Measures for Further Reinforcement of Cyber-security at Medical Facilities
– Basic Policy for Cyber-security Measures at Medical Facilities From Now On –

12th Meeting of Health/Healthcare/Nursing Care Information Utilization/Application Council Working Group for Healthcare and Other Information Utilization/Application (September 5, 2022) Material 2-2

(1) Short-term cyber-security measures at medical facilities

1. Routine preventive measures

(1) Improving the training on cyber-security measures for medical facilities (2) Ensuring updating of apparatus shown/known to be vulnerable

(3) Establishing an information sharing system related to cyber-security in the medical field (ISAC) (4) Reinforcing the detecting function

(5) Conducting investigation of medical facilities using the G-MIS (Gathering Medical Information System)

2. Initial measures after outbreak of an incident

(1) Securing the coming-to-aid function upon incident outbreak (2) Ensuring reporting to relevant administrative entities or the like

3. Recovery works to restore routine clinical practices

(1) Ensuring preparation/management of backups (2) Setting the emergency dealing procedure and practicing its training

(2) Medium- and long-term cyber-security measures at medical facilities

1. Backup data encryption and concealing

2. SOC (Security Operation Center) establishment in public health/healthcare fields

Positioning of What Needs to be Followed by the Administrator at Each Medical Facility

Based on the past arguments at this WG, what needs to be followed by the administrator of each medical facility has been positioned as follows.

Past arguments at WG

○ Conventionally, security measures at medical facilities have been taken voluntarily at each facility on the basis of “Guidelines on Safety Management of Healthcare Information Systems.” Following recent increase in cyber-attacks, resulting in long-term suspension of healthcare at some facilities, an urgent investigation of hospitals revealed insufficiency of conventional measures to cope with such attacks. As a routine preventive measure, it is necessary to ensure updating of the apparatus shown to be vulnerable. (11th Meeting of Health/Healthcare/Nursing Care Information Utilization Council Working Group for Healthcare and Other Information Utilization/Application [May 27, 2022])

○ It is desirable to specify concrete measures for ensuring cyber-security at medical facilities and to perform inspection of medical facilities laying emphasis on providing support and advice, rather than imposing penalties. (11th Meeting of Health/Healthcare/Nursing Care Information Utilization Council Working Group for Healthcare and Other Information Utilization/Application [May 27, 2022])

○ The ministerial ordinance will be amended during fiscal 2022 to position what needs to be followed by the administrator at each medical facility. (12th Meeting of Health/Healthcare/Nursing Care Information Utilization Council Working Group for Healthcare and Other Information Utilization/Application [September 5, 2022])

Outline of amendment/Direction of countermeasures

○ Paragraph 2 will be added to the Enforcement Regulations on the Medical Care Act Article 14, so that taking measures needed to ensure cyber-security may be added to what needs to be followed by the administrator at each hospital, clinic, or midwife station.

○ Made public on March 10, 2023, Enforced on April 1 (plan)

○ ”Necessary measures” means appropriate measures related to security measures in general, including countermeasures against cyber-attacks, which should be taken with reference to “Guidelines on Safety Management of Healthcare Information Systems” (hereinafter called “Safety Management Guidelines”).

○ The Ministry of Health, Labour and Welfare (MHLW) will prepare a checklist of measures to be taken with priority among the matters described in the Safety Management Guidelines so that this may facilitate checks at each medical facility.

○ In addition, checking of the status of measures to ensure cyber-security will be positioned as an item of the on-site inspection rules based on the Medical Care Act Article 25 Paragraph 1.

◎Enforcement Regulations on the Medical Care Act (Order of the Ministry of Health and Welfare No. 50 1948)

Article 14　(skipped)
2　The administrator of a hospital, clinic, or birthing center must take the necessary measures to ensure cyber-security (meaning the cyber-security prescribed in Article 2 of the The Basic Act on Cyber-security (Act No. 104 of 2014)) so that there is no risk of significant hindrance to the provision of medical care.

