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.

Personal Information Protection Rules

April 1, 2015

Rules No. 27

Revisions: Rules No. 33 of January 1, 2016

Rules No. 50 of April 1, 2016

Rules No. 89 of June 30, 2017

Rules No. 106 of October 10, 2018

Rules No. 33 of March 27, 2020

Rules No. 18 of March 24, 2022

Rules No. 20 of March 29, 2023

Rules No. 28 of March 17, 2025

Table of Contents

Chapter 1: General Provisions

Section 1: General Rules

(Purpose)

Article 1.

The purpose of these Rules shall be to protect individuals' rights and interests while ensuring the proper and smooth operation of the Japan Agency for Medical Research and Development (hereinafter referred to as the "AMED") by stipulating the items necessary for appropriate management of personal information retained by the AMED.

(Definitions)

Article 2.

The definition of terms used in these Rules shall be as presented in the following items, in addition to the provisions of Articles 2, 16, and 60 of the Act on the Protection of Personal Information (Law No. 57 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 (Law No. 27 of 2013; hereinafter referred to as the "Individual Number Act").

(1) Department/Office shall refer to those specified in Article 10 of the Organization Regulations (Regulations No. 4 of 2015).
(2) Division shall refer to those specified from Articles 11 to 17-2 of the Organization Regulations.
(3) Officers and Employees shall refer to the AMED's officers, employees, and persons acknowledged by General Personal Information Protection manager to comply with these Rules.
(4) Overseas Office shall refer to those specified in Attached Table of the Organization Regulations.
(5) Head of Overseas Office shall refer to the person specified in Article 4 of the Directive on Principal Regions, etc. of Overseas Offices (Directive No. 23 of 2016).

(Scope of Application)

Article 3.

The handling of personal information, specific personal information, and personal and specific personal information files held by the AMED shall be governed by the Act, the Individual Number Act and these Rules.

(Responsibilities of Officers and Employees)

Article 4.

Officers and Employees shall, in accordance with the purpose of the Act and the Individual Number Act, handle retained personal and specific personal information (hereinafter referred to as "Retained

Personal Information, etc.") in compliance with the relevant laws and regulations, illustrative rules, and the instructions of General Personal Information Protection manager, Assistant general personal information protection manager, and Personal information protection manager.

Section 2: Management Framework for Retained Personal Information, etc.

(General Personal Information Protection manager, etc.)
Article 5.
The AMED shall have a General Personal Information Protection manager, assigned to Executive Director.

2 There shall be one Assistant general personal information protection manager, assigned to the Managing Director of the Department of General Affairs. In addition, there shall be one assistant to the Assistant general personal information protection manager, assigned to the Director of the Division of General Affairs.

3 Department/Office shall have one Chief personal information protection manager, assigned to the head of Department/Office.

4 Division and Overseas Office shall have one Personal information protection manager, assigned to the head of Division and Overseas Office.

5 Division and Overseas Office shall have one Privacy Staff, assigned to staff engaged in the general management designated by the Personal information protection manager. The Personal information protection manager shall report the name, position, etc. of Privacy Staff to the Assistant general personal information protection manager, promptly after their appointment.

6 The AMED shall have a Privacy Audit Officer, assigned to the Managing Director of the Office of Audit.

(Duties of General Personal Information Protection manager, etc.)
Article 6.
The General Personal Information Protection manager shall oversee the AMED's administration of Retained Personal Information, etc.

2 The Assistant general personal information protection manager shall assist the General Personal Information Protection manager in performing the duties under the order of the General Personal Information Protection manager. The Assistant general personal information protection manager shall also assist the Assistant general personal information protection manager in performing the duties.

3 The Chief personal information protection manager shall oversee the administration of personal information in the relevant Department/Office.

4 The Personal information protection manager shall be responsible for ensuring appropriate management of Retained Personal Information, etc. in the relevant Division and Overseas Office. If Retained Personal Information, etc. is handled by information systems, the Personal information protection manager shall perform such duties in cooperation with the administrator of the relevant information systems.

5 Privacy Staff, under the order of the Personal information protection manager, assists the Personal information protection manager in the administration management of Retained Personal Information, etc. in the relevant Division and Overseas Office.

6 Privacy Audit Officer shall be in charge of auditing the status of the management of Retained Personal Information, etc.

7 The Personal information protection manager shall designate the employees (hereinafter referred to as the “Administration Staff”) who handle personal numbers and specific personal information (hereinafter referred to as "Specific Personal Information, etc."), and specify their roles and the scope of Specific Personal Information, etc. to be handled by each Administration Staff.

(Committee for Appropriate Management of Retained Personal Information, etc.)
Article 7.
The General Personal Information Protection manager shall, when deemed necessary to make decisions, communicate and coordinate important matters related to the management of the AMED's Retained Personal Information, etc., establish a committee consisting of Officers and Employees concerned, which will meet on a regular or ad-hoc basis.

(Education and Training)
Article 8.
The General Personal Information Protection manager shall ensure that Officers and Employees engaged in handling Retained Personal Information, etc. have a better understanding thereof, and provide education and other necessary training to raise their awareness of the protection of personal and specific personal information (hereinafter referred to as "Personal Information, etc.")

2 The General Personal Information Protection manager shall provide Officers and Employees engaged in the administration of information systems that handle Retained Personal Information, etc. with necessary education and training on the management, operation, and security measures of information systems for the appropriate management of Retained Personal Information, etc.

3 The General Personal Information Protection manager shall conduct training for Personal information protection managers and Privacy Staff on the proper management of Personal Information, etc. in the field of Division and Overseas Office.

