Notice to Users

· Translations

Only the original Japanese texts of the provisions and regulations are official texts, and the translations are to be used solely as reference materials to aid in the understanding of Japanese provisions and regulations.

Regulations for the Protection of Personal Information

April 1, 2015

Regulation No. 27

Revisions: Regulation No. 33 of January 1, 2016

Regulation No. 50 of April 1, 2016

Regulation No. 89 of June 30, 2017

Regulation No. 106 of October 10, 2018

Regulation No. 33 of March 27, 2020

Table of Contents

Chapter 1: General provisions

Section 1: Common provisions

(Purposes)

Article 1.

The purposes of these regulations are to stipulate the matters that are necessary for appropriate management of the personal information possessed by the Japan Agency for Medical Research and Development (hereinafter referred to as “AMED”) and thereby strive for appropriate and smooth operation of AMED’s work while protecting individuals’ rights and interests.

(Definitions)

Article 2.

In these regulations, the definitions of the terms stated in each of the items below will be according to the stipulations of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003; hereinafter referred to as the “Act”) and Article 2 of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the “Numbers Act”), as well as the stipulations of each relevant item.

(1) Department or office This refers to a department or office stipulated in Article 10 of the Organization Regulations (Regulation No. 4 of 2015).
(2) Division: This refers to a division stipulated in Article 11 through Article 17 of the Organization Regulations.
(3) Board member or employee: This refers to a board member or employee of AMED or a person who the general personal information protection manager has recognized as a person who should comply with these regulations.
(4) Overseas office: This refers to an overseas office stipulated in Article 15-3.2 of the Organization Regulations.
(5) Director of an overseas office: This refers to a person stipulated in Article 4 of the Notification Concerning the Main Handled Areas for Overseas Offices (Notification No. 23 of 2016).

(Scope of application)

Article 3.

Handling of personal information, specific personal information, personal information files, and specific personal information files possessed by AMED will follow the Act, the Numbers Act,

guidelines related to measures for appropriate management of personal information held by incorporated administrative agencies, and these regulations.

(Duties of board members and employees)

Article 4.

Board members and employees must, in accordance with the intent of the Act and the Numbers Act, handle the possessed personal information and possessed specific personal information (hereinafter referred to as the "Possessed Personal Information") by following the stipulations of related laws, ordinances, and established rules and the instructions of the general personal information protection manager, the assistant general personal information protection manager, and the personal information protection manager.

Section 2: Management system for the Possessed Personal Information

(General personal information protection manager)

Article 5.

1. AMED will have one general personal information protection manager, and the Executive Director will serve in that position.
2. There will be one assistant general personal information protection manager, and the managing director of the Department of General Affairs will serve in that position. There will also be one assistant to the assistant general personal information protection manager, and the director of the Division of General Affairs will serve in that position.
3. There will be one chief personal information protection manager in a department or office, and the managing director of the relevant department or office will serve in that position.
4. There will be one personal information protection manager in a division or overseas office, and the director of the relevant division or overseas office will serve in that position.
5. There will be one person in charge of personal information protection in a division or overseas office, and the employee in charge of general management who was designated by the personal information protection manager will serve in that position. After designating the person in charge of personal information protection, the personal information protection manager must promptly report that person's name and position to the assistant general personal information

protection manager.

6. AMED will have a person responsible for personal information audits, and the managing director of the Office of Audit will serve in that position.

(Duties of the general personal information protection manager)

Article 6.

1. The general personal information protection manager will have general control over clerical matters related to management of the Possessed Personal Information at AMED.
2. The assistant general personal information protection manager will receive orders from the general personal information protection manager and provide assistance for the clerical work conducted by the general personal information protection manager. The assistant to the assistant general personal information protection manager will provide assistance for the clerical work conducted by the assistant general personal information protection manager.
3. The chief personal information protection manager will be in charge of clerical work related to management of personal information in the relevant department or office.
4. The personal information protection manager will conduct duties to ensure appropriate management of the Possessed Personal Information in the relevant division or overseas office. In the event that the Possessed Personal Information will be handled by an information system, the personal information protection manager will cooperate with the manager of the relevant information system and conduct those duties.
5. The person in charge of personal information protection will receive orders from the personal information manager, assist the personal information protection manger, and handle clerical work related to management of the Possessed Personal Information in the relevant division or overseas office.
6. The person responsible for personal information audits will conduct duties to audit the state of management of the Possessed Personal Information.
7. The personal information protection manager will designate some employees (hereinafter referred to as the “Persons in Charge of Handling Clerical Work”) for handling personal numbers and specific personal information (hereinafter referred to as the “Specific Personal Information) and will designate that person’s role and the scope of the Specific Personal Information that will be handled by each Person in Charge of Handling Clerical Work.