*The underlined part has been added.

Checklist Concerning Cyber-security Measures at Medical Facilities (For checks at medical facilities during fiscal 2023)

	Check item	Check results (date)
Presence/absence of healthcare information system	A healthcare information system has been introduced and been operated. (If "No" there is no need of checking the subsequent items)	Yes・No (/)

During fiscal 2023

* Measures need to be taken so that you can answer (encircle) "Yes" to all of the following items during fiscal 2023.
* Regarding 2(2)and 2(3), entry is not needed if there is no contract concluded with any agent.
* If your answer to the first check is "No", please enter the target date of completion of the measures concerned taken during fiscal 2023.

	Check item	Check results (date)		
		First	Target date	Second
1 Organizational arrangement	(1) Healthcare Information System Safety Administrator has been appointed.	Yes・No (/)	(/)	Yes・No (/)
2 Healthcare information system management/operation	**The following measures have been taken on the healthcare information system in general.**			
	(1) Ledger control on servers, terminal PCs, and network apparatus has been implemented.	Yes・No (/)	(/)	Yes・No (/)
	(2) Checked with the vendor about presence/absence of apparatus utilizing the remote maintenance services.	Yes・No (/)	(/)	Yes・No (/)
	(3) Has instructed the vendor to submit healthcare information security disclosure documents (MDS/SDS) prepared by manufacturers/service providers.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on the servers.			
	(4) Access/utilization authorization has been set for each information category tailored to the job and duty of individual	Yes・No (/)	(/)	Yes・No (/)
	(5) Unnecessary accounts, such as the accounts of retired employees and inactive accounts, have been deleted.	Yes・No (/)	(/)	Yes・No (/)
	(6) Access logs have been managed.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on the network apparatus.			
	(7) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(8) Connection source restriction has been imposed.	Yes・No (/)	(/)	Yes・No (/)
3 Measures to prepare for incident outbreak	(1) A system chart for communication within the organization and to external related organizations (vendor, MHLW, police, etc.) is available.	Yes・No (/)		

○ Reference items (during fiscal 2024)

* Measures need to be taken so that you can answer (encircle) “Yes” to all of the following items during fiscal 2024.

	Check item	Check results (date)		
		First	Target date	Second
2 Healthcare information system management/ operation	**The following measures have been taken on the servers.**			
	(7) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(9) Unnecessary software and services working in the background have been stopped.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on terminal PCs.			
	(4) Access/utilization authorization has been set for each information category tailored to the job and duty of individual users.	Yes・No (/)	(/)	Yes・No (/)
	(5) Unnecessary accounts, such as the accounts of retired employees and inactive accounts, have been deleted.	Yes・No (/)	(/)	Yes・No (/)
	(7) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(9) Unnecessary software and services working in the background have been stopped.	Yes・No (/)	(/)	Yes・No (/)
3 Measures to prepare for incident outbreak	(2) The information needed for continuation of healthcare upon incident outbreak has been discussed, accompanied by implementation of data/system backup and confirmation of the restoration procedure.	Yes・No (/)	(/)	Yes・No (/)
	(3) A business continuation plan (BCP) based on the assumption of cyber-attacks has been devised or plans to be devised during fiscal 2024.	Yes・No (/)	(/)	Yes・No (/)

Checklist Concerning Cyber-security Measures at Medical Facilities (For checks by agents during fiscal 2023)

○ During fiscal 2023

* Measures need to be taken so that you can answer (encircle) “Yes” to all of the following items during fiscal 2023.

* If your answer to the first check is “No”, please enter the target date of completion of the measures concerned taken during fiscal 2023.