4 The Personal information protection manager shall provide Officers and Employees of the Division and Overseas Office with opportunities to participate in training sessions conducted by the General Personal Information Protection manager for proper management of Retained Personal Information, etc.

Chapter 2: Handling of Personal Information, etc.

Section 1: Acquisition, Use, etc. of Personal Information, etc.

(Specifying the Purpose of Use)
Article 9.
Officers and Employees must handle personal information only if necessary to perform their duties under the laws and regulations, and specify the purpose for which the information is to be used to the extent possible.

2 Officers and Employees must not hold Personal Information, etc. beyond the extent necessary for the purpose of use specified pursuant to the provisions of the preceding paragraph (hereinafter referred to as the “Purpose of Use”).

3 Officers and Employees must not alter the Purpose of Use beyond a reasonable extent from the original Purpose of Use.

(Restriction owing to Purpose of use)
Article 10.
Officers and Employees must not handle personal information beyond the scope necessary for achieving the Purpose of Use specified pursuant to the provisions of the preceding Article without obtaining the identifiable person's consent to do so beforehand.

2 If, owing to a merger or other such circumstances, Officers and Employees acquire personal information when succeeding to the business of another business handling personal information, it must not handle that personal information beyond the scope necessary for achieving the pre-succession Purpose of Use for that personal information without obtaining the identifiable person's consent to do so in advance.

3 The provisions of the preceding two paragraphs do not apply in the cases stipulated in paragraph (3), Article 18 of the Act.

(Prohibition of Inappropriate Utilization)
Article 10-2.
Officers and Employees must not use personal information in a way that there is a possibility of fomenting or inducing an unlawful or unjust act.

(Proper Acquisition)

Article 11.

Officers and Employees must not acquire Personal Information, etc. by deception or other wrongful means.

2 Officers and Employees must not acquire sensitive personal information without obtaining the identifiable person's consent in advance, except in cases stipulated in paragraph (2), Article 20 of the Act.

3 Administration Staff may, if necessary, request Individual Numbers from an identifiable person (including persons in the same household thereof) in order to process the affairs handling specific personal information.

4 Administration Staff must, upon receiving Individual Numbers from an identifiable person in accordance with the preceding paragraph, verify the identity of the identifiable person in accordance with the relevant laws and regulations.

5 Administration Staff may not ask an identifiable person to provide their Individual Number, except for the case in paragraph (3).

(Notification of a Purpose of Use when Acquiring Personal Information)

Article 11-2.

Unless the Purpose of Use has already been disclosed to the public, Officers and Employees must promptly notify identifiable persons of that Purpose of Use, or disclose this to the public once the personal information is acquired.

2 Notwithstanding the provisions of the preceding paragraph, Officers and Employees must explicitly specify the Purpose of Use to identifiable persons, before acquiring their personal information specified in a written agreement or other document (including an electronic or magnetic record; hereinafter the same applies in this paragraph) accompanying the execution of an agreement with the identifiable persons, or acquiring their personal information specified in a document, directly from the identifiable persons, provided, however, that this does not apply in cases where there is an urgent need to protect the human life, wellbeing or property of an individual.

3 Officers and Employees must, upon altering the Purpose of Use, notify identifiable persons of the altered Purpose of Use or disclose this to the public.

4 The provisions of the preceding three paragraphs do not apply in the cases stipulated in Items (i) through (iv), paragraph (4), Article 21 of the Act.

(Maintaining the Accuracy of Data)

Article 12.

Officers and Employees must keep the content of personal data accurate and up to date, within the scope necessary for achieving the Purpose of Use, and delete the personal data immediately if they no longer require it.

(Security Management Measures)
Article 13.
Officers and Employees must, pursuant to the provisions of these Rules, take necessary and appropriate measures for managing the security of retained personal information, preventing its leaking, loss or damage.

2 Officers and Employees must comply with these Rules and, considering that the AMED is an academic research institution, etc., manage the AMED's corporation documents electronically in a centralized document management system for the safe management of retained personal information handled for academic research purposes.

(Supervision of Employees)
Article 13-2.
In having an employee handle personal data, the General Personal Information Protection manager must exercise the necessary and adequate supervision over the employee to ensure the secure management of personal data.

(Supervision of an Entrusted Person)
Article 13-3.
Officers and Employees must, upon entrusting another person with all or part of the handling of personal data, exercise the necessary and adequate supervision over the entrusted person, so as to ensure the secure management of the personal data with whose handling it entrusts that person.

(Restrictions on Provision of Personal Data to Third Parties)
Article 14.
Officers and Employees must not provide personal data to a third party without obtaining the identifiable person's consent in advance, except in cases set forth below:

(1) cases based on laws and regulations;
(2) cases in which there is a need to protect the life, wellbeing, or property of an identifiable person, and it is difficult to obtain the consent of the identifiable person;
(3) cases in which there is a special need to improve public wellbeing or promote healthy child development, and it is difficult to obtain the consent of the identifiable person;

(4) cases in which there is a need to cooperate with national government organs, local government organs, or a person entrusted thereby with performing the functions prescribed by laws and regulations, and obtaining the consent of the identifiable person is likely to interfere with the performance of those functions.

(5) cases in which the business handling personal information is an academic research institution or the equivalent, and providing the personal data for the purpose of publication of academic research results or teaching is unavoidable (excluding cases in which there is a risk of unjustly infringing on individuals' rights and interests);

(6) cases in which the business handling personal information is an academic research institution or the equivalent, and needs to provide personal data for the academic research purpose (including cases in which a part of the purpose of handling the personal data is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individuals' rights and interests) (limited to cases in which the business handling personal information and the third party jointly conduct academic research);

(7) cases in which the third party is an academic research institution or the equivalent, and the third party needs to handle the personal data for academic research purposes (including cases in which part of the purpose of handling the personal data is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individuals' rights and interests).

