BBJ Data Handling Security Guidelines (for Users)

Established on September 14, 2018

Revised on December 23, 2020

Introduction

Biobank Japan (hereinafter referred to as "BBJ") under the Biobank Japan Project for Genomic and Clinical Research operates a biobank in accordance with the BBJ Sample and Data Utilization Guidelines (hereinafter referred to as the "Utilization Guidelines"). These guidelines stipulate the minimum matters that should be complied with in order to utilize the data defined in the Utilization Guidelines for research activities safely without leakage.

While data provided by BBJ is anonymized, the data may include data that can be collated with other information and thereby identify a specific individual. The Data Users, therefore, are required to take measures at a security level designated by BBJ for each type of data: standard level [Type I], high level [Type II], and Statistics Act level.

On the other hand, IT environments vary greatly among the Data Users and change from day to day, which means that compliance with these guidelines may not be enough for data security. The Data Users, therefore, are also required to understand their own IT environments and take additional security measures as necessary by referring to the security regulations of their own organization and other guidelines [1] [2].

These guidelines are to be revised from time to time in accordance with the development of IT environments.

1. Definition of Terms

(1) Data

Data provided by BBJ

(2) Principal Researcher

A principal researcher registered at the time of data utilization application

(3) Data Users

The Principal Researcher and co-researchers

(4) Organization LAN

A LAN of the organization to which Data Users belong. It shall be controlled at a high level of security by limiting its access to the outside to the minimum necessary by using a firewall managed by a network administrator (e.g., limiting IP addresses or ports used for access sources and access destinations).

(5) Limited-access Data Server

An unremovable computer used for saving and calculation of Data. If it is connected to the Organization LAN, connection of the Organization LAN to other devices shall be controlled appropriately by using a firewall.

(6) Terminal

A device that enables access to the Data saved in the Limited-access Data Server without locally saving the Data permanently

(7) Cause-of-death Information

Data of causes of death of research participants that is prepared based on questionnaire information collected through a survey for vital statistics and that is converted in accordance with ICD-10. Only persons who have made an application to the Ministry of Health, Labour and Welfare and obtained its approval may utilize the Cause-of-death Information. For the purpose of these guidelines, the Cause-of-death Information includes information related to causes of death prepared based on treatment information and other relevant information of cooperating medical institutions.

(8) Cause-of-death Information, etc.

The Cause-of-death Information, as well as input and output sheets, checked data, matched data and other product materials containing questionnaire information collected through a survey for vital statistics that are produced in the course of analysis, collection and other handling of the Cause-of-death Information and until the completion of a result table and other final product material

2. Measures Necessary for Standard Level [Type I] Security

2-1. Principles for Data Utilization

The Data provided by BBJ shall be utilized based on the following principles.

(1) The Data shall be saved in a Limited-access Data Server that is connected to the Organization LAN (connection of the Organization LAN to other devices shall be controlled appropriately by using a firewall) or a limited-access Data Server that is not connected to the Organization LAN, and shall not be transferred from such Limited-access Data Server.

(2) If it is inevitably needed to transfer the Data from such Limited-access Data Server for a short period of time within the Organization LAN, such Data shall be deleted promptly after utilization.

(3) A copy of the Data shall not be made, except for the following cases:

- In the case of making a backup copy of the Data;
- In the case of making a copy for a short period of time when transferring the Data; or
- In the case where copies are made by software for a short period of time.

(4) The Data shall be accessed only by the Data Users and only from Terminals.

(5) IT environments vary greatly among the Data Users and change from day to day, which means that compliance with these guidelines may not be enough for data security. The Data Users shall understand their own IT environments and take additional security measures as necessary by referring to the security regulations of their own organization and other guidelines [1] [2].

2-2. Matters That Should Be Complied with by the Principal Researcher and co-researchers

(1) For general utilization

(i) Ensure that the Data Users understand and comply with the BBJ Data Handling Security Guidelines.

