ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Japan

Status of Consent for Processing Personal Data

SEPTEMBER 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Professor Masahiro Sogabe

Kyoto University

Professor Yuko Nishitani

Kyoto University

Ryoya Shibaike

Kyoto University

Takeshige Sugimoto

Managing Director and Partner, S&K Brussels LPC

ACKNOWLEDGEMENTS

This Report benefitted from contributions and editing support from Catherine Shen.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1. Act on Protection of Personal Information ("APPI") 1
1.2. Amendments to the APPI 1
1.3. Other relevant laws and regulations 2
2. ROLE OF THE PERSONAL INFORMATION PROTECTION COMMISSION ("PPC") 2
2.1. Advisory 2
2.2. Enforcement 2
3. SECTORAL GUIDELINES 4
3.1. Financial sector 4
3.2. Healthcare sector 4
3.3. Information and Communications sector 5
4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE APPI 5
5. CONDITIONS FOR CONSENT 6
5.1. Definition and forms of consent 6
a. Informed consent 6
b. Express and implied consent 7
c. Formalities in sector-specific guidelines 9
5.2. Withdrawal of consent 9
5.3. Bundled consent 9
6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA 9
6.1. Children 10
6.2. Cookies and online tracking 11
6.3. Direct marketing 11
6.4. Biometric data 11
6.5. Genetic data 12
6.6. Financial information 12
6.7. Pseudonymized data 12
7. CONSENT FOR CROSS-BORDER DATA TRANSFERS 12
8. TRANSPARENCY AND NOTICE 13
9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT 14
10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW 14
10.1. Using and disclosing personal information without consent under the APPI 14
a. Where permissible by law 15

b. Protection of life, body, or fortune 16
c. Public health....17
d. Cooperation with public bodies 18
10.2. Using and disclosing sensitive personal information without consent under the APPI 18
a. Healthcare sector 19
b. Credit sector 20
10.3. Exemptions to the APPI....20
10.4. Research purposes (including medical research)....20

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Japan's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

Japan's legal framework for data protection and privacy is based on Article 13 of the Constitution, which provides: "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs."

Based on this Article, Japan's Supreme Court has recognized a constitutional right to privacy and data protection.[1] In a 1969 decision, the Court held that every individual has the liberty of protecting his/her personal information from disclosure to a third party or the public without good reason.[2]

1.1. Act on Protection of Personal Information ("APPI")

The primary legislation in Japan governing the collection, use, and disclosure of personal information is the Act on the Protection of Personal Information ("**APPI**"), which took effect in 2003.[3] The APPI applies to the handling of the "**personal information**"[4] of "**principals**"[5] (i.e., data subjects) in Japan by, among others, "**personal information handling business operators**" ("**PIHBOs**").[6]

1.2. Amendments to the APPI

The APPI was substantially amended in 2015, 2020, and 2021. These amendments did not significantly impact the APPI's notice and consent framework.

The 2015 amendments, among others, introduced a set of enforceable rights and established an independent supervisory authority to oversee and enforce the APPI, the Personal Information Protection Commission ("**PPC**").

The 2020 amendments clarified the extraterritorial application of the APPI and disclosure and due diligence requirements for cross-border data transfer and introduced a mandatory data breach notification scheme and new categories of "pseudonymously processed personal information," "personally referable personal information," and "anonymous personal information."[7]

---

[1] Supreme Court, Judgment of the Grand Bench of 24 December 1969, Keishu Vol. 23, No 12, p. 1625.

[2] This holding was upheld in a 2008 decision of the Supreme Court (Supreme Court, Judgment of 6 March 2008, Minshu Vol. 62 No. 3, p. 665).

[3] Act No. 57 of 2003 (last amended by Act No. 37 of 2021), available in Japanese at https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000057. Note that there used to be equivalent legislation for administrative entities (the Act on the Protection of Personal Information Held by Administrative Organs, and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies), but these Acts have were abolished and incorporated into Chapter V of the APPI following the 2021 amendments to the APPI.

[4] **"Personal information"** is defined as information relating to a living individual that contains a description that has been stated, recorded, or otherwise expressed, whereby a specific individual can be identified (whether alone or in combination with other information), or which contains an "individual identification code" prescribed by cabinet order (APPI, Article 2(1) – see also Cabinet Order No. 507 of 2003, Article 1 for individual identification codes). Under the APPI, "personal information" is distinct from "**personal data**" (APPI, Article 16(3)) – the latter refers to personal information constituting a "**personal information database,**" i.e., a collective body of information containing personal information, which is systematically organized so that personal information is searchable by a computer (APPI, Article 16(1)).