2 Notwithstanding the provisions of the preceding paragraph, Officers and Employees may provide the personal data to a third party, when the provision of personal data that identifies a person to a third party is to be suspended at the request of the identified person, and the following items are notified or made readily available to the identifiable persons in advance, as provided for in the Order of the Personal Information Protection Commission, and reported to the Personal Information Protection Commission in advance; provided, however, that this does not apply if personal data provided to a third party is sensitive personal information, or personal data obtained in violation of Article 11, paragraph (1) or provided by another business handling personal information pursuant to the provisions of the main clause of this paragraph (including those reproduced or processed in whole or in part):

(1) name and address of the AMED and the name of the President;

(2) the fact that providing the data to the third party constitutes the Purpose of Use;

(3) the details of the personal data it will provide to the third party;

(4) the means or manner in which it will acquire the data it provides to the third party;

(5) the means or manner in which it will provide the data to the third party;

(6) the fact that it will cease to provide personal data that can be used to identify the identifiable person to a third party at the request of the identifiable person;

(7) the means of receiving the identifiable person's request;

(8) other matters prescribed by Order of the Personal Information Protection Commission as those necessary to protect individuals' rights and interests.

3 If the details set forth in item (i) of the preceding paragraph are altered, or businesses handling personal information have ceased to provide personal data pursuant to the provisions of the preceding paragraph, the businesses must notify the identifiable person of this or make this readily accessible to the person, and notify the Personal Information Protection Commission of this, pursuant to Order of the Personal Information Protection Commission, without delay; and if the businesses seek to alter the details set forth in items (iii) through (v), item (vii), or item (viii) of that paragraph, the businesses must do so beforehand.

4 In the following cases, a person receiving personal data is not to fall under a third party regarding applying the provisions of each preceding paragraph:

(1) the businesses handling personal information entrusts a person with all or part of the handling of personal data within the scope necessary for achieving the Purpose of Use;

(2) the personal data is provided when a person succeeds to the business owing to a merger or other such circumstances;

(3) the personal data is provided to specific persons who have joint use of that data; the business notifies the person identifiable by that data of this in advance as well as the details of that data, the extent of the joint users, the users' Purpose of Use, and the name and address of the person responsible for managing the personal data. If the user is a corporation, the name of its representative or the business makes the foregoing information readily accessible to the person identifiable by that data in advance.

5 If the name and address of the person responsible for managing the personal data, or in cases of a corporation, the name of the representative, as provided for in item (iii) of the preceding paragraph are altered, the business handling personal information must notify or make this readily accessible to the person identifiable by that data immediately. If the business intends to alter a user's Purpose of Use or the person responsible for the management as provided for in that item, the business must do so beforehand.

(Restriction on Provision of Specific Personal Information)

Article 15.

Officers and Employees shall not provide specific personal information, except as limited and specifically stated in the Individual Number Act.

(Restriction on Use of Specific Personal Information)

Article 16.

Administration Staff shall not use specific personal information for any purpose other than those specified in the Individual Number Act.

2 Notwithstanding the provisions of the preceding paragraph, Administration Staff may use specific personal information for purposes other than the Purpose of Use, when it is necessary for the protection of the life, body, or property of an identifiable person, where consent of the identifiable person is obtained, or it is deemed difficult to obtain consent of the identifiable person concerned, and when it is recognized that there is no risk of unreasonable infringement on the rights and interests of the identifiable person or a third party by using the specific personal information for a purpose other than Purpose of Use.

3 The provisions of the preceding paragraph do not preclude the application of the provisions of laws and regulations which restrict the use of specific personal information.

(Restrictions on the Provision of Personal Data to Third Parties in Foreign Countries)

Article 17.

Except cases presented in the items of Article 14, paragraph 1, Officers and Employees must, when providing personal data to a third party located in a foreign country (referring to a country or region outside Japan; the same shall apply hereinafter in this Article and Article 18-3, paragraph (1), Item (ii)) (excluding foreign countries specified by the Order of the Personal Information Protection Commission as having a system for the protection of personal information considered to be on the same level as Japan in protecting the rights and interests of identifiable persons; the same shall apply hereinafter in this Article and the said items) obtain consent of the identifiable person in advance to the effect that the personal data may be provided to a third party located in the foreign country (excluding those who have established a framework that conforms to the standards specified in the Order of the Personal Information Protection Commission as necessary, to continuously take measures equivalent to those required of businesses handling personal data (referred to as "Equivalent Measures" in paragraph (3)) pursuant to the provisions of this Section; the same shall apply hereinafter in this paragraph, the next paragraph and the said items). In this case, the provisions of the preceding Article do not apply.

2 When intending to obtain an identifiable person's consent pursuant to the provisions of the preceding paragraph, Officers and Employees must provide the person in advance with information on the personal information protection system of the foreign country, on the measures the third party takes for the protection of personal information, and other information that serves as a reference to the person, pursuant to Order of the Personal Information Protection Commission.

3 Upon having provided personal data to a third party (limited to a person establishing a system prescribed in paragraph (1)) in a foreign country, Officers and Employees must take necessary

measures to ensure continuous implementation of the Equivalent Measures by the third party, and provide information on the necessary measures to the identifiable person at the request of that person, pursuant to the Order of the Personal Information Protection Commission.

