

About Ensuring Awareness of the Matters Regarding Disclosure of Retained Personal Data

Bosch Health Insurance Society (hereinafter referred to as "Society"), in accordance the Personal Information Protection Act, will respond to Requirement of Disclosure etc. of Retained Data (Notification of Purpose of Use, Disclosure, Correction, Addition or Deletion of Content, Suspension of Use, and Erasure) in accordance with the following guidelines.

1. Organization Name, Address, and Representative

Organization Name: Bosch Health Insurance Society

Address: 5-5 Yakyu-cho 2-choume, Higashimatsuyama City, Saitama

Representative: Chairman of the Board

2. Personal Information Protection Supervisor, Affiliation, and Contact

Supervisor: Manager

Affiliation: Secretariat

Contact: 0493-22-0890

3. Purpose of Retained Personal Data Use

(1) Personal Information of Members, etc.

- For various procedures, such as applications and contracts, related to the use of our health care activities, health checkups, and medical treatment services
- For communication related to the use of our health care activities, health checkups, and medical treatment services

(2) Personal Information of Employees (including job applicants and retired employees)

- For personnel and labor management such as employment and recruitment, and for on-the job confirmation related to accounting and general affairs, etc.

(3) Personal Information of Contracted Employees

- For verifying the identity of the person himself / herself based on the performance of various contracts

(4) Security Camera Footage

- For crime prevention and disaster prevention

4. Scope of Disclosure, etc.

The scope of disclosure, etc. is, other than individual's address, name, the purpose of use by Society, limited to the information included in the retained personal data that has been acquired and is currently held by Society.

5. Where to request the disclosure, etc.

If you want to the disclosure, etc., please apply by postal mail attaching the necessary documents on the designated application form to the address listed below.

〒355-0028

5-5 Yakyu-cho, 2-chome, Higashimatsuyama City, Saitama

"Bosch Health Insurance Society, Secretariat, Administration Office,
Customer Consultation Desk"

6. Documents etc. to be Submitted When Requiring Disclosures

If you yourself require disclosures, etc., filling out all designated information included in the "Application Form of Personal information Disclosure, Correction, Addition, Deletion, and Suspension of Use", enclosing the document verifying your identification together, mail them to the address listed above 5 (Customer Consultation Desk) by the method that leaves a sending record such as a registered mail.

If your present address and the address in the data held by Society is different, please submit a document that shows your relocation history.

In the meanwhile, if your permanent address or other information is listed on the document below, please black out the relevant sections beforehand so that they are illegible.

(1) When making a requirement by the person himself / herself

1. Application Form of Personal information Disclosure, Correction, Addition, Deletion, and Suspension of Use
2. Document for verifying the identity of the person himself / herself ※One of the following from a to c:
 - a. Copy of Driver's License
 - b. Copy of Passport
 - c. Copy of Alien Registration Certificate

(2) Requests by Legal Representative of a Minor or Adult Ward

1. Application Form of Personal information Disclosure, Correction, Addition, Deletion, and Suspension of Use
2. Document for verifying the identity of the person himself / herself
※Same as above (1) - 2
3. Copy of Family Register
4. Documents for Identification of the Legal Representative of the Minor or Adult Ward himself / herself ※Same as above (1) - 2
5. Certificate of Registration Evidencing Adult Guardian (Only for Adult Ward)

(3) Requests for Disclosure, etc. Made by an Agent Delegated by the person himself / herself

1. Application Form of Personal information Disclosure, Correction, Addition, Deletion, and Suspension of Use
2. Seal Certificate of the person himself / herself※Issued within the last three months
3. Document for verifying the identity of the person himself / herself
※Same as above (1) – 2
4. Document for verifying the identity of the agent himself / herself

※Same as above (1) - 2

5. Power of Attorney

6. Recipient of Disclosure Results: If an agent receives the results of disclosure, etc. from Society, you are requested to write "I delegate the authority to receive the results of disclosure, etc. to the agent." on the power of attorney.

In this case, you are also requested to stamp your own registered seal to the power of attorney and submit it together with the registered seal certificate.

Please note that if the statement of your delegating the authority to receive the results of disclosure, etc., is not written, if your official seal is not stamped, and if a seal certificate is not submitted, Society notifies the results of disclosure, etc. to the person himself / herself.

7. Disclosure Costs

1) The disclosure fee is ¥300 per requirement

2) Costs related to confirming disclosure, etc.