[5] "**Principal**" is defined as the specific individual identified by personal information (APPI, Article 2(4)).

[6] APPI, Article 16(2). Specifically, this term refers to persons providing a "personal information database" (see above) for use in business.

[7] For further information on the 2020 amendments, please refer to Takeshige Sugimoto, Akihiro Kawashima, Tobyn Aaron, "A New Era for Japanese Data Protection: 2020 Amendments to the APPI" *Future of Privacy Forum Blog* (April 13, 2021), available at https://fpf.org/blog/a-new-era-for-japanese-data-protection-2020-amendments-to-the-appi/.

The 2021 amendments, among others, established a unified data protection system for both businesses and administrative entities of central and local governments, expanded the scope of an exemption to the APPI for use of personal information in academic studies, and introduced more detailed regulations.

1.3. Other relevant laws and regulations

The APPI is supplemented by various implementing rules and regulations, including the Implementation Rules on the APPI,[8] issued in 2016, and the Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision,[9] issued in 2018.

In 2016, the Cabinet of Japan (the Prime Minister and Ministers forming his government) issued an order pursuant to Article 7 of the APPI to promote measures concerning the protection of personal information ("**Cabinet Order**").[10] The Cabinet Order was amended in 2018 to facilitate cross-border data transfers and to empower the PPC to issue stricter rules than those under the APPI and the Cabinet Order.

2. ROLE OF THE PERSONAL INFORMATION PROTECTION COMMISSION ("PPC")

The APPI establishes the PPC as an independent entity which is responsible for administering the APPI.[11]

2.1. Advisory

The PPC has published several guidelines which aid in the interpretation of the APPI, including elaborating in detail on key terms in the APPI and providing examples of how the APPI's provisions are applied in practice, especially for specific sectors.

In 2016, the PPC issued comprehensive guidelines on the APPI ("**General Guidelines**"), which were partially revised in 2021.[12] These Guidelines are of general application and should be followed even where sector-specific guidelines apply.

In 2017, the PPC released further guidance in a question-and-answer format ("**PPC Q&A**")[13] which addresses the application of the APPI to a wide range of common business situations.

2.2. Enforcement

The PPC is empowered to request documents on PIHBOs' processing operations and to carry out inspections, both on-site and of books or other documents.[14] To the extent necessary to enforce the APPI, the PPC may also provide PIHBOs with guidance or advice regarding their handling of personal information.[15]

Most importantly, the PPC has the power – acting on a complaint or its own initiative – to issue recommendations and orders to enforce the APPI and other binding rules in individual cases.[16]

---

[8] PPC Rules No. 3 of 2016 (last amended by the PPC Rules No. 4 of 2021), available in Japanese at https://elaws.e-gov.go.jp/document?lawid=428M60020000003.
[9] Available in Japanese at https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf and in English at https://www.ppc.go.jp/files/pdf/supplementary_rules_eu_uk.pdf.
[10] Cabinet Order No. 507 of 2003 (last amended by Cabinet Order No. 292 of 2021).
[11] See, generally, APPI, Chapter VI.
[12] Available in Japanese at https://www.ppc.go.jp/files/pdf/211116_guidelines01.pdf.
[13] Available in Japanese at https://www.ppc.go.jp/files/pdf/2205_APPI_QA.pdf.
[14] See, generally, APPI, Article 146.
[15] APPI, Article 147.
[16] APPI, Article 148.

Specifically, Article 148 of the APPI provides for a two-step mechanism for addressing violations of certain requirements under the APPI, including, among others:

- handling personal information beyond the scope necessary to achieve the utilization purpose without the principal's consent or a valid exception, in violation of Article 18 of the APPI;
- acquiring personal information by deceit or improper means, in violation of Article 20(1) of the APPI;
- handling personal information requiring special care without the principal's consent or a valid exception, in violation of Article 20(2) of the APPI;
- failing to comply with notice requirements in Article 21 of the APPI; or
- disclosing personal information to a third party without the principal's consent or a valid exception, in violation of Article 27 or Article 28 of the APPI.