(Preparing of Records on Provision of Personal Data to Third Parties)
Article 18.
Officers and Employees shall, when providing personal data to a third party (excluding those listed in each item of paragraph (2), Article 16 of the Act; the same shall apply hereinafter in this and the following Articles (including cases where it is applied mutatis mutandis by replacing the term in paragraph (3) of Article 18-3), prepare the records of the date the personal data was provided, a name of the third party, and other matters specified in accordance with the provisions of the Order of the Personal Information Protection Commission; provided, however, that this does not apply if the provision of said personal data falls under any items under paragraph (1) or paragraph (4) of Article 14 (in the case of the provision of personal data pursuant to paragraph (1) of Article 14, any item of paragraph (1) of Article 14).
2 Officers and Employees must keep a record under the preceding paragraph for a period of time prescribed by the Order of the Personal Information Protection Commission from the date when it prepared the record.

(Confirmation on Receiving Personal Data from a Third Party)
Article 18-2.
Officers and Employees must, when receiving personal data from a third party, confirm the following items as required by the Order of the Personal Information Protection Commission; provided, however, that this does not apply if the provisions of such personal data fall under any item of paragraph (1) or (4) of Article 14.
(1) the name and address of the third party and, if the third party is a corporation, the name of its representative;
(2) background of the acquisition of the personal data by the third party.
2 If Officers and Employees conduct confirmation under the preceding paragraph, a third party referred to in the preceding paragraph must not deceive the Officers and Employees on a matter relating to the confirmation.
3 Upon having given confirmation under paragraph (1), Officers and Employees must prepare a record pursuant to Order of the Personal Information Protection Commission on the date when it received the personal data, matters concerning the confirmation, and other matters prescribed by Order of the Personal Information Protection Commission.

4 Officers and Employees must keep a record under the preceding paragraph for a period of time prescribed by the Order of the Personal Information Protection Commission from the date when it prepared the record.

(Restrictions on the Provision of Information Related to Personal Information to Third Parties)
Article 18-3.
Except cases set forth in each item of Article 14, paragraph (1), if it is assumed that a third party acquires information related to personal information (limited to those compiled in a database or the equivalent of information related to personal information; hereinafter the same applies in this Section) as personal data, Officers and Employees must not provide the information related to personal information to the third party without confirming the matters set forth as follows, pursuant to Order of the Personal Information Protection Commission:

(1) the identifiable person's consent to the effect that the person approves of the third party acquiring information related to personal information as personal data that can identify the person from Officers and Employees has been obtained;
(2) for provision to a third party in a foreign country, before the businesses obtain the identifiable person's consent referred to in the preceding item, information on the personal information protection system of the foreign country, information on the measures the third party takes for the protection of personal information, and other information that serves as a reference to the person, has been provided in advance to the person pursuant to Order of the Personal Information Protection Commission.

2 The provisions of Article 17, paragraph (3) apply mutatis mutandis to cases in which Officers and Employees provide information related to personal information pursuant to the provisions of the preceding paragraph. In this case, the phrase ", and provide information on the necessary measures to the identifiable person at the request of that person," in Article 17, paragraph (3) is deemed to be replaced with ",".
3 The provisions of paragraphs (2) through (4) of the preceding Article apply mutatis mutandis to cases in which Officers and Employees conduct confirmation pursuant to the provisions of paragraph (1). In this case, the phrase "received" in paragraph (3) of the preceding Article is deemed to be replaced with "provided."

(Complaint Processing)
Article 18-4.
Officers and Employees must endeavor to process complaints about the handling of personal information appropriately and promptly.

2 The Personal information protection manager must endeavor to establish the necessary systems for achieving the purpose referred to in the preceding paragraph.

(Responsibilities of Academic Research Institutions or the Equivalent)
Article 18-5.
Officers and Employees must endeavor to comply with the provisions of this Act as well as personally take necessary measures for ensuring the appropriate handling of personal information for academic research purposes, and endeavor to the public the content of those measures.

Section 2: Handling of Retained Personal Information, etc.

(Access Restriction)
Article 19.
Personal information protection manager shall limit the scope and authority of Officers and Employees who have access to Retained Personal Information, etc. to the minimum necessary to achieve the Purpose of Use, depending on the confidentiality of the Retained Personal Information, etc. (the degree of ease of identification of specific persons, any inclusion of sensitive personal information, and the nature and extent of damage that could occur in the event of a leakage, etc. shall be considered; the same shall apply hereinafter).
2 Officers and Employees who do not have access privileges shall not access Retained Personal Information, etc.
3 Officers and Employees shall not, despite being authorized, access Retained Personal Information, etc. for any purpose other than business purposes.

(Restriction on Reproduction, etc.)
Article 20.
Even if Officers and Employees handle Retained Personal Information, etc. for business purposes, the Personal information protection manager shall limit the following acts to the minimum necessary, depending on confidentiality and other factors of such Retained Personal Information, etc., and Officers and Employees shall perform such acts in accordance with the Personal information protection manager's instruction:
(1) Duplication of Retained Personal Information, etc.;
(2) Transmission of Retained Personal Information, etc.;
(3) Sending or taking outside the company the media on which Retained Personal Information, etc., is recorded;

(4) Other acts that may interfere with appropriate management of Retained Personal Information, etc.

(Correction, etc. of Errors)
Article 21.
Officers and Employees shall, if discovering any errors in Retained Personal Information, etc., correct such information in accordance with the instructions of the Personal information protection manager, unless such errors are clearly acknowledged to be minor.