(Committee for appropriate management of the Possessed Personal Information)

Article 7.

When the general personal information protection manager recognizes that it is necessary in order to make a decision, contact, or coordination for an important matter related to the management of AMED's Possessed Personal Information, the person will establish a committee that has related board members and employees as its constituent members and have the committee hold meetings regularly or as necessary.

(Education and training)

Article 8.

1. For board members and employees who engage in handling the Possessed Personal Information, the general personal information protection manager will conduct activities to raise awareness and other necessary education and training in order to strive to deepen their understanding about handling the Possessed Personal Information and increase their awareness related to protection of personal information and specific personal information (hereinafter referred to as the "Personal Information").
2. For board members and employees who engage in clerical work related to management of information systems that handle the Possessed Personal Information, the general personal information protection manager will conduct the necessary education and training in relation to the management and operation of and security measures for information systems for the purpose of the appropriate management of the Possessed Personal Information.
3. For the personal information protection manager and the person in charge of personal information protection, the general personal information protection manager will provide education and training for the purpose of appropriate management of the Personal Information in the division or at the site of the overseas office.
4. For board members and employees in the relevant division or overseas office, the personal information protection manager must implement the necessary measures, such as giving them opportunities to participate in the education and training conducted by the general personal information protection manager, for the purpose of appropriate management of the Possessed Personal Information.

Chapter 2: Handling of the Personal Information

Section 1: Acquisition and use of the Personal Information

(Restriction of possession of the Personal Information)

Article 9.

1. Possession of the Personal Information by board members and employees will be limited to cases in which it is necessary for performing work stipulated in laws and ordinances, and to the extent possible, they must specify those purposes of use.
2. Board members and employees may not possess the Personal Information beyond the scope that is necessary for accomplishing the purposes of use (hereinafter referred to as the "Purposes of Use") that were stipulated based on the provisions of the previous clause.
3. In the event that a Purpose of Use will be changed, the board member or employee may not go beyond the scope that will be reasonably recognized as having equivalent relevance with the Purpose of Use before the change.

(Clear indication of the Purposes of Use)

Article 10.

Except in the cases stated below, when a board member or employee will acquire the Personal Information of the relevant person that was directly recorded by that person in a document, the person must clearly indicate the Purposes of Use for that information to that person in advance.

(1) When there is an urgent necessity in order to protect a person's life, body, or assets
(2) When there is a possibility that clearly indicating the Purposes of Use to the relevant person will result in harming the life, body, assets, or other rights or interests of the relevant person or a third party
(3) When there is a possibility that clearly indicating the Purposes of Use to the relevant person will result in hindering the appropriate performance of clerical work or business conducted by a national government organization, an incorporated administrative agency, or a local government
(4) When it can be recognized from the state of acquisition that the Purposes of Use are clear

(Appropriate acquisition)

Article 11.

1. Board members and employees may not acquire the Personal Information by using falsehoods or other fraudulent means.
2. When it is necessary for the purpose of handling clerical work that handles specific personal information, the Persons in Charge of Handling Clerical Work can ask the relevant person to provide the personal number (including personal numbers of people who belong to the same household as that person).
3. When the Persons in Charge of Handling Clerical Work will receive provision of a personal number from the relevant person based on the previous clause, the person must verify the person's identity according to the stipulations of laws and ordinances.
4. Except in cases of Article 11.2, the Persons in Charge of Handling Clerical Work may not ask the relevant person to provide a personal number.

(Ensuring accuracy)

Article 12.