	Check item	Check results (date)		
		First	Target date	Second
1 Organizational arrangement	(1) An administrator on provision of healthcare information system, etc., has been appointed within the vendor.	Yes・No (/)	(/)	Yes・No (/)
2 Healthcare information system management/operation	**The following measures have been taken on the healthcare information system in general.**			
	(2) Presence/absence of impacts on the apparatus undergoing remote maintenance has been checked.	Yes・No (/)	(/)	Yes・No (/)
	(3) Has submitted healthcare information security disclosure documents (MDS/SDS) prepared by manufacturers/service providers to the medical facility.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on the servers.			
	(4) Access/utilization authorization has been set for each information category tailored to the job and duty of individual users.	Yes・No (/)	(/)	Yes・No (/)
	(5) Unnecessary accounts, such as the accounts of retired employees and inactive accounts, have been deleted.	Yes・No (/)	(/)	Yes・No (/)
	(6) Access logs have been managed.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on network apparatus.			
	(7) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(8) Connection source restriction has been imposed.	Yes・No (/)	(/)	Yes・No (/)

Reference items (during fiscal 2024)

* Measures need to be taken so that you can answer (encircle) “Yes” to all of the following items during fiscal 2024.

	Check item	Check results (date)		
		First	Target date	Second
2 Healthcare information system management/ operation	**The following measures have been taken on the servers.**			
	(8) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(9) Unnecessary software and services working in the background have been stopped.	Yes・No (/)	(/)	Yes・No (/)
	The following measures have been taken on terminal PCs.			
	(6) Access/utilization authorization has been set for each information category tailored to the job and duty of individual users.	Yes・No (/)	(/)	Yes・No (/)
	(7) Unnecessary accounts, such as the accounts of retired employees and inactive accounts, have been deleted.	Yes・No (/)	(/)	Yes・No (/)
	(8) Security patches (latest firmware and updated programs) have been applied.	Yes・No (/)	(/)	Yes・No (/)
	(10) Unnecessary software and services working in the background have been stopped.	Yes・No (/)	(/)	Yes・No (/)

Manual for the Checklist Concerning Cyber-security Measures at Medical Facilities —for medical facilities/agents— (1/2)

Manual for the Checklist Concerning Cyber-security Measures at Medical Facilities

—for medical facilities/agents—

This manual provides easily understandable commentary to the "Checklist Concerning Cyber-security Measures at Medical Facilities (hereinafter called simply "Checklist")." Referral to this manual is recommended when the checklist is utilized.

$—Introduction—

○ Cyber-attacks to medical facilities, etc., have recently tended to increase, and their threat has been intensifying day after day. It is essential for medical facilities to take appropriate measures so that leakage of patient's healthcare information and its illegal utilization via information security incidents (e.g., cyber-attacks) may be prevented. The healthcare information system has been playing a significant role in providing efficient and precise healthcare services. Also, from the viewpoint of supporting healthcare sustainability, it is required to utilize the healthcare information system under appropriate management.

○ Regarding the cyber-security measures at medical facilities, etc., it has been recommended to take appropriate measures with reference to the Guidelines on Safety Management of Healthcare Information Systems (hereinafter called "Guidelines") prepared by the MHLW. Of these measures, those to be taken preferentially by medical facilities have been summarized into this checklist.

So that the check using the checklist at medical facilities may become more feasible and that the checklist may be understandable easily even for individuals unfamiliar with cyber-security measures, this manual is designed to give commentary using plain language about the views underlying check items, methods of check, terminology, and so on.

○ Medical facilities and healthcare information system/service vendors (hereinafter called "vendors") are invited to routinely take valid cyber-security measures by utilizing this checklist while referring to this manual.