The PPC must first make a non-binding recommendation to a PIHBO to cease a violating act or take such other action as is necessary to rectify the violation.[17]

Thereafter, if the PIHBO fails to comply with the recommendation "without legitimate grounds," and the PPC "recognizes that a serious infringement of an individual's rights and interests is imminent," the PPC may make a binding order for the PIHBO to take action in line with the recommendation.[18] This two-step mechanism is not required in cases of urgency.[19]

Non-compliance with an order issued by the PPC is a criminal offense punishable with imprisonment with labor for up to one year or a fine of up to 1,000,000 yen.[20] Furthermore, pursuant to Article 182(i) of the APPI, lack of cooperation with the PPC or obstruction to its investigation is punishable with a fine of up to 500,000 yen.[21] These criminal sanctions apply in addition to those that may be imposed for substantive violations of the APPI.

The notice and consent provisions have been effectively enforced by the PPC so far. One notable case concerned Recruit Career, a PIHBO that provided web services related to student employment activities.

In August 2019, the PPC found that this PIHBO had, among others, provided students' personal information to third parties without obtaining the students' consent, in violation of Article 23(1) of the APPI.

The PPC found that the personal information handled by the PIHBO was job-related information that could affect the lives of students and that the PIHBO had handled personal information entrusted to it by other PIHBOs. In addition to those findings, the PPC found that there was no internal system within Recruit Career to prevent, discover, and correct deficiencies related to privacy policy and that the PIHBO has given no appropriate judgment or consideration to compliance with the APPI. After making these findings, the PPC advised Recruit Career to implement the following measures within approximately one month from the date that the advice was provided:

- take necessary measures, such as reviewing the organizational structure and reforming the mindset of the entire company including the management team, so as to properly protect the rights and interests of individuals when handling personal information;
- design, and operate a system for handling personal information in accordance with the APPI for new any services that the PIHBO implemented in future.

Additionally, in December 2019, the PPC determined that Recruit Career had committed another violation of the APPI by providing students' personal information (specifically regarding declined job offers) to third parties without having obtained valid consent from those students. The PPC therefore advised Recruit Career to review its organizational structure and reform the mindset of the entire company, including its top management team, to protect the rights and interests of individuals. In particular, the PPC advised the company to:

---

[17] APPI, Article 148(1).
[18] APPI, Article 148(2).
[19] APPI, Article 148(3).
[20] APPI, Article 178.
[21] APPI, Article 182(i).

- set up an organizational structure to consider and design lawful handling of personal information when considering new products;
- properly notify principals of the utilization purpose and disclose such purpose publicly by specifying as much as possible the content of the products when collecting personal information; and
- take necessary actions, including exercising necessary and appropriate supervision over its trustees when entrusting the handling of personal information with those trustees.

3. SECTORAL GUIDELINES

3.1. Financial sector

In 2017, the PPC, in conjunction with other government agencies, released several guidelines on personal data protection in the financial sector, namely:

- Guidelines for Personal Information Protection in the Credit Sector ("**Credit Sector Guidelines**"),[22] released in conjunction with the Ministry of Economy, Trade, and Industry ("**METI**");
- Guidelines for Personal Information Protection in the Financial Sector ("**Financial Sector Guidelines**"),[23] released in conjunction with the Financial Services Agency ("**FSA**"); and
- Practical Guidelines for Security Policies regarding Protection of Personal Information in the Financial Sector,[24] released in conjunction with the FSA.

Also in 2017, the Ministry of Justice issued its Guidelines concerning the Protection of Personal Information in the Debt Collection Service Sector ("**Debt Collection Sector Guidelines**").[25]

3.2. Healthcare sector

In 2017, the Ministry of Health, Labor, and Welfare ("**MHLW**") issued Guidance for the Appropriate Handling of Personal Information by Medical or Long-Term Case Businesses ("**Medical Sector Guidelines**").

These guidelines provide detailed explanations and examples of how the APPI's requirements apply to businesses operators in the medical sector, such as private hospitals, clinics, pharmacies, and persons who provide in-home services under Japan's Long-Term Insurance Act.