(Management, etc. of Media)
Article 22.
Officers and Employees shall, in accordance with the instructions of the Personal information protection manager, keep the media in which Retained Personal Information, etc. is recorded in a designated place and, if deemed necessary, store and lock them in a fireproof safe. In principle, if the media on which Retained Personal Information is recorded is sent or taken outside the Company, necessary measures for access control, such as setting a function to identify the authority using a password, etc. (referring to a password, IC card, biometric information, etc.; the same shall apply hereinafter) (hereinafter referred to as "Authentication Function") must be taken.

(Prevention of Erroneous Sending, etc.)
Article 22-2.
Officers and Employees shall take necessary measures such as checking by multiple staff members and using checklists depending on the confidentiality of personal information handled in each administration work or project, to prevent erroneous transmission, delivery or issue of electromagnetic records or media containing retained personal information, or erroneous posting of such information on websites, etc.

(Disposal, etc.)
Article 23.
Officers and Employees shall, if Retained Personal Information, etc. or media (including those built into terminals and servers) on which Retained Personal Information, etc. is recorded are no longer needed, erase such information or dispose of such media in a manner that makes it impossible to recover or decipher such Retained Personal Information, etc. under the Personal information protection manager's instruction. In particular, if erasure of retained personal information or disposal of media on which retained personal information is recorded is entrusted (including subcontracting and beyond), it must be confirmed that the erasure and disposal are securely conducted by the

entrusted person by having staff members witnessing the erasure and disposal if necessary, or receiving a document with photographs, etc. evidencing the erasure and disposal.

(Assessment of External Environment)
Article 23-2.
Officers and Employees shall, if retained personal information is handled in a foreign country, take necessary and appropriate measures for the safe management of retained personal information, based on their knowledge of the systems for the protection of personal information in the foreign country.

(Measures to be taken when Entrusting Handling of Personal Information to External Party)
Article 23-3.
When entrusting the handling of personal information to an outside contractor, necessary measures shall be taken to ensure that a competent party is selected for appropriate management of personal information. In addition, the following matters must be clearly stated in the contract, as well as the management and implementing framework of managers and staff of the entrusted person, inspections of the state of management of personal information, and other necessary matters must also be confirmed in writing:

(1) Obligation to maintain confidentiality and prohibit use of personal information outside the intended purpose;
(2) Conditions pertaining to subcontracts (including cases where a subcontractor is the subsidiary of the entrusted person (as defined in Article 2, paragraph (1), item (iii) of the Companies Act (Act No. 86 of 2005); the same shall apply in this item and item (iv) of the same paragraph of the same article), such as restrictions on or prior approval of subcontract (a contract document with the entrusted party shall clearly specify the requirements of subcontractors upon subcontracting even when the subcontractor is a subsidiary);
(3) Restrictions on the reproduction, etc., of personal information;
(4) Security control measures for personal information;
(5) Measures to be taken in the event of an incident such as the leakage of personal information;
(6) Erasure of personal information and return of media at the end of entrustment;
(7) Termination of the contract, liability for damages, and other necessary matters in the event of violating laws and regulations and the contract;
(8) Regular reports on the status of compliance with the contract and audits, etc. to ascertain the status of handling entrusted personal information by the entrusted person (including audits, etc. of subcontractors).

2 If Officers and Employees entrust handling of retained personal information to an outside party, the scope of entrusted personal information must be the minimum necessary in light of the content of entrusted operations.

3 Officers and Employees shall, if entrusting work pertaining to the handling of retained personal information to an outside party, confirm through on-site inspection at least once a year in principle, the status of management and implementation framework and personal information management, depending on confidentiality and other factors, and the volume of the retained personal information pertaining to the entrusted work.

4 Officers and Employees shall, if an entrusted person subcontracts work pertaining to the handling of retained personal information, have the entrusted person take measures specified in item (i) above, and conduct the measures specified in item (iii) above through the entrusted person or by the Company itself, depending on confidentiality and other factors of retained personal information related the work to be subcontracted. The same shall apply if a subcontractor subcontracts the work pertaining to handling of retained personal information.

5 Officers and Employees shall, if they have dispatched workers to perform work involving the handling of retained personal information, specify in the worker dispatch contract matters concerning the handling of personal information, including the obligation to maintain confidentiality.

6 Officers and Employees shall, when providing or entrusting retained personal information, consider the Purpose of Use by the party provided with such information, content of entrusted business, confidentiality of retained personal information, etc., in light of mitigating risks of damage owing to leakage, etc., and take measures such as deleting all or part of the descriptions that can identify specific persons or replacing them with other symbols, etc., as necessary.

(Measures for Receiving Dispatched Workers)

Article 23-4.

Personal information protection managers shall, when having dispatched workers perform work involving the handling of Retained Personal Information, etc., specify the handling of personal information, including the obligation of confidentiality, in the dispatched workers' contract.

Section 3: Ensuring Security in Information Systems

(Access Control)

Article 24.

The Personal information protection manager shall take necessary measures for access control, such as setting a function to identify the authority (hereinafter referred to as

"Authentification Function") using passwords, etc. (passwords, IC cards, biometric information, etc.; the same shall apply hereinafter), depending on confidentiality and other factors of Retained Personal Information, etc. (limited to those handled by information systems).

2 The Personal information protection manager shall, if taking measures set forth in the preceding paragraph, establish rules for the management of passwords, etc. (including regular or ad hoc reviews), and take necessary measures to prevent the reading of passwords, etc.

(Access Logs)

Article 25.

The Personal information protection manager shall record the status of access to Retained Personal Information, etc. (limited to those handled by information systems), depending on confidentiality and other factors, keep such records for a certain period of time, and take necessary measures to analyze the access logs on a regular or ad hoc basis. (hereinafter referred to as "Access Logs").

2 The Personal information protection manager shall take necessary measures to prevent alteration, theft or unauthorized erasure of Access Logs.