I How to use the checklist

1. Making the checklist ready for use
   - ○ The check by medical facilities should use the checklist "for check at medical facilities," and the check by vendors should use the checklist "for check by vendors." In cases where the medical facility has no contract-based vendors, the check with the checklist "for check by vendors" is unnecessary.
   - ○ Medical facilities are required to provide the vendors with the checklist "for check by vendors" and to request check of the status of measures by the agents. If multiple healthcare information systems are being utilized, the check with the checklist needs to be requested to each of the vendors providing such systems. The information about this program will be disseminated also to vendors.
2. How to fill in the checklist
   - ○ The status of implementation of each item is checked and either "Yes" or "No" is encircled, followed by entry of the date of check. If the answer of the first check is "No", please enter the target date for your implementation of the measures concerned during fiscal 2023. The checklist may be used either in paper form or in electronic medium.
   - ○ Each medical facility should attempt with linkage vendor(s) so that all check items may be answered with "Yes" during fiscal 2023 in the checklist "for check at medical facilities."
     (*) Entry into 2(2) and 2(3) is unnecessary for medical facilities with no contract-based vendors.
   - ○ For medical facilities with multiple contract-based vendors, check of part of the items of the checklist "for check by vendors" may be skipped depending on the contractual provisions. The checklist "for checks by vendors" has a column for entry of the vendor's name. This checklist needs to be recollected from each vendor by the medical facility.
3. Reference items
   - ○ Both the checklist "for checks at medical facilities" and the checklist "for checks by vendors" have reference items. Attempts should be made so that all reference items may be answered with "Yes" during fiscal 2024 in these checklists.
4. Others
   - ○ The results of checks using the checklist should be referred to at appropriate timing so that they may be utilized for routine implementation of measures.
   - ○ Inspection using the checklist should be done at least once a year.
   - ○ For vendors with no direct contract-based relationship to any medical facility, it is unnecessary to fill in the checklist "for checks by vendors."

—The checklist will be checked during on-site inspection —

The on-site inspection pursuant to the Medical care Act is intended to check implementation of measures needed to ensure cyber-security at hospitals, clinics, and mid-wife stations.

Inspection during fiscal 2023 will focus on entry of the date of the first check, answer, etc., in all items of the checklist "for checks at medical facilities" and that "for checks by vendors"(*). During this check, the original version will be checked concerning availability of the system chart for communication described in 3(1). So, please prepare it by the time of on-site inspection.

Reference items will not be checked during the on-site inspection in fiscal 2023.

It is advisable to check again the status of cyber-security measures using the checklist before the planned on-site inspection, in addition to making such a check routinely.

Medical facilities are required to recollect the checklist from their agents prior to the on-site inspection.

(*) For medical facilities with no contract-based vendor, checks 2(2) and 3(3) using the checklist "for checks at medical facilities" are not required.

II Commentary to each check item

Presence/absence of healthcare information system [For checks at medical facilities]

A healthcare information system has been introduced and been operated.

The healthcare information systems covered by this checklist include not only the systems for storage of healthcare information but also the information systems in general dedicated to handling of healthcare information (e.g., NHI billing computers, electronic medical chart systems, ordering systems). These include not only the systems provided by vendors but also the systems developed/established by medical facilities, etc.

If your answer to all of these items is “No”, there is no need to check the items given below.

▸Overview 2.3

1 System arrangement [For checks at medical facilities and checks by vendors]

(1) The Healthcare Information System Safety Administrator has been appointed.

At medical facilities, etc., the management team is required to appoint a Healthcare Information System Safety Administrator who directly implements safety management. The duties of the Healthcare Information System Safety Administrator include devising information security strategy and promoting information security measures including education and training. To ensure the validity of information security measures, it is desirable that one of the management team members assumes the office of Healthcare Information System Safety Administrator. Occasionally, however, this office is assumed concurrently by the Planning Administrator depending on the scale, organizational features, etc., of the medical facility.

Also, the agents are required to appoint an administrator related to the provision of healthcare information systems, etc.

(Terminology)

Planning administrator: Indicates the staff member in charge of practical operations related to safety management of healthcare information systems at medical facilities.

▸Business Management 3.1.2 (2)

3.2

2 Healthcare information system management/operation [For checks at medical facilities and checks by agents]

(Terminology)

Medical information system in general: Indicates the servers, terminal PCs and network apparatus.