Also in 2017, the MHLW issued two sets of guidelines for health insurance associations, namely:

- Guidance for the Appropriate Handling of Personal Information at Health Insurance Associations ("**Health Insurance Association Guidelines**");[26] and
- Guidance for the Appropriate Handling of Personal Information at National Health Insurance Associations ("**National Health Insurance Association Guidelines**").[27]

Lastly, in 2004, the METI issued Guidelines for the Protection of Personal Information in the Economic and Industrial Sector Using Personal Genetic Information ("**Genetic Information Guidelines**"). These guidelines were revised in 2008 and 2014.[28]

---

[22] Available in Japanese at https://www.ppc.go.jp/files/pdf/shinyou_GL.pdf.
[23] Available in Japanese at https://www.ppc.go.jp/files/pdf/kinyubunya_GL.pdf.
[24] Available in Japanese at https://www.ppc.go.jp/files/pdf/zitsumushishin.pdf.
[25] Available in Japanese at https://www.moj.go.jp/content/001218341.pdf.
[26] Available in Japanese at https://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/0000168757.pdf.
[27] Available in Japanese at https://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/0000168758.pdf.
[28] Available in Japanese at https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/bio/kojin_iden/pdf/009_s01_00.pdf.

3.3. Information and Communications sector

The PPC has also issued, among others, the Guidelines for the Protection of Personal Information in the Electronic Communications Sector.[29]

4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE APPI

The APPI does not require consent for every collection or use of personal information and instead, permits PIHBOs to collect and/or use personal information for a lawful purpose (the "**utilization purpose**"), which must be specified as explicitly as possible,[30] without also requiring the PIHBO to obtain the principal's consent in relation to the collection or use.

On obtaining personal information, a PIHBO must promptly inform the principal of the PIHBO's utilization purpose for that personal information or disclose the utilization purpose to the public (i.e., via a privacy policy).[31] Where a PIHBO acquires personal information from another business operator, the PIHBO is, in principle, free to set a new utilization purpose.

Even though the APPI does not require consent in the above circumstances, collection and use of personal information is still subject to constraints.

In particular, the PIHBO may only use the personal information without the principal's consent to the extent that such use is:

- necessary to achieve the utilization purpose[32] and
- within a scope that would reasonably be recognized as relevant to the original purpose.[33]

Further, all handling of personal information must be lawful and fair as the APPI prohibits a PIHBO from acquiring personal information by deceit or other improper means[34] and from using personal information in a manner that has the possibility of fomenting or prompting an unlawful or unfair act.[35]

Consent plays a number of important, albeit secondary, roles in the APPI, which allow principals to exercise a degree of control over how a PIHBO uses their personal information.

By default, a PIHBO must obtain a principal's consent in advance in order to:

- handle personal information beyond the scope necessary to achieve the utilization purpose;[36]
- disclose personal information about the principal to a third party;[37]
- obtain and handle "personal information requiring special care" (i.e., a class of sensitive personal information recognized by the APPI);[38] and/or
- disclose personal information to a third party.[39] Note that where personal information is disclosed to a third party, a PIHBO must also, among others, keep a record of the fact that the principal has given consent for such disclosure.[40]

---

[29] Available in Japanese at https://www.ppc.go.jp/files/pdf/telecom_GL.pdf.
[30] APPI, Article 17(1). See also General Guidelines, section 3-1-1.
[31] APPI, Article 21(1).
[32] APPI, Article 18(1).
[33] APPI, Article 17(2).
[34] APPI, Article 20(1).
[35] APPI, Article 19.
[36] APPI, Article 18(1).
[37] APPI, Article 27(1).
[38] See "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA" below for further information on the scope of the term "personal information requiring special care."
[39] APPI, Article 27(1). Note that disclosure of personal information to certain entities would not be deemed to be a disclosure to a third party for purposes of this provision (APPI, Article 27(5)).
[40] APPI, Article 30(3).

Though the APPI provides a number of exceptions to these consent requirements, these exceptions are generally only available where it is difficult to obtain the principal's consent[41] or where seeking consent would interfere with performance of a lawful function by a public authority.[42]

Lastly, consent is also one of the main legal bases under the APPI for transferring personal information from Japan to a third country.[43]

Certain guidelines also specifically require consent rather than notification to handle personal information for certain utilization purposes. Specifically:

- PIHBOs in the financial sector must obtain consent to use of personal information for purposes of providing credit[44] and must obtain informed consent to disclosure of personal information to a personal credit information agency.[45]
- The Health Insurance Association Guidelines and the National Health Insurance Association Guidelines require consent to use of personal information for provision of insurance benefits to insured persons (though note that such consent can be inferred in certain circumstances – see below).[46]

Although the APPI does not require consent for all use of personal information, PIHBOs in practice commonly obtain consent from a principal to demonstrate that they have complied with their obligation to inform the principal of the utilization purpose in relation to that personal information.