3) If a decision is made to disclose information after disclosure requirement, in addition to the disclosure fee, ¥10 per A4 document is charged.

4) If sending by postal mail is required, you will be charged the equivalent postage amount (registered mail, certified mail, express mail).

8. How we respond to requirement of disclosure, etc.

Concerning the requirement of disclosure, etc., as a general rule, we respond using the method you specify. However, if you do not specify a method, or if Society determines that it would be difficult to respond using your specified method due to the reason that using the specified method would be prohibitively expensive etc., we may respond in writing.

If we respond in writing, we will send the response by registered mail to the address written on the requirement.

If we respond electronically, we send an email to the email address listed on the requirement.

9. Regarding the handling of personal information obtained in connection with requirement of disclosure, etc.

Personal information obtained in connection with requirement of disclosure, etc. will be handled only to the extent necessary to respond to the requirement.

After responding to the requirement of disclosure, etc., submitted documents will be securely stored and managed as records for a certain period of time and then disposed of in an appropriate manner.

10. Regarding non-disclosure of retained personal data, if any of the following reasons apply, we will be unable to accommodate your requirement of disclosure, etc. However, we will notify you of this and the reasons.

- (1) If we cannot verify the identity of the person himself / herself
- (2) If we cannot verify the power of attorney
- (3) If we cannot verify the identity of the agent
- (4) If the documents are incomplete
- (5) If the information in the requirement does not allow Society to identify the retained personal data
- (6) If the requested disclosure does not fall within the scope of the retained personal data
- (7) If there is a risk of harm to the life, body, property, or other rights and interests of the individual or a third party
- (8) If there is a risk of significant disruption to the proper performance of Society activities
- (9) If violation of laws and regulations is caused

11. Other Notes

Depending on the content of your requirement, it may take some time for us to respond.

12. Where to file complaints regarding the handling of retained personal data

Complaints Handling Desk Manager: Secretariat, General Affairs Section,
Contact (Telephone): 0493-22-0890

13. Name of Certified Personal Information Protection Organization and Contact for Complaint Resolution

Name of Certified Personal Information Protection Organization:

Japan Institute for Promotion of Digital Economy and Community (JIPDEC)

Complaint Resolution Contact:

Accredited Personal Information Protection Organization

Address: 〒106-0032

Roppongi First Building, 9-9 Roppongi 1-chome, Minato-ku, Tokyo

Telephone Number: 03-5860-7565, 0120-700-779 (Toll-Free)

[This is not a contact point for inquiries regarding Society.]

14. Measures Taken for Secure Management of Retained Personal Data

(1) Establishment of Basic Policy

To ensure the proper handling of personal data, we established "Personal Information Protection Policy."

(2) Improvement of Disciplines for Handling Personal Data

We improved internal regulations regarding the protection and use of personal information establishing the rules about handling methods, responsible person, and person in charge for each process of acquisition, use, transfer, storage, provision, deletion, and disposal of personal data.

(3) Organizational Security Control Measures

In accordance with our internal regulations regarding the protection and use of personal information, we are implementing the following organizational safety management measures.

- Appointing a person responsible for handling personal data and clarifying his / her responsibilities
- Clarifying the staffs who handle personal data and their roles
- Establishing the procedures for handling personal data from acquisition to disposal and ensure thorough management in accordance with the procedures
- Establishment of a system for prompt response and reporting in the event of a violation of internal regulations or an occurrence of a personal data leak.
- Regular inspection of the personal data handling, review of security control measures and implementation of improvement

(4) Personnel Security Control Measures

In accordance with internal regulations regarding the protection and use of personal information, we implement the following personnel security control measures.

- Training, etc. of all staffs on the handling of personal data
- Concluding confidentiality agreements with all staffs regarding the handling of personal data

(5) Physical Security Measures

In accordance with internal regulations regarding the protection and use of personal information, the following physical security measures are implemented:

- Management of areas where personal data are handled
- Prevention of theft of devices and electronic media, etc.
- Prevention of leaks when electronic media, etc. are carried
- Deletion of personal data and disposal of devices, electronic media, etc.

(6) Technical Security Control Measures

- Access restrictions
- Identification and authentication of accessors
- Prevention of unauthorized external access, etc.
- Prevention of leaks, etc. associated with the use of information systems
- Prevention of accidents during telework