Server: Indicates the computers providing information and services on the network, such as electronic medical chart serves and NHI billing computer servers.

Network apparatus: Indicates wireless LAN, routers, etc.

(1) Ledger control on servers, terminal PCs, and network apparatus has been implemented. (Healthcare information system in general)

To ensure the safety of information apparatus, etc., used for healthcare information systems, it is necessary to appropriately manage the location of information apparatus, etc., and the availability for use of such apparatus, etc. To this end, the Planning Administrator is required to prepare and manage the apparatus ledger covering the information apparatus, etc., used for the healthcare information systems possessed by a given medical facility and to check that such apparatus, etc., are in a condition suitable for utilization. The management team of medical facilities is required to receive reports on the management status periodically and to supervise the staff so that the status and responsibility for management are made clear. The information to be covered by ledger management includes the location, users, software/service version, and so on of information apparatus, etc.

(Terminology)

Location of information apparatus, etc.: Indicates the location actually installed, the network identification information, and so on.

(Supplements)

If ledger management has been conducted on the medical information systems possessed at your medical facility among the servers, terminal PCs, and network apparatus, please encircle “Yes” in 2(1) of the checklist “for checks at medical facilities.”

▸Business Management 1.2.1< Responsibility for management> (2)

▸Planning management 9.1

● Example of apparatus ledger

Control No.	Manufacturer	OS	Software	Software version	IP address	Computer name	Installed location	User	Registration date	Status	Explanation
001	Company A	Win11	XX Electronic Medical Chart	2.0	192.168. X.X	PC 1 in Room 1	Room 1	Physician a (Department XX)	Dec 1, 2020	Under use	
002	Company A	Win11	XX Electronic Medical Chart	1.2	192.168. X.X	PC 2 in Room 1	Room 1	Physician b (Department XX)	Dec 1, 2020	Out of use	Maintenance
003	Company A	Win8	XX Electronic Medical Chart	2.0	192.168. X.X	PC 1 in Room 2	Room 2	Physician c (Department XXX)	Oct 1, 2014	Under use	
004	Company B	Win11	XX Management System	5.0.1	192.168. X.X	PC 1 in Room 3	Room 3	Physician a (Department XX), Physician b (Department XX), Physician c (Department XXX)	Aug 1, 2021	Under use	

Support and Investigation Program for Healthcare Information Security Training and Initial Measures upon Cyber-security Incident Outbreak (Fiscal 2022)

13th Meeting of Health/Healthcare/Nursing Care Information Utilization/Application Council Working Group for Healthcare and Other Information Utilization/Application (December 15, 2022) Material 3 (partially modified)

Background

In view of intensifying threats against healthcare cyber-security in recent years, support, etc., is provided to training for medical facilities and initial measures upon the outbreak of cyber-security incidents within the framework of the MHLW Program in Fiscal 2022.

Program Overview

(1) Implementation of training for medical facilities about cyber-security measures

: Providing training tailored to different strata of medical facility staff members (beginners, management team, system security administrators, etc.)

(2) Continuing educational support

: Preparation, collection, and publication of educational contents useful in training by Healthcare Information System Safety Administrator

(3) Investigation of routine cyber-security incident dealing procedure and proposal of existing BCP review

: Assuring appropriate flow of actions dealing with an outbreak of cyber-security incidents and proposal of BCP (Business Continuity Plan)

(4) Support to initial measures of medical facilities upon an outbreak of cyber-security incidents

: Support is provided to initial measures for the purpose of identifying the cause at the medical facility facing an outbreak of a cyber-security incident and enabling early restoration of clinical practices

Assignee

Software Association of Japan

: A general incorporated association consisting of about 700 companies of software products and aimed at contributing to healthy industrial development and national life improvement through the business activities for advances in software industry.