Board members and employees must, within the scope that is necessary for accomplishing the Purposes of Use, strive to ensure that the Possessed Personal Information matches past or current facts.

(Ensuring safety)

Article 13.

Board members and employees must strive to ensure the safety of the Possessed Personal Information based on the stipulations of these regulations.

(Use and provision of personal information for purposes other than the Purposes of Use)

Article 14.

1. In the event that the personal information protection manager intends to use or provide possessed personal information for a purpose other than the Purposes of Use, based on Article 9.1 or Article 9.2 of the Act, in principle, the person must notify the assistant general personal

information protection manager in advance.

2. In the event that the personal information protection manager will provide possessed personal information based on Article 9.1 or Article 9.2.3 and Article 9.2.4 of the Act, in principle, the person will, for the party that will receive provision of that possessed personal information, confirm a document concerning the matters stated below related to that possessed personal information for which use is intended.
   (1) The recorded scope and the recorded matters
   (2) The Purposes of Use
   (3) The form of use
   (4) The law or ordinance that is the basis for the work for conducting use
   (5) Other matters that are recognized as necessary
3. The personal information protection manager will ask the party that received the provision under the previous clause to implement the measures for ensuring safety, and when the personal information protection manager recognizes that it is necessary, the person will conduct practical investigation, either before provision or as necessary, confirm the state of measures and record those results, and implement the measures for requesting improvements.

(Restriction of provision of specific personal information)

Article 15.

Except in cases that are clearly stated in a limited way in the Numbers Act, the personal information protection manager may not provide specific personal information.

(Restriction of use of specific personal information)

Article 16.

1. The Persons in Charge of Handling Clerical Work may not use specific personal information for anything other than the clerical work stipulated in the Numbers Act.
2. Irrespective of the provisions of the previous clause, in the event that it is necessary in order to protect a person’s life, body, or assets, when the relevant person has agreed or when it can be recognized that it will be difficult to obtain the relevant person’s agreement, and when it can be recognized that there is no possibility of infringing the rights or interests of the relevant person or a third party by using the relevant specific personal information for a purpose other than the

Purposes of Use, the Persons in Charge of Handling Clerical Work can use specific personal information for a purpose other than the Purposes of Use.

3. The provisions of the previous clause will not hinder the application of laws or ordinances that restrict the use of specific personal information.

(Measures for cases of consignment of work)

Article 17.

1. In the event that the work related to the handling the Possessed Personal Information will be outsourced (including contracting; hereinafter the same), the personal information protection manager must implement the necessary measures so that a party that does not have the abilities to appropriately manage the Personal Information will not be selected, such as checking whether or not the party being considered for that consignment has internal provisions for handling the Personal Information.
2. An agreement related to consignment will state the matters stated below, and written confirmation will be conducted concerning the necessary matters, such as the implementation system and management by the people responsible and the people engaged in work at the consigned party, and matters related to inspections concerning the state of management of the Personal Information.
   (1) Matters related to obligations for maintaining confidentiality related to the Personal Information and prohibiting its use for anything other than its purposes
   (2) Matters related to the restriction of reconsignment (including cases in which the re-consigned party is a subsidiary (refers to a subsidiary stipulated in Article 2.1.2 of the Companies Act (Law No. 86 of 2005)) of the consigned party; the same in this item and in Article 17.4 and Article 17.6) (in the agreement with the consigned party, it is to be clearly stated that the matters that will be required of the re-consigned party for reconsignment should be required in the same way even if the re-consigned party is a subsidiary) or conditions for reconsignment, such as advance approval
   (3) Matters related to the restriction of the duplication of the Personal Information
   (4) Matters related to ensuring the safety of the Personal Information
   (5) Matters related to the handling in times when a case, such as a leak of the Personal Information occurs

(6) Matters related to elimination of the Personal Information and return of media when consignment ends

(7) Agreement cancellation, liability for damage compensation, and other necessary matters for cases in which there was a violation

3. In the event that work related to the handling of the Possessed Personal Information will be consigned to an external party, confirmation will be conducted in principle by on-site inspection at least once a year, concerning the management system, the implementation system, and the state of management of the Personal Information at the consigned party, in accordance with the confidentiality, content, and amount of the Possessed Personal Information related to the work that is consigned.