(Monitoring of Access Status)

Article 26.

The Personal information protection manager shall, depending on confidentiality and other factors and volume of Retained Personal Information, etc. (limited to those handled by information systems), set up the function, by which warnings are displayed if more than a certain amount of information that contains or may contain Retained Personal Information, etc. is downloaded from the information systems, and conduct regular inspections of such functions and other necessary measures to monitor any unauthorized access to such Retained Personal Information, etc.

(Setting Administrator’s Privileges)

Article 27.

Personal information protection manager shall, depending on confidentiality and other factors of Retained Personal Information, etc. (limited to those handled by information systems), take necessary measures, such as minimizing the privileges of information system administrators to mitigate damage caused by any fraudulent theft of such privileges and to prevent unauthorized manipulation of such privileges from the inside.

(Prevention of Unauthorized Access from Outside)

Article 28.

Personal information protection manager shall take necessary measures, such as route control by setting up firewalls, to prevent fraudulent access from outside to information systems that handle Retained Personal Information, etc.

(Prevention of Leakage, etc. by Malicious Programs)
Article 29.
The Personal information protection manager shall take necessary measures to prevent the leakage, loss, or damage of Retained Personal Information, etc. (limited to those handled by information systems) caused by malicious programs, including elimination of publicly disclosed vulnerabilities of software and the prevention of infection of any malicious programs that become known (including keeping the installed software up-to-date at all times).

(Processing of Retained Personal Information, etc. on Information Systems)
Article 30.
Officers and Employees shall, when duplicating Retained Personal Information, etc. for temporary processing, etc., limit duplication to the minimum necessary and promptly erase information that is no longer needed after the processing is completed. The Personal information protection manager shall monitor the status of erasure, etc. as necessary, depending on confidentiality and other factors of such Retained Personal Information, etc.

(Encryption)
Article 31.
The Personal information protection manager shall take necessary measures to encrypt Retained Personal Information, etc. (limited to those handled by information systems) depending on confidentiality and other factors thereof.
2 Officers and Employees shall encrypt Retained Personal Information, etc. (limited to those handled by information systems) for the following acts: (1) Saving Retained Personal Information, etc. in a shared drive
(2) Taking outside the company the media on which Retained Personal Information, etc., is recorded
(3) Other acts that may interfere with appropriate management of Retained Personal Information, etc.

(Restriction on Connecting Equipment and Media with Recording Function)
Article 32.

The Personal information protection manager shall, depending on confidentiality and other factors of Retained Personal Information, etc. (limited to those handled by information systems), take necessary measures to prevent leakage, loss, or damage of the Retained Personal Information, etc. by restricting connection, etc. of smartphones, USB memory sticks and other equipment and media with recording functions to information system terminals, etc. (including measures for updating such equipment).

(Cross-checking Input Information, etc.)
Article 33.
Officers and Employees shall, depending on the importance of Retained Personal Information, etc. handled in the information system, cross-check the original input form with the entered data, verify the contents of such Retained Personal Information, etc. before and after processing, cross-check with existing Retained Personal Information, etc.

(Backup)
Article 34.
The Personal information protection manager shall take necessary measures to create backups and retain them in a decentralized manner, depending on the importance of Retained Personal Information, etc. (limited to those handled by information systems).
2 Officers and Employees must back up Retained Personal Information, etc. as instructed by the Personal information protection manager.

(Management of Information System Design Documents, etc.)
Article 35.
The Personal information protection manager shall take necessary measures for the storage, reproduction, and disposal of documents such as information system design documents and configuration drawings pertaining to Retained Personal Information, etc., to prevent them from being known to outside parties.

(Limitation of Terminals)
Article 36.
The Personal information protection manager shall take necessary measures to limit the terminals for processing Retained Personal Information, etc. (limited to those handled by information systems) depending on confidentiality and other factors thereof.

(Prevention of Theft of Terminals, etc.)

Article 37.
The Personal information protection manager shall take necessary measures to prevent theft or loss of terminals, such as securing terminals and locking the office.
2 Officers and Employees shall not take out to or bring in the terminals from outside, except when the Personal information protection manager deems it necessary.

(Prevention of Access by Third Parties)
Article 38.
Officers and Employees shall, in using the terminals, take necessary measures, such as logging off from the information system depending on the circumstances of use, to ensure that Retained Personal Information, etc. (limited to those handled by information systems) is not viewed by a third party.

(Ensuring Cybersecurity)
Article 38-2.
Officers and Employees shall, in handling personal information or constructing or using information systems, take necessary measures to ensure cybersecurity by referring to the standards for cybersecurity measures set forth in Article 26, paragraph (1), item (ii) of the Basic Act on Cybersecurity (Law No. 104 of 2014), and ensure an appropriate level of cybersecurity considering the nature of retained personal information handled.

Section 4: Security Management of Information System Room, etc.

(Room Access Control)
Article 39.
The head of Division and Overseas Office, who manages rooms and other areas (hereinafter referred to as “Information System Room, etc.”) where the core servers and equipment handling Retained Personal Information, etc. are installed (hereinafter referred to as “Head of Information System Room, etc.”) shall take measures such as determining who is authorized to enter the Information System Room, etc., as well as checking businesses, recording entries and exits, identifying outsiders, presence of Officers and Employees or monitoring by surveillance equipment if outsiders enter, and restrictions or inspections on taking in, using, and taking out external electromagnetic recording media. In addition, the same measures must be taken if necessary, even if there are facilities established to retain media that record Retained Personal Information, etc.

2 The Head of Information System Room, etc. shall, when deemed necessary, take measures such as facilitating access control by specifying the entry and exit of the Information System Room, etc., and restricting the display of location.