(Major activities related to cyber-security)

- Implementing seminars/training related to software and cyber-security
- Creation and operation of cyber-security volunteer system
- Exchanging and disseminating information related to cyber-security

Re: Ransomware Infection at the Osaka Prefectural Hospital Organization Osaka General Medical Center

13th Meeting of Health/Healthcare/Nursing Care Information Utilization/Application Council Working Group for Healthcare and Other Information Utilization/Application (December 15, 2022) Material 3 (partially modified)

Incident Overview

Early in the morning of October 31, 2022 (Monday), the Osaka Prefectural Hospital Organization Osaka General Medical Center (hereinafter called "Osaka General Medical Center") received a cyber-attack with ransomware, resulting in the encryption of files which made it impossible to use the electronic medical charts. The investigation made by the initial measure supporting team (Software Association of Japan), sent from the MHLW, revealed a high probability that the infection had occurred via the system of the meal service provider to which out-of-hospital cooking had been assigned.

At the Osaka General Medical Center, acceptance of new outpatients has been stopped after this incident, but treatments of high urgency and surgery are being provided continuously. Patients with low levels of urgent care were discharged home temporarily or referred to surrounding hospitals, thus avoiding influence on the lives of patients and so on. No leak of personal information has yet been found. (As of December 12)

(Reference Information) Osaka General Medical Center
Number of beds: 865 (831 general beds, 34 psychiatric beds)
Hospital functions: Core disaster-dealing hospital, high-level critical care center, regional perinatal maternal & child care center, regional pediatric care center, regional healthcare support hospital, core regionally linked cancer care hospital, etc.
Total annual number of inpatients: 223,000 (646/day)
Total annual number of outpatients: 295,000 (1,268/day)

Chronological course

October 31 (Monday): Outbreak of incident In response to the request of a support to initial measures from the Osaka General Medical Center, the MHLW sent an initial measure support team. In the evening of the same day, the incident was made public at a press conference.
November 4 (Friday): Scheduled surgery was partially resumed.
November 7 (Monday): One week after the outbreak, the current status of the incident and the plan for restoration were made public at a press conference. It was announced that the highly probable route of the infection was the VPN apparatus installed at the meal service provider.
November 10 (Thursday): Referring to the electronic medical charts was resumed partially under tentative environments, accompanied by resumption of acceptance of patients for tertiary critical care and part of critical pediatric care.
November 17 (Thursday): Referring to the electronic medical charts at the outpatient critical care units was resumed under tentative environments, enabling acceptance of patients for critical care in general.
December 12 (Monday): The electronic medical chart system re-establishment was completed and began to be put into operation in steps under regular environments. Each ordering system is planned to be resumed in steps.
January of next year: Full-scale system resumption planned

Measures taken by MHLW

1. In response to the request from the medical facility, the MHLW sent experts, thus providing support to initial measures such as identification of the cause of infection and instruction of what is to be done.
2. On November 10, an alert was issued to nationwide medical facilities, calling for attention to the need of reinforcing cyber-security measures. (Reference 3)

Clerical Communication dated November 10, 2022
Re: Reinforcing cyber-security measures at medical facilities, etc. (alert)
(Excerpts)

1 Check of the overall risk for the supply chain

The security control system at the relevant service providers/traders needs to be checked and the points of network connection to each relevant service provider/trader (particularly the points of connection to the Internet) should be placed under control, accompanied by implementation of countermeasures against vulnerability.

2 Risk-reducing measures

・The password should be changed into a more complex one, and use of the same password for multiple systems should be avoided. Unnecessary accounts should be deleted and the authorization for access should be checked. Multi-factor authentication should be utilized to reinforce user authentication.
・The status of possession of information assets (including IoT apparatus) should be checked.
・Since the vulnerability of the gateway apparatus which controls connection to the Internet (including VPN apparatus) has the potential of being misused for attacks, security patches (latest firmware, updated programs, etc.) should be applied without delay.
・Regarding the vulnerability whose misuse has been reported, it is necessary to confirm complete implementation of developed-recommended measures such as log checks and password changes.
・Appropriate Internet-based access restriction should be imposed for the VPN apparatus control interface.
・Files attached to E-mails should not be opened carelessly. Clicking on the URL contained in the E-mails should be avoided. Upon receipt of suspicious E-mails, appropriate notification and consultation steps should be taken, followed by dissemination of the fact across the organization.