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

The APPI does not define consent or explain the forms that valid consent can take.

However, guidance provided by the PPC in the General Guidelines suggests that consent must minimally be:

- **specific** – in that the General Guidelines define consent as consent as "the individual's consent to the handling of personal information *in the manner indicated by the PIHBO*" (emphasis added)[47] – and
- **voluntary** – in that the General Guidelines require a PIHBO, when obtaining a principal's consent, to provide the principal with a reasonable and appropriate method to make a decision.[48] Note also that the APPI prohibits a PIHBO from acquiring personal information by deceit or other improper means.[49]

a. Informed consent

Generally, the APPI requires a PIHBO to inform principals of the utilization purpose in relation to the principal's personal information regardless of whether the PIHBO seeks consent from principal for activities in relation to that information.[50]

However, the APPI does specifically require that consent must be informed where consent is sought to transfer personal information to a third party located outside of Japan.[51]

---

[41] APPI, Articles 18(3)(ii), 18(3)(iii), 20(2)(ii), 20(2)(iii), 27(1)(ii), and 27(1)(iii).
[42] APPI, Articles 18(3)(iv), 20(2)(iv), and 27(1)(iv).
[43] APPI, Article 28(1).
[44] Financial Sector Guidelines, Article 2(3).
[45] Financial Sector Guidelines, Articles 2(4) and 12(2); Credit Sector Guidelines, section II(2)(5).
[46] Health Insurance Association Guidelines, section II(8); National Health Insurance Association Guidelines, section II(8).
[47] General Guidelines, section 2-16.
[48] General Guidelines, section 2-16.
[49] APPI, Article 20(1).
[50] APPI, Articles 21(1) and 21(2).
[51] APPI, Article 28(2). See "CONSENT FOR CROSS-BORDER DATA TRANSFERS" below.

Additionally, certain sectoral guidelines also require consent to be informed under certain circumstances and to that end, prescribe certain information that must be provided to principals before their consent will qualify as informed. In particular, consent for disclosure of personal information to a personal credit information agency is only valid if the method by which a PIHBO obtains consent (e.g., a contract) provides sufficient detail to enable the person to determine whether or not to give consent to such disclosure.[52]

Additionally, the Genetic Information Guidelines require informed consent for handling of personal genetic information.[53] Such consent must be accompanied by a written explanation of certain prescribed matters, including:

- the significance, purpose, and method of handling;
- the method and contact details required to withdraw informed consent;
- contact details of the PIHBO or its representative;
- specific anonymization methods and security control measures employed at each stage of handling of the personal information, from acquisition to disposal of samples;
- whether analysis is outsourced to another business entity, and if so, the contact details of that entity;
- the fact that the project has been reviewed in a fair and neutral manner by the Personal Genetic Information Handling Review Committee;
- matters concerning the disclosure of personal genetic information (including the address and method of acceptance, and whether a fee is charged for disclosure);
- availability of genetic counseling; and
- contact information for inquiries, complaints, etc.[54]

b. Express and implied consent

Express consent would be recognized as valid for purposes of the APPI's consent requirements.

This interpretation is supported by the General Guidelines, which list a number of examples of usual business practices in Japan for obtaining consent[55] – all of which, notably, constitute express forms of consent. These include oral agreement, returning forms or other documents, agreement via e-mail, ticking a box on a web page, clicking on a home page, using a consent button, or tapping a touch panel.

The PPC Q&A recognizes that implied consent could, in principle, apply in appropriate cases[56] but does not provide examples of possible cases where implied consent may be recognized.

There appear to be limits to the circumstances in which implied consent may be recognized as the PPC Q&A emphasizes that consent must be obtained using a rational and appropriate method that enables the principal to make a decision regarding whether to give consent[57] and notably, appears to reject deemed consent by notification: for example, there is no valid consent where a PIHBO sends a notification (e.g., by email) to the principal stating that the principal's consent will be deemed if the principal does not respond within a certain period of time, and thereafter, the principal does not respond within the prescribed period.[58]

---

[52] Financial Sector Guidelines, Article 11(2). See also Credit Sector Guidelines, section II(2)(v).