(ii) Manage information on the Data Users and Limited-access Data Servers (including storage locations within a file system) by an electronic file or any other ledger that only the Data Users can access, and update the information every time when a change occurs. Keep the history of changes for subsequent check. Acquire access logs of user authentication, connection, and operation, and manage the trails appropriately.

(iii) Respond to an audit on the implementation status of security measures which audit is to be conducted by a third party at the request of the BBJ Sample and Data Utilization Review Committee or BBJ.

(iv) Submit a "BBJ Data Handling Security Guideline Checklist" to the Office of BioBank Japan at the time of the utilization application and every August; provided, however, that in the case where the last day of August comes within six months from the starting day of utilization, the submission for August at that occasion is not required.

(2) For Limited-access Data Servers

(i) Have in place a server (including virtual server) for exclusive use and a file system that have been submitted at the time of the data utilization application. If it is inevitably needed to use the server or system jointly with users other than the Data Users, grant access authority for a folder containing the Data only to the Data Users.

(ii) When connecting to a network, use the Organization LAN and satisfy the following requirements:

- Apply the latest security patches as much as possible; and
- Activate the firewall that comes with the OS (e.g., iptables in the case of Linux) at the minimum so that connection from the Organization LAN will be limited appropriately by the administrator.

(iii) Do not share a user ID or a password for a Limited-access Data Server even among the Data Users, and use a password that is strong enough to prevent others from guessing its combination.

(iv) Do not install unnecessary software. Especially, do not install file-sharing (file-exchange or P2P) software (e.g., Winny and BitTorrent).

(v) Stop unnecessary processes that automatically start running at the time of activation of an OS as much as possible.

(vi) In the case of making copies of the Data in more than one Limited-access Data Server for distributed processing or any other similar purpose, ensure that additional servers also satisfy the above requirements (i) to (v).

2-3. Matters That Should Be Complied with by the Data Users

(1) When logging in to a Limited-access Data Server, encrypt the communication path with adequate strength.

(2) When leaving a Terminal, log out from the Limited-access Data Server or lock the Terminal. Moreover, use a function that locks the screen when a Terminal is not operated for a certain period of time (about 15 minutes).

(3) Do not make a copy of the Data on the screen of a Terminal to save it in a local disk. It is preferable to use a Terminal that cannot make a copy of the Data on the screen to save it in a local disk.

(4) In the case where a Terminal has a function of saving data automatically (so-called cache function), deactivate the function.

(5) Do not access the Data from a Terminal that is used by many and unspecified users (e.g., PC of an Internet

cafe).

(6) Apply the latest security patches to Terminals.

(7) When making a backup, satisfy one of the following requirements:

- In the case of saving the backup in a server or any other unremovable device, meet the requirements specified in "2-2. Matters That Should Be Complied with by the Principal Researcher and co-researchers—For Limited-access Data Servers."
- In the case of saving the backup in a removable device (e.g., tape, USB flash drive, CD-ROM, and notebook PC), encrypt the backup data and delete it after utilization. Moreover, manage the removable devices by an electronic file or any other ledger that only the Data Users can access in order to minimize the risks of theft and loss, as well as to enable early detection of such accidents.

(8) If it is inevitably needed to use a removable device for transfer of the Data for a short period of time, handle the Data in the same way as backup data.

(9) If it is inevitably needed to print out the Data, strictly manage the printed copy so that it will be available only to the Data Users, and shred it after utilization.

(10) When completing utilization of the Data, delete the Data from all devices. Moreover, it is preferable to delete temporary files that are created in the course of calculation frequently.

3. Measures Necessary for High Level [Type II] Security

In addition to "2. Measures Necessary for Standard Level [Type I] Security" above, the following measures shall be taken for Limited-access Data Servers.

Limited-access Data Servers shall be placed in a server room that satisfies all of the following requirements.