3 Early detection of incidents

・Various logs of servers, etc., should be checked. (E.g., presence/absence of traces of massive log-in failures)
・Telecommunication surveillance/analysis and access control should be inspected again. (E.g., presence/absence of access to suspicious websites)

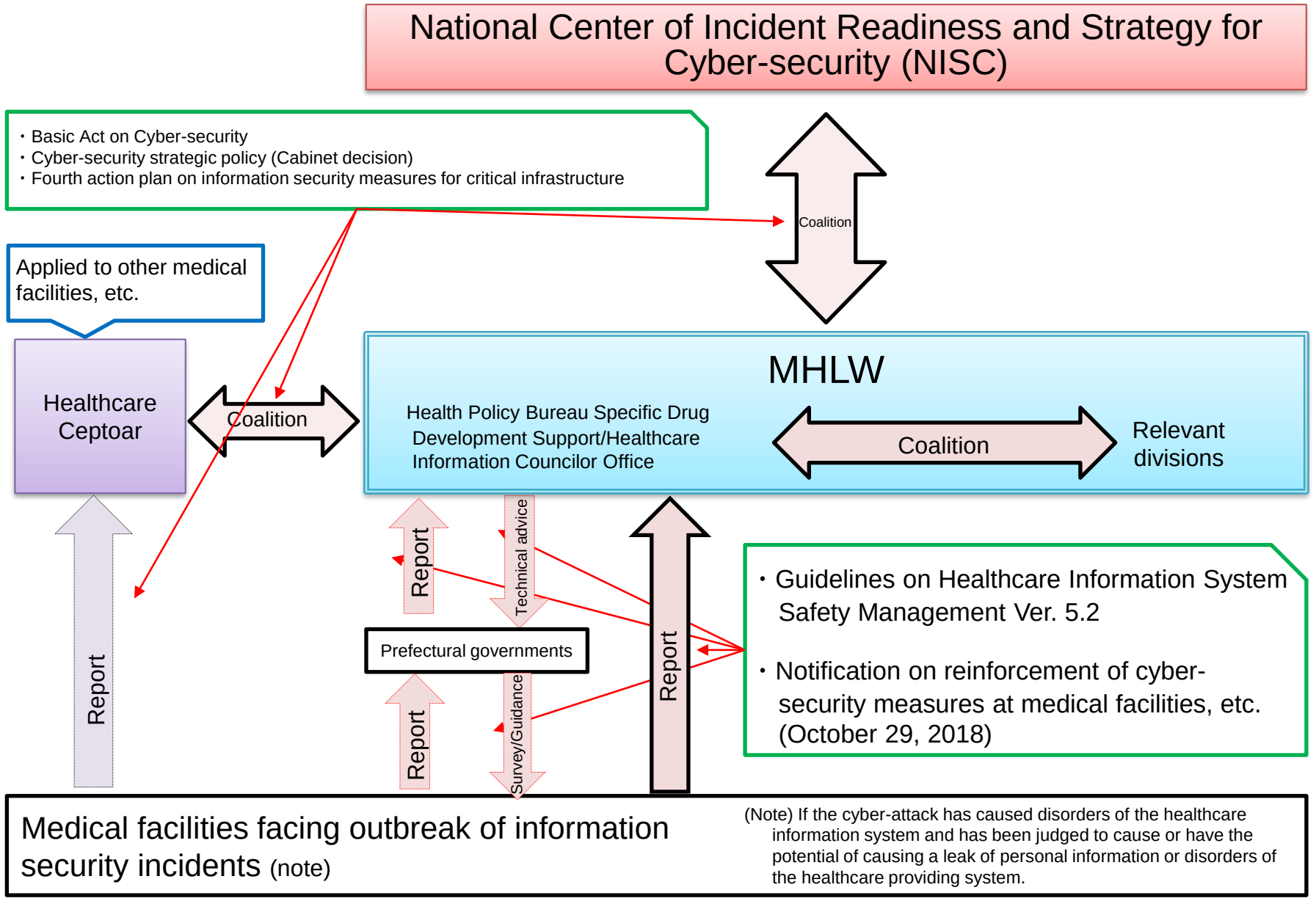
4 Appropriate countermeasures/recovery upon outbreak of incidents