[53] Genetic Information Guidelines, section II(1-4)(xxv). Note that "**informed consent**" is defined as consent given by a principal freely after receiving a sufficient explanation from the PIHBO as to how it will handle personal genetic information and having understood the significance, purpose, methods, expected results, disadvantages, and accuracy of the handling (Genetic Information Guidelines, section II(1-3)(xix)). Further, "**personal genetic information**" is defined as information that indicates an individual's genetic characteristics or constitution based on such characteristics, and that can be used to identify an individual (Genetic Information Guidelines, section II(1-1)(v)).

[54] Genetic Information Guidelines, sections II(1-4)(xxv) and II(2)(iii).

[55] General Guidelines, section 2-16.

[56] PPC Q&A, Question 1-61, page 16.

[57] PPC Q&A, Question 1-61, page 16.

[58] PPC Q&A, Question 1-60, page 15.

That said, certain sector-specific guidelines identify a number of circumstances in which consent can be inferred or deemed.

For example, the Medical Sector Guidelines provide that consent for use of personal information by a medical institution may be inferred where:[59]

- the information is normally considered necessary for the medical institution to provide medical services to patients, including:
  - collaborating with other medical institutions, etc., in order to provide medical care to patients;
  - seeking opinions and advice from outside physicians and others for the provision of medical care to patients;
  - responding to inquiries from other medical institutions for the provision of medical care to patients; and
  - explaining medical conditions to family members and others when providing medical care to patients.[60]
- the use is clarified by a notice in the medical institution's facility (e.g., a hospital bulletin board); and
- there is no clear objection or reservation on the part of the patient.

A similar rule also covers disclosure of the personal information of a patient to a third party where necessary for the provision of medical care to the patient, including recovery from the patient's injury or illness.[61]

The Medical Sector Guidelines further provide that consent for use of personal information (including information requiring special care) may be inferred where a patient provides information on his/her own physical or medical condition in response to a medical questionnaire at the reception desk of a medical institution and requests a medical examination together with his/her insurance card.[62]

Additionally, the Debt Collection Sector Guidelines provide that consent for disclosure of personal information to a third party may be presumed:

- in the context of assignment of a legal claim, where the personal information relates to a debtor or guarantor and is necessary for management of the claim; and
- where necessary for "preparatory acts", such as due diligence and selection of assignees.[63]

Finally, the Health Insurance Association Guidelines and the National Health Insurance Association Guidelines permit consent to be inferred where:

- use of information is normally necessary for the provision of insurance benefits to the insured and is beneficial to the insured; or
- obtaining express consent would require disproportionate effort on the part of the insurer; and

and where the principal does not expressly object after being notified via posting on a website, distributed pamphlets, posting on a bulletin board, or public notice, etc.[64]

Further, these Guidelines provide that consent for handling of personal information requiring special care can be inferred where an individual voluntarily provides this information to an insurer.[65]

---

[59] Medical Sector Guidelines, section II(9).
[60] Medical Sector Guidelines, section IV(9)(iii)1. See also the Medical Sector Guidelines, page 48 for examples of how the rules apply to these purposes in practice.
[61] Medical Sector Guidelines, section IV(9)(iii)3.
[62] Medical Sector Guidelines, section IV(6).
[63] Debt Collection Sector Guidelines, section 8(2).
[64] Health Insurance Association Guidelines, sections II(8) and III(7)(iii); National Health Insurance Association Guidelines, sections II(8) and III(7)(iii).
[65] Health Insurance Association Guidelines, section II(8); National Health Insurance Association Guidelines, section II(8).

c. Formalities in sector-specific guidelines

PIHBOs in the financial sector must record consent in writing or an electromagnetic record[66] in a manner that reflects an individual's intention to give consent[67] (e.g., a tick box).[68]

Such PIHBOs must state the utilization purpose in the contract in a manner that is clearly separate from other contractual provisions.[69] Contractual clauses pertaining to the handling of personal information must also either be kept in a separate document from other contractual clauses or if they are kept in the same document, the clauses pertaining to the handling of personal information must be clearly distinguished from other contractual clauses.[70] The PIHBOs must also take measures (e.g., by using specific fonts or formatting) to facilitate consumers' understanding of terms relating to the handling of their personal information.[71]

Additionally, the Genetic Information Guidelines require that consent for use of genetic information must also be obtained in writing.[72]

5.2. Withdrawal of consent

The APPI is silent on withdrawal of consent.

