through 4, 6 through 8, 11, 12, 3

*Referring recommended after replacing the term “staff” with “Planning Administrator.”
*Regarding the other items, inquiry should be made to the information system/service provider depending on the healthcare information system configuration. If covered by the contract with the provider, simplification is possible.</td></tr>
</table>

Note) There is no need to refer to the item “Electronic signature for the name print/seal required under statutes” at medical facilities, etc., having not yet introduced any system using electronic signature and to the item “electronic conversion of healthcare information from a paper medium or the like” at medical facilities, etc., having not yet introduced electronic conversion of healthcare information from a paper medium or the like.