4. In the event that work related to the handling the Possessed Personal Information will be reconsigned by the consigned party, the consigned party will be made to implement the measures of Article 17.1 and Article 17.2, and the measures of Article 17.3 will be conducted either through the consigned party or by the consignor itself, in accordance with the confidentiality and other aspects of the content of the Possessed Personal Information related to the work that will be reconsigned. The same will also apply in cases in which the reconsigned party will conduct re-reconsignment for work related to the handling of the Possessed Personal Information and thereafter.

5. In the event that all or a portion of clerical work related to personal numbers will be consigned, confirmation will be conducted in advance concerning whether or not measures that are equivalent to the safety management measures that AMED should carry out based on the Numbers Act will be implemented by the consigned party. In addition, when consignment is conducted, the necessary and appropriate supervision will be conducted so that measures that are equivalent to the safety management that AMED should carry out will be implemented by the party that receives consignment.

6. When a party that received consignment of all or a portion of clerical work related to personal numbers will conduct reconsignment, that party will confirm the fact that efforts are being made for appropriate safety management of the specific personal information that will be handled for the clerical work related to personal numbers that will be consigned, and the party will then make a judgment about consent or refusal of reconsignment.

7. In the event that the Possessed Personal Information will be provided or work for the Possessed

Personal Information will be consigned, consideration will be given to that content, such as the Purposes of Use at the party receiving provision, the content of the work that will be consigned, and the confidentiality of the Possessed Personal Information, and measures to make the information anonymous, such as replacing names with numbers, will be taken as necessary, from the perspective of reducing the risk of damage occurring due to leaks.

(Measures for cases in which dispatch of dispatched workers will be received)
Article 18.
In the event that work related to the handling of the Possessed Personal Information will be conducted by a dispatched worker, the personal information protection manager must clearly state, in the dispatched worker agreement, matters related to the handling of personal information, such as the obligation of maintaining confidentiality.

Section 2: Handling of the Possessed Personal Information

(Restriction of access)
Article 19.

1. The personal information protection manager must, in accordance with the confidentiality and other aspects of the Possessed Personal Information's content (consideration is to be given to the ease of identifying individuals (the degree to which people have been made anonymous), whether or not there is personal information that requires special care, and the nature and degree of damage that could be incurred if a leak occurs; hereinafter the same), limit the scope and content of authority of the board members and employees who will access the relevant Possessed Personal Information to the minimum number of board members and employees who are necessary in order to accomplish the Purposes of Use for that information.
2. Board members and employees who do not have authority for access may not access the Possessed Personal Information.
3. Even in the event that a board member or employee has the authority to access, the person may not access the Possessed Personal Information for a purpose other than a work-related purpose.

(Restriction of duplication)

Article 20.

Even in the event that a board member or employee will handle the Possessed Personal Information for a work-related purpose, the personal information protection manager will, for the actions stated below and in accordance with the confidentiality and other aspects of the content of the relevant Possessed Personal Information, limit the cases in which it will be possible to conduct such actions, and the board member or employee will conduct the actions by following the instructions of the personal information protection manager.

(1) Duplication of the Possessed Personal Information
(2) Sending the Possessed Personal Information
(3) Sending or taking media in which the Possessed Personal Information is recorded to an external party
(4) Other actions that have a possibility of hindering appropriate management of the Possessed Personal Information

(Correction of errors)

Article 21.

Excluding cases in which the relevant error can be recognized as clearly being insignificant, in the event that a board member or employee has discovered an error in the content of the Possessed Personal Information, the person must follow the instructions of the personal information protection manager to make corrections.

(Management of media)

Article 22.

Board members and employees must follow the instructions of the personal information protection manager to store media in which the Possessed Personal Information is recorded in the stipulated places and must store and lock them in a fireproof safe when it is recognized as necessary.

(Disposal)

Article 23.