However, in practice, it is understood that where handling of personal information is based on consent, PIHBOs may handle personal information for a given utilization purpose for as long as principals' consent to the handling of their personal information for that purpose continues to exist (and even if a principal has withdrawn consent in respect of other utilization purposes).

This understanding is stated explicitly in the Medical Sector Guidelines, which provide that where a principal revokes his/her consent in respect of certain utilization purposes, his/her personal information may no longer be handled for those purposes but may be handled for other purposes for which consent was previously given and has not been revoked.[73]

5.3. Bundled consent

The APPI does not contain express provisions on bundled consent or whether access to services may be conditional on consent. However, such practices may be inconsistent with the APPI's prohibitions on acquiring personal information by deceit or other improper means.[74]

Several guidelines in the financial sector prohibit PIHBOs who provide credit from denying credit to persons who refuse to consent to use of their personal information for promotional purposes.[75]

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The APPI recognizes a class of sensitive data – "**personal information requiring special care**" – which is defined as personal information about a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions prescribed by cabinet order

---

66 Financial Sector Guidelines, Articles 3 (use) and 12 (disclosure); Credit Sector Guidelines, section II(1)(iii).
67 Credit Sector Guidelines, section II(1)(iii).
68 Financial Sector Guidelines, Articles 3 and 6.
69 Financial Sector Guidelines, Articles 2(3) and 3.
70 Financial Sector Guidelines, Article 3; Credit Sector Guidelines, section II(1)(iii); Debt Collection Sector Guidelines, section 2-5.
71 Financial Sector Guidelines, Article 3; Credit Sector Guidelines, section II(1)(iii).
72 Genetic Information Guidelines, sections II(1-4)(xxv).
73 Medical Sector Guidelines, section IV(3) (page 27).
74 APPI, Article 20(1).
75 Financial Sector Guidelines, Article 2(3); Credit Sector Guidelines, section II(2)(2).

which must be handled with special care so as not to cause unfair discrimination, prejudice, or other disadvantages to the principal.[76]

As is clear from the wording of the provision, this is not a closed list as further categories of data can be added by the Cabinet Order to the extent that their processing creates a risk of "unfair discrimination, prejudice or other disadvantages to the principal." To date, the Cabinet Order has added the following categories of "personal information requiring special care":

- the fact of having physical, intellectual, and mental disabilities;[77]
- the results of a medical check-up or other examination for the prevention and early detection of a disease[78] and any treatment or care prescribed;[79]
- the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant;[80] and
- juvenile protection case history.[81]

The General Guidelines clarify that the scope of personal information requiring special care is narrowly interpreted and does not include information from which personal information requiring special care can be inferred.[82]

For example, information that a person has purchased or borrowed a book on religion would not qualify as personal information requiring special care, but information that a person holds religious beliefs would so qualify. Further, information about a person's skin color would not qualify as personal information requiring special care, but information that a person belongs to a particular ethnic group would so qualify.

Specific safeguards apply to handling of this class of personal information.

Specifically, PIHBOs must obtain the principal's prior consent for processing of such information, subject to limited exceptions.[83]

Further, this category of personal information is excluded from the possibility of third-party disclosure based on the procedure provided under Article 27(2) of the APPI (allowing transmission of data to third parties without the prior consent of the individual concerned).

6.1. Children

The APPI does not make specific provisions for consent in relation to children's personal information. Note, however, that the APPI takes children's interests into account by expressly providing an exception to consent requirements where there is a "special need" to promote fostering of healthy children.[84]

The General Guidelines provide that where a minor lacks capacity to judge the consequences of handling of his/her personal information, a PIHBO must obtain consent from a person with parental responsibility for the minor or from the minor's legal representative.[85]

The PPC Q&A further clarifies that it would generally be necessary to obtain the consent from a legal representative for handling of the personal information of children under the age of 15; however, the PPC Q&A also advocates for a flexible approach: the specific age at which a PIHBO would be required