3 The Head of Information System Room, etc. shall, if deemed necessary, set the Authentification Function for access control to the Information System Room, etc. and the storage facilities, and take necessary measures to establish provisions for the management of passwords, etc. (including their regular or ad-hoc reviews), and prevent reading of passwords, etc.

(Management of Information System Room, etc.
Article 40.
Head of Information System Room, etc. shall take measures such as installing locks, alarms, and monitoring equipment in the Information System Room, etc. to guard against any unauthorized entry from outside.

2 The Head of Information System Room, etc. shall take necessary measures such as earthquake-proofing, fire-proofing, smoke-proofing, and waterproofing in the Information System Room, etc. in preparation for disasters, etc., as well as securing a backup power supply for servers and other equipment, and preventing damage to wiring.

Chapter 3: Preparation and Publication, etc. of Personal Information File Registers

(Preparation and Publication, etc. of Personal Information File Registers)
Article 41.
The General Personal Information Protection manager shall, pursuant to the provisions of Cabinet Order, prepare and publish a register of the matters listed in Article 74, paragraph (1), items (i) through (vii), (ix) and (x) of the Act and other matters specified by the Cabinet Order regarding the personal information files held by the AMED (hereinafter referred to as the "Personal Information File Register" in this Chapter).

(1) The Personal information protection manager shall immediately notify the Assistant general personal information protection manager when a personal information file that is to be published as a Personal Information File Register is retained.

(2) The Personal Information File Register shall be kept in a place for access and made available for public inspection, except if required for maintenance.

2 The provisions of the preceding paragraph do not apply to the personal information file presented in the following:

(1) a personal information file set forth in items (i) through (x) of paragraph (2), Article 74 of the Act.

(2) a personal information file that contains all or a part of the recorded information contained in another personal information file subject to the publication prescribed in paragraph (1), Article 74 of the Act, if its Purpose of Use, recorded matters, and scope of record are within the scope of those subject to that publication.

(3) a personal information file designated by Cabinet Order as being equivalent to the personal information file listed in item (ii), paragraph (2), Article 75 of the Act.

3 Notwithstanding the provisions of paragraph (1), if inclusion of a part of the recorded particulars, the matters listed in paragraph (1), item (v) or (vii) of Article 74 of the Act, or a personal information file in the Personal Information File Register is likely to particularly hinder the appropriate execution of processes or services in relation to the Purpose of Use owing to their nature, the head of AMED may refrain from including that part of the recorded particulars, the matters listed in those items, or the personal information file in the Personal Information File Register.

(Maintenance of Register at the Division and Overseas Office)
Article 42.
The Personal information protection manager shall maintain a ledger of personal information files held by the Division and Overseas Office, and record and update the status of use, retention, and other handling of such Retained Personal Information, etc.

2 The ledgers set forth in the preceding paragraph shall be maintained for each Division and Overseas Office, and the Privacy Staff thereof shall be responsible for recording and managing the ledgers.

Article 43 Abolished

(Records on Handling Status of Retained Personal Information, etc.)
Article 44.
The Assistant general personal information protection manager shall maintain a ledger of Retained Personal Information, etc. notified pursuant to the provisions of Article 41, and record the use, retention, etc. of such Retained Personal Information, etc.

Chapter 4: Reporting cases and Measures to Prevent Recurrence

(Reporting etc. Personal Information Leaks, etc.)
Article 44-2.

In the case of leakage, loss, or damage and other situations concerning the security of personal information as prescribed by Order of the Personal Information Protection Commission that is highly likely to harm individuals' rights and interests, the General Personal Information Protection manager must report that effect to the Personal Information Protection Commission, pursuant to Order of the Personal Information Protection Commission; provided, however, that this does not apply if the handling of said personal information has been entrusted in whole or in part by another business handling personal information or administrative entities, and another business handling personal information or administrative entities have been notified of the event of a situation, as provided for in the Order of the Personal Information Protection Commission.

2 In cases prescribed in the preceding paragraph, the General Personal Information Protection manager (excluding those that have given a notice under the proviso of that paragraph) must notify the identifiable person of the occurrence of the situation, pursuant to the Order of the Personal Information Protection Commission; provided, however, that this does not apply if it is difficult to notify the identifiable person of the event, and the necessary alternative measures are taken to protect the person's rights and interests.

(Reporting and Measures, etc. for Personal Information Leaks, etc.)

Article 45.

Officers and Employees, who become aware of a problem or threat of a problem in terms of security, such as leakage of retained personal information, must immediately report that effect to the Personal information protection manager who manages the retained personal information; provided, however, that any measures that can be taken shall be implemented immediately to prevent the spread of damage, such as turning off the wireless LAN or unplugging the LAN cable of the terminal suspected of being infected with unauthorized access or malicious programs from the outside.

2 Personal information protection manager shall, upon receiving a report from Officers and Employees pursuant to the provisions of the preceding paragraph, promptly take necessary measures to prevent the spread and restore the damages.

3 The Personal information protection manager shall, promptly after taking the measures set forth in the preceding paragraph, investigate the cause of the incident and damages, and report to the Chief and Assistant general personal information protection managers; provided, however, that if the incident is deemed particularly serious, the Chief and the Assistant general personal information protection managers shall be informed of the details of such an incident, immediately.

4 The General Personal Information Protection manager shall, upon receiving a report under the preceding paragraph, promptly report to the President the details, circumstances, and damages thereof, depending on the nature of the case.

5 The General Personal Information Protection manager shall, depending on the nature of the case, promptly provide information on the details, circumstances and damages thereof to the administrative entity that has jurisdiction over the AMED.