In the event that the Possessed Personal Information or a medium in which the Possessed Personal Information is recorded (including anything installed inside a terminal or server) has become

unnecessary, the board member or employee must follow the instructions of the personal information protection manager to eliminate the relevant information or dispose of the relevant medium by using a method by which it is not possible to restore or decipher the Possessed Personal Information.

Section 3: Ensuring the safety of information systems

(Control of access)

Article 24.

1. In accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system), the personal information protection manager must implement the measures that are necessary for controlling access, such as setting a function that uses a password (refers to a password, IC card, or bio-information; hereinafter the same) to discern authority (hereinafter referred to as the "Authentication Function").
2. When the personal information protection manager will implement the measures of the previous clause, the person must prepare stipulations related to management of the password (including regular reconsideration or reconsideration as necessary for those stipulations) and implement the measures that are necessary for preventing the reading of the password.

(Access record)

Article 25.

1. For the Possessed Personal Information (limited to matters that are handled by an information system), the personal information protection manager must, in accordance with the confidentiality and other aspects of the content, record the state of access to the relevant Possessed Personal Information, save that record (hereinafter referred to as the "Access Record") for a certain period, and implement the measures that are necessary for regularly, or whenever necessary, analyzing the Access Record.
2. The personal information protection manager must implement the measures that are necessary for preventing alteration, theft, or improper elimination of the Access Record.

(Monitoring the state of access)

Article 26.

In accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system) and in accordance with its amount, the personal information protection manager must implement the measures that are necessary for monitoring inappropriate access to the relevant Possessed Personal Information, such as setting a function by which a warning is displayed if information of a certain amount or larger that contains or possibly contains the Possessed Personal Information was downloaded from an information system and regularly checking that function.

(Setting manager authority)

Article 27.

The personal information protection manager must, in accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system), implement the necessary measures, such as minimizing the privileges of the authority of managers of information systems, for the purposes of minimizing damages when those privileges are dishonestly stolen and preventing unauthorized operation from within the organization.

(Prevention of unauthorized access by external parties)

Article 28.

In order to prevent unauthorized access from external parties to information systems that handle the Possessed Personal Information, the personal information protection manager must implement the necessary measures, such as conducting routing control by setting a firewall.

(Prevention of leaks caused by malicious programs)

Article 29.

In order to prevent leaks, loss, or damage of the Possessed Personal Information (limited to matters that are handled by an information system) due to malicious programs, the personal information protection manager must implement the necessary measures (including always maintaining the most recent state of software that was introduced) for resolving vulnerabilities that were unveiled in relation to software and preventing infection by malicious programs that were ascertained.

(Processing the Possessed Personal Information on an information system)

Article 30.

In the event that a board member or employee will conduct duplication of the Possessed Personal Information in order to conduct handling, such as temporary processing, the matters that are subject will be limited to the minimum number that are necessary, and after the handling ends the information that became unnecessary will be promptly eliminated. The personal information protection manager will, in accordance with the confidentiality and other aspects of the content of the relevant Possessed Personal Information, conduct focused checks as necessary concerning the state of implementation of elimination.

(Encryption)

Article 31.

1. The personal information protection manager must implement the measures that are necessary for encryption in accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system).
2. For the actions stated below, board members and employees must conduct encryption for the Possessed Personal Information (limited to matters that are handled by an information system).
   (1) Saving the Possessed Personal Information in a shared drive
   (2) Taking a medium in which the Possessed Personal Information is recorded outside the organization
   (3) Other actions that have a possibility of hindering appropriate management of the Possessed Personal Information

(Restriction of connection to equipment or media that have recording functions)

Article 32.

In accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system), the personal information protection manager must implement the measures that are necessary in order to prevent leaks, loss, or damage of the relevant Possessed Personal Information, such as restricting connection to information system terminals of devices or media that have recording functions, such as smartphones

or USB memory (including responding to updates to the relevant devices).

(Verification of entered information)

Article 33.

In accordance with the degree of importance of the Possessed Personal Information that will be handled by an information system, board members and employees must verify input content against its source documents, confirm the content of the relevant Possessed Personal Information before and after processing, and conduct verification with existing Possessed Personal Information.

(Backups)

Article 34.