(1) Persons entering the room shall be limited by means of multi-factor authentication that uses two or more of the following three authentication methods:

- Biometric authentication (e.g., palm veins, fingerprint, iris, and face)
- Object-based authentication (e.g., IC card, one-time password, and USB token)
- Knowledge-based authentication (e.g., password)

(2) The record of entry shall be kept automatically and shall be available for future audits.

(3) The server room shall be used exclusively for purposes submitted at the time of the application. If a server room for exclusive use cannot be secured, Limited-access Data Servers shall be placed on a server rack for exclusive use that is always locked.

4. Measures Necessary for Statistics Act Level Security

When utilizing the Cause-of-death Information, etc., the Data Users shall, until completion of the utilizatio n, comply with the Statistics Act and the Regulation for Enforcement of the Statistics Act, and shall man age the Cause-of-death Information, etc. appropriately by the management methods submitted based on the "Ministry of Health, Labour and Welfare Processing Manual for Provision of Questionnaire Information B ased on Article 33 of the Statistics Act" [3]. For appropriate management of the Cause-of-death Informatio n, etc., the following measures shall be taken.

(1) For utilization of the Cause-of-death Information, etc. (including storage of data files of the Cause-of-death Information), a place (within Japan) that can be locked physically shall be used so that the information cannot be brought out from the place, and entry to and exit from the utilization place shall be controlled so that a person in the utilization place at the time of utilization of the Cause-of-death Information, etc. can be checked.

(2) The Cause-of-death Information, etc. shall be stored in a prescribed medium, and the medium shall be stored in a cabinet or any other container that can be locked. Limited-access Data Servers and Terminals that use the Cause-of-death Information, etc. shall be fixed with wire or any other similar means or kept in a cabinet or any other container that can be locked when they are not being used. Moreover, security measures shall be taken so that the Cause-of-death Information, etc. cannot be brought out wrongfully from the utilization place.

(3) For deletion of the Cause-of-death Information, etc., and disposal of devices and other media containing the Cause-of-death Information, etc., a specialized tool or any other means that makes the information unrecoverable shall be used.

(4) For an information system using the Cause-of-death Information, etc., preventive measures against unauthorized operation, such as user identification and authentication, and screen lock, shall be taken so that persons other than the Data Users cannot access a computer containing the Cause-of-death Information, etc.

(5) For an information system using the Cause-of-death Information, etc., preventive measures against unauthorized access, such as measures against computer viruses and security holes, shall be taken.

(6) In the case where a computer that may be connected to an external network or a computer that may be used by persons other than the Data Users is to be used, preventive measures against leakage and other accidents of the Cause-of-death Information, etc. (including disposed of information) shall be taken by, for example, conducting data collection and other operations offline and leaving none of the Cause-of-death Information, etc. in the computer after the operations, or monitoring downloading and uploading.

(7) An “Administrative File for Cause-of-death Information” shall be used to record the status of utilization by each Data User. Moreover, storage and management of the Cause-of-death Information, etc. shall be conducted by the Principal Researcher.

(8) If leakage, loss or alteration of the Cause-of-death Information, etc. occurs, or its sign is detected, measures shall be taken immediately in order to prevent the damage from spreading and prevent occurrence of the secondary damage and recurrence of similar accidents, and report to the Office of BioBank Japan shall be made.

4. Contact Information for These Guidelines

Office of BioBank Japan
4-6-1 Shirokanedai, Minato-ku, Tokyo 108-8639
Tel./Fax: 03-5449-5122

References

[1]. Wellcome Trust Sanger Institute. WTSI Human Data Security Policy (October 2015). https://www.sang

er.ac.uk/legal/assets/wtsi-hgdsp-201510hpfinal.pdf

[2]. Ministry of Health, Labour and Welfare “Security Guidelines for Medical Information Systems Version 5 (May 2017)”https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf

[3]. Ministry of Health, Labour and Welfare “Ministry of Health, Labour and Welfare Processing Manual f or Provision of Questionnaire Information Based on Article 33 of the Statistics Act (May 1, 2019)”https://www.mhlw.go.jp/toukei/sonota/chousahyo.html