---

[76] APPI, Article 2(3). Note that reference to "**race**" covers "ethnic ties or ties to a certain part of the world," while "**creed**" is understood to encompass both religious and political views (General Guidelines, section 2-3)
[77] Cabinet Order, Article 2(1).
[78] Cabinet Order, Article 2(2).
[79] Cabinet Order, Article 2(3).
[80] Cabinet Order, Article 2(4).
[81] Cabinet Order, Article 2(5).
[82] General Guidelines, section 2-3.
[83] APPI, Article 20(2).
[84] APPI, Articles 18(3)(iii) (use beyond scope of specified utilization purpose), 20(2)(iii) (acquisition of personal information requiring special care), and 27(1)(iii) (disclosure to a third party).
[85] General Guidelines, section 2-16.

to obtain consent from a child's legal representative should be determined on a case-by-case basis, taking into account the specific items of personal information involved and the nature of the business.[86]

6.2. Cookies and online tracking

The 2020 amendments to the APPI introduced the concept of "**personally referrable information**" (i.e., information which relates to a living individual but does not fall under the definitions of personal information, pseudonymously processed personal information, or anonymously processed personal information[87]). This concept includes cookies or purchase history.[88]

Where a business operator handles "personally referable information" which is capable of identifying a person, the business operator must obtain consent from that person before disclosing the information to a third party.[89]

6.3. Direct marketing

The APPI is silent on direct marketing, However, as discussed above, guidelines in the financial sector provide that provision of credit may not be made conditional on consent to handling of personal information for promotional purposes.[90]

6.4. Biometric data

The APPI does not make express provisions for biometric data. It is possible that such information could qualify as personal information requiring special care under certain circumstances, where it reveals any of the prescribed categories for this class of information (such as race or ethnic origin).

In any case, note the Cabinet Order provides that the following forms of digitized biometric information would qualify as personal information (insofar as they relate to a specific living individual):[91]

- DNA taken from a cell;[92]
- appearance decided by facial bone structure and skin color as well as the position and shape of eyes, nose, mouth, or other facial elements;[93]
- iris prints;[94]
- voice prints and shape and motion of the vocal organs;[95]
- posture and gait;[96]
- the shape of veins in the hands and fingers;[97] and
- finger or palm prints.[98]

---

86 PPC Q&A, Question 1-62, page 16.
87 APPI, Article 2(vii).
88 Takeshige Sugimoto, Akihiro Kawashima, Tobyn Aaron, "A New Era for Japanese Data Protection: 2020 Amendments to the APPI" *Future of Privacy Forum Blog* (April 13, 2021), available at https://fpf.org/blog/a-new-era-for-japanese-data-protection-2020-amendments-to-the-appi/.
89 APPI, Article 31(1).
90 Financial Sector Guidelines, Article 2(3); Credit Sector Guidelines, section II(2)(i)2.
91 APPI, Article 2(1)(ii) read with Cabinet Order, Article 1.
92 Cabinet Order, Article 1(i)(a).
93 Cabinet Order, Article 1(i)(b).
94 Cabinet Order, Article 1(i)(c).
95 Cabinet Order, Article 1(i)(d).
96 Cabinet Order, Article 1(i)(e).
97 Cabinet Order, Article 1(i)(f).
98 Cabinet Order, Article 1(i)(g).

6.5. Genetic data

The Genetic Information Guidelines require informed consent for handling of personal genetic information.[99] Such consent must be in writing and accompanied by a written explanation of certain prescribed matters.[100]

The Medical Sector Guidelines also require that special attention should be paid to information obtained through genetic testing of persons due to the risk of harm that such information poses to those persons and their relatives.[101] In particular, even where a person consents to such testing, medical institutions should provide information and support to the person and his/her family members so that they can understand the meaning and impact of test results.[102]

6.6. Financial information

Financial information does not qualify as personal information requiring special care under the APPI.

6.7. Pseudonymized data

Following the 2020 amendments, the APPI now recognizes the concepts of "**pseudonymously processed personal information**"[103] and "**pseudonymously processed information handling business operators**" ("**PPIHBOs**").[104]

The APPI defines "**pseudonymously processed information**" as information relating to an individual that can be produced from processing personal information so as not to be able to identify a specific individual unless collated with other information by partially or wholly deleting information or replacing information with other descriptions using a method with no regularity so that the original descriptions cannot be restored.[105]

PPIHBOs, on acquiring pseudonymously processed personal information, must disclose the utilization purpose to the public.[106] PPIHBOs are also prohibited from handling pseudonymously processed personal information