1. In accordance with the degree of importance of the Possessed Personal Information (limited to matters that are handled by an information system), the personal information protection manager must implement the measures that are necessary in order to create backups and conduct dispersed storage.
2. Board members and employees must follow the instructions of the personal information protection manager to conduct backups of the Possessed Personal Information

(Management of information system design specifications)

Article 35.

The personal information protection manager must implement the measures that are necessary for storage, duplication, and disposal of documents, such as design specifications and configuration diagrams for information systems related to the Possessed Personal Information so that they will not be learned by external parties.

(Limitation of terminals)

Article 36.

In accordance with the confidentiality and other aspects of the content of the Possessed Personal Information (limited to matters that are handled by an information system), the personal information protection manager must implement the measures that are necessary for limiting the terminals on which the Possessed Personal Information will be processed.

(Prevention of theft of terminals)

Article 37.

1. The personal information protection manager must implement the measures that are necessary in order to prevent theft or loss of terminals, such as making terminals immovable and locking offices.
2. Excluding times when the personal information protection manager recognizes that it is necessary, board members and employees may not take terminals out or bring them in from outside.

(Prevention of access by third parties)

Article 38.

For use of terminals, board members and employees must implement the measures that are necessary to ensure that the Possessed Personal Information (limited to matters that are handled by an information system) will not be accessed by third parties, such as being thorough about logging off information systems in accordance with the state of use.

Section 4: Safety management for the Information System Office

(Management of entering and leaving an office)

Article 39.

1. The managing director (hereinafter referred to as the “Managing director of the Information System Office”) of the division or overseas office that manages an office or other area in which equipment, such as a main server that handles the Possessed Personal Information, is installed (hereinafter referred to as the “Information System Office”) must stipulate the people who have the authority to enter the Information System Office, and must also implement measures such as confirming reasons for entry, recording entry/ exit, identifying people from outside the department, having a board member or employee be present or conducting monitoring by monitoring equipment when a person from outside the department enters, and conducting restriction or inspection for bringing in, using, or taking out external electromagnetic recording media. In addition, in a case in which facilities have been established for storing media that

record the Possessed Personal Information, the same measures must also be implemented when it is recognized as necessary.

2. When it is recognized as necessary, the Managing director of the Information System Office must implement the measures, such as specifying entrances to and exits from the Information System Office, thereby making it easy to manage entering and leaving, and restricting indications of locations.
3. For management of entering and leaving the Information System Office and storage facilities, when it is recognized as necessary, the Managing director of the Information System Office must set the Authentication Function for entry and implement the measures that are necessary for conducting the preparation of stipulations related to management of the password (including regular reconsideration or reconsideration as necessary for those stipulations) and prevention of reading the password.

(Management of the Information System Office)

Article 40.

1. In order to take precautions against unauthorized intrusion from the outside, the Managing director of the Information System Office must implement the measures for equipment, such as lock devices, alarm devices, and monitoring equipment in the Information System Office.
2. In order to take precautions against disasters, the Managing director of the Information System Office must implement the measures that are necessary for earthquake-proofing, fireproofing, smoke-proofing, and waterproofing in the Information System Office, and must implement the measures for ensuring a backup electricity source for equipment, such as servers and preventing damage to wiring.

Chapter 3: Reports related to possession of personal information files

(Reports related to possession of personal information files)

Article 41.

1. When a division or overseas office has come into possession of personal information files (including specific personal information files; hereinafter the same) (excluding the things stated in each of the items of Article 11.2 of the Act), the personal information protection manager of

the relevant division or overseas offices must state in a ledger based on the provisions of Article 42 each of the items of Article 11.1 of the Act, Article 11.3 of the Act, and other necessary matters and make a report to the assistant general personal information protection manager within the fiscal year in which the files were obtained. The same will also apply when such matters have been changed. Excluding cases in which the stipulations in Article 19.11 through Article 19.14 of the Numbers Act applies, and specific personal information will be provided or its provision will be received, specific personal information files may not be created beyond the scope that is necessary for processing personal numbers.