・A business continuity plan should be devised, based on assumption of outbreak of serious system disorders following a cyber-attack.
・Data backup implementation and recovery procedure should be checked in preparation for data loss, etc.
・The procedure for dealing with incidence detection should be checked in preparation for incident outbreak, and the systems for communication with relevant outside organizations within one's own organization and so on should be arranged.
・Upon outbreak of an incident or its suspicion, contact with the relevant entities, such as the MHLW, should be made immediately.

5 Dealing with demands to money payment

Paying money to the cyber-attacker in response to its demand is equivalent to providing support to the criminal organization and should be strictly avoided from the following points of view.
・There is no guarantee that payment of money can stop disclosure or sale of the illegally picked out data or that the encrypted data can be restored to normal by payment of money.
・Once money has been paid, there is a higher probability of receiving another attack or another demand for payment.

Measures upon Outbreak of Cyber-security Incidents at Medical Facilities



Information Sharing System (Outline of CEPTOAR)

Name	**Healthcare CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis, and Response)**
Secretariat	**Japan Medical Association Information System Division**
Outline	**1. Functions** "Healthcare CEPTOAR" has been founded as an organization with "information sharing/analysis functions" in the field of healthcare for the purpose of facilitating appropriate sharing/analysis of the information provided from the Government, etc., among healthcare providers and so on, with the ultimate goal of improving the maintenance/recovery capabilities of healthcare providers through prevention of IT disorders, prevention of IT disorder expansion, promotion of rapid recovery from IT disorders, and prevention of IT disorder recurrence by analysis/verification of factors causing IT disorders. Adjustments toward improvement will be continued within the present framework concerning the information circulation systems, etc., described below in (1) through (3). (1) Information sharing and coalition for prevention of IT disorders, prevention of IT disorder expansion, promotion of rapid recovery from IT disorders, and prevention of IT disorder recurrence through analysis/verification of involved factors, etc., related to healthcare services. (2) Supply of the information provided from the Government, other CEPTOARs, and so on to members of this organization. (3) Information sharing about matters related to the information provided from the Government, other CEPTOARs, and so on. **2. Composition** ● Japan Medical Association, Japan Dental Association, Japan Pharmaceutical Association, Japanese Nursing Association (information sharing function) ● Japanese Association of Medicalcare Corporations, Japan Psychiatric Hospitals Association, Japan Hospital Association, All Japan Hospital Association (information sharing function) ● Japan Municipal Hospital Association, Japanese Association of Private Medical Schools, Japan Association of Medical and Care Facilities, Japan Organization of Occupational Health and Safety, Association of Japanese Social Medical Corporations, National Hospital Organization, Japan Community Health Care Organization, Japan Association of Rehabilitation Hospital and Institution, Japanese Association of Hospitals for Community-based Care, University Hospital Council (information sharing function) ● Japanese Association of Healthcare Information Systems Industry as an observer (information sharing function) **3. Characteristics** ● A practically valid system based on conventional activities and current organizations ● A characteristic of healthcare field lies in that a system for sharing information with prefectural governments is indispensable in establishing and maintaining the healthcare provision system. So, coalition with prefectural governments to an extent not seen in any other field is needed.