(Measures to Prevent Recurrence of Personal Information Leaks, etc.)

Article 46.

The Personal information protection manager shall, in the event of a leakage of retained personal information or any other problem regarding the management of personal information, analyze the cause of the incident based on the results of the investigation, in accordance with the provisions of paragraph (3) of the preceding Article, take necessary measures to prevent a recurrence of such an incident, and share the measures to prevent recurrence with the Departments/Offices conducting similar operations.

(Publication, etc. of Personal Information Leaks, etc.)

Article 47.

The AMED shall take measures such as publishing the facts and measures to prevent recurrence, and responding to persons of retained personal information related to the incident, depending on the details of the incident and its impact.

2 Regarding incidents to be published, the AMED shall promptly report to the Personal Information Protection Commission on the details, circumstances, and damages thereof.

(Reporting of Specific Personal Information Leaks, etc.)

Article 48.

Officers and Employees shall, upon acknowledging any violation or potential violation of the Individual Number Act, or detecting any serious or potentially serious cases (e.g., a leak of information from the information system handling Individual Numbers to outside parties (including those caused by unauthorized access or malicious programs), the number of identifiable persons in the specific personal information is 101 or more, the information has been made available to an unspecified number of people, the information is taken out by Officers and Employees for fraudulent purposes, and the AMED deems it to be a serious case), immediately report to the Personal information protection manager who manages the specific personal information and prevent the spread of damage.

2 The Personal information protection manager shall, upon receiving a report from Officers and Employees pursuant to the provisions of the preceding paragraph, investigate the facts and determine the cause thereof, and promptly report to the General Personal Information Protection manager and the Assistant general personal information protection manager.
3 The General Personal Information Protection manager shall, upon receiving a report under the preceding paragraph, promptly report to the President the details, circumstances, and damages thereof.
4 The General Personal Information Protection manager shall, in a timely manner (or immediately for any serious or potentially serious cases), report to the Personal Information Protection Commission on the facts and measures to prevent the recurrence of such a case.

(Measures to Prevent the Recurrence of Specific Personal Information Leaks, etc.)
Article 49.
The Personal information protection manager shall specify the scope of the impact caused by the incident assessed in accordance with the provisions of paragraph (2) of the preceding Article, consider measures to prevent recurrence based on the cause identified, and promptly implement them.

(Publication, etc. of Specific Personal Information Leaks, etc.)
Article 50.
The AMED shall, depending on the nature of the incident, promptly inform the identifiable person or make the facts readily available to the identifiable person, and promptly publish the facts and measures to prevent recurrence, to prevent secondary damage and avoid similar incidents, etc.

Chapter 5: Inspection and Audit, etc.

(Inspection)
Article 51.
The Personal information protection manager shall inspect the recording media, processing routes, storage methods, etc. of Retained Personal Information, etc. in the Division and Overseas Office on a regular basis and as needed, and when deemed necessary, report the results of such inspections to the General Personal Information Protection manager.

(Audit)
Article 52.

The Privacy Audit Officer shall conduct regular and necessary audits (including external audits; the same applies hereinafter) of the AMED's management of Retained Personal Information, etc., to verify the appropriate management of Retained Personal Information, etc., and report the audit results to the General Personal Information Protection manager. Audits shall be conducted as focused audits, including on-site audits, depending on confidentiality and other factors of Retained Personal Information, etc.

(Assessment and Review)
Article 53.
The Assistant general personal information protection manager shall assess the measures for the appropriate management of Retained Personal Information, etc. in light of effectiveness, etc. considering the results of inspections or audits, etc., and review the measures when necessary.
2 The Assistant general personal information protection manager shall report to the General Personal Information Protection manager the reviewed results, etc. as specified in the preceding paragraph.

Chapter 6: Provision of Anonymized Personal Information Administrative Entities Hold

(Preparation and Provision of Anonymized Personal Information Administrative Entities Hold)
Article 53-2.
Anonymized personal information shall be handled appropriately in accordance with the provisions of Articles 109 to 123 of the Act.

Chapter 7: Auxiliary Provisions

(Cooperation with Administrative Entity)
Article 54.
The AMED shall, considering the "Basic Policy on the Protection of Personal Information" (Cabinet Decision on April 2, 2004), appropriately manage the personal information it holds in close cooperation with the administrative entity that has jurisdiction over the AMED.

(Formulation of Specifics of the Rules)
Article 55.
In addition to the provisions of these Rules, necessary details regarding the protection of Retained Personal Information, etc. of the AMED shall be determined separately.

Supplementary Provisions

These Rules shall come into effect as of April 1, 2015.

Supplementary Provisions (Rules No. 33 of January 1, 2016)

These Rules shall come into effect as of January 1, 2016.

Supplementary Provisions (Rules No. 50 of April 1, 2016)

These Rules shall come into effect as of April 1, 2016.

Supplementary Provisions (Rules No. 89 of June 30, 2017)

These Rules shall come into effect as of October 10, 2017.

Supplementary Provisions (Rules No. 106 of October 10, 2018)

These Rules shall come into effect as of October 10, 2018.

Supplementary Provisions (Rules No. 33 of March 27, 2020)

These Rules shall come into effect as of April 1, 2020.

Supplementary Provisions (Rules No. 18 of March 24, 2022)

These Rules shall come into effect as of April 1, 2022.

Supplementary Provisions (Rules No. 20 of March 29, 2023)

These Rules shall come into effect as of May 1, 2023.

Supplementary Provisions (Rules No. 28 of March 17, 2025)

These Rules shall come into effect as of April 1, 2025.