2. In addition to the personal information files for which the report stipulated in the previous clause was made, when the personal information protection manager has come into possession of the Possessed Personal Information (excluding the items stipulated in Article 11.2.1 through Article 11.2.6 and in Article 11.2.8 of the Act) for which the number of relevant people is 1,000 people or more, the person must notify the assistant general personal information protection manager of each of the items of Article 11.1 of the Act, Article 11.3 of the Act, and other necessary matters without delay. The same will also apply when information will be changed.

(Maintenance of ledgers in divisions and overseas offices)

Article 42.

1. The personal information protection manager must prepare ledgers concerning the Possessed Personal Information of the relevant division or overseas office, in accordance with the confidentiality and other aspects of the content of the Personal Information, and keep records concerning the state of handling for use and storage for the relevant Possessed Personal Information.
2. For the ledgers of the previous clause, the person in charge of personal information protection in each relevant division and overseas office will conduct clerical work for the records and management of that work.
3. The personal information protection manager will prepare the means of checking the state of handling specific personal information files and keep records concerning the state of handling for the use and storage for the relevant specific personal information.

(Creation and public announcement of a register of personal information files)

Article 43.

1. The general personal information protection manager must follow the provisions of Article 11 of the Act to create and publicly announce AMED's register of personal information files.
2. When maintaining the register of personal information files, the general personal information protection manager will pay sufficient attention to the necessity of maintaining confidentiality.
3. Except for cases when it is necessary for maintenance, the register of personal information files will be kept in an accessible place and provided for general access.

(Records of the state of handling the Possessed Personal Information)

Article 44.

For the Possessed Personal Information for which notification was received based on the provisions of Article 41, the assistant general personal information protection manager must prepare a ledger and keep records concerning handling, such as use and storage of the relevant Possessed Personal Information.

Chapter 4: Reporting cases, and measures to prevent recurrence

(Reporting cases of leaks of personal information)

Article 45.

1. In the event that a board member or employee became aware of the occurrence of a case that will be a problem in terms of ensuring safety, such as a leak of Possessed Personal Information or the possibility of a case that will be a problem, that board member or employee who became aware of that case must immediately report that fact to the personal information protection manager who manages the relevant Possessed Personal Information. Provided, however, that the person will immediately implement the measures that can be immediately taken for preventing the spread of damage, such as turning off the wireless LAN or unplugging the LAN cable for the relevant terminal that is suspected of being accessed by an external party without authorization or infected by a malicious program.
2. When the personal information protection manager has received a report from a board member or employee based on the provisions of the previous clause, the person must promptly implement the measures that are necessary for the restoration and prevention of the spread of

damage.

3. After taking the measures of the previous clause, the personal information protection manager must promptly investigate the history and state of damage that arose for the case and then make a report to the general personal information protection manager and the assistant general personal information protection manager. Provided, however, that in the event that a case recognized as particularly serious has arisen, the personal information protection manager will immediately report the content of the relevant case to the general personal information protection manager and the assistant general personal information protection manager.
4. In the event that the general personal information protection manager has received a report of the previous clause, the person must promptly report the content, history, and state of damage of the relevant case to the President in accordance with the content of the case.
5. In accordance with the content of the case, the general personal information protection manager will promptly provide information, concerning the content, history, and state of damages of the case to an administrative organ that has jurisdiction over AMED.

(Measures to prevent a recurrence of cases of leaks of personal information)

Article 46.

In the event that a leak of Possessed Personal Information or another case that will be a problem in relation to the management of personal information has arisen, the personal information protection manager must analyze the cause of the occurrence of that case based on the results of an investigation based on the provisions of Article 45.3 and implement the measures that are necessary for the prevention of a recurrence.

(Public announcement of cases of leaks of personal information)

Article 47.

1. In accordance with the content and effects of a case, AMED will implement the measures, such as publicly announcing facts and measures to prevent a recurrence and responding to the relevant person for the Possessed Personal Information related to the relevant case.
2. For a case that will be publicly announced, information will be promptly provided to the Ministry of Internal Affairs and Communications (Administrative Management Bureau) concerning the content, history, and state of damage of the relevant case.

(Reporting cases of leaks of specific personal information)

Article 48.

1. In the event that a board member or employee has ascertained a violation of the Numbers Act or the possibility of violating the Numbers Act, or in the event that the person has discovered a serious case (a case in which information was leaked to an external party from an information system that handles personal numbers (including problems caused by unauthorized access or malicious programs), a case in which the number of relevant people for the specific personal information for the case is 101 people or more, a case that has become a situation in which it is possible for a large number of unspecified people to access information, a case in which a board member or employee took information outside for an unauthorized purpose, or another case that AMED judges to be a serious case), or a case that has a possibility of being a serious case, the person must immediately report that fact to the personal information protection manager who manages the relevant possessed specific personal information and prevent the spread of damage.
2. When the personal information protection manager has received a report from a board member or employee based on the provisions of the previous clause, the person must investigate the facts, investigate the causes, and promptly make a report to the general personal information protection manager and the assistant general personal information protection manager.
3. In the event that the general personal information protection manager has received a report of the previous clause, the person must promptly report to the President the relevant case's content, history, and state of damage.
4. The general personal information protection manager must promptly (for serious cases or cases that may be serious, immediately) make a report about the facts and measures to prevent a recurrence to the Personal Information Protection Commission.

(Measures to prevent a recurrence of cases of leaks of specific personal information)

Article 49.

The personal information protection manager must specify the scope of the effects caused by a case that was ascertained based on the provisions of Article 48.2, consider measures to prevent a recurrence based on the causes that were investigated, and then promptly implement the measures.

(Public announcement of cases of leaks of specific personal information)

Article 50.

In accordance with the content of cases and from the perspectives of preventing secondary damage and avoiding the occurrence of similar cases, AMED must promptly contact the relevant person concerning the facts or create a situation in which the relevant person can easily learn them and then promptly make a public announcement about the facts and measures for preventing a recurrence.

Chapter 5: Inspections and audits

(Inspections)

Article 51.

The personal information protection manager will conduct inspections regularly and whenever necessary concerning the recording media, processing path, and storage method of the Possessed Personal Information in divisions and overseas offices, and when the person recognizes that it is necessary, the person will report those results to the general personal information protection manager.

(Audits)

Article 52.

In order to verify the appropriate management of the Possessed Personal Information, the person responsible for personal information audits will conduct regular audits and audits whenever necessary (including external audits; hereinafter the same) concerning the state of management of the Possessed Personal Information at AMED and report those results to the general personal information protection manager. Audits will be conducted as focused audits that include on-site audits in accordance with the confidentiality and other aspects of the content of the Possessed Personal Information.

(Evaluation and reconsideration)

Article 53.

1. For measures for the purpose of the appropriate management of the Possessed Personal Information, the assistant general personal information protection manager will conduct

evaluations concerning measures for the purpose of the appropriate management of the Possessed Personal Information from perspectives, such as effectiveness, and based on the results of an inspection or audit, and when the person recognizes that it is necessary, the person will implement the measures for reconsideration of those measures.

2. The assistant general personal information protection manager will report the results of the reconsideration of the previous clause to the general personal information protection manager.

Chapter 6: Auxiliary provisions

(Cooperation with administrative organs)

Article 54.

Based on the Basic Policy on the Protection of Personal Information (Cabinet decision of April 2, 2004), AMED will closely cooperate with the administrative organs that have jurisdiction over AMED and will appropriately manage the personal information that it possesses.

(Formulation of regulation details)

Article 55.

In addition to the stipulations of these regulations, details that are necessary in relation to AMED's protection of the Possessed Personal Information will be stipulated separately.

Supplementary provisions

These regulations will go into effect on April 1, 2015.

Supplementary provision (Regulation No. 33 of January 1, 2016)

These regulations will go into effect on January 1, 2016.

Supplementary provision (Regulation No. 50 of April 1, 2016)

These regulations will go into effect on April 1, 2016.

Supplementary provision (Regulation No. 89 of June 30, 2017)

These regulations will go into effect on July 1, 2017.

Supplementary provision (Regulation No. 106 of October 10, 2018)

These regulations will go into effect on October 10, 2018.

Supplementary provision (Regulation No. 33 of March 27, 2020)

These regulations will go into effect on April 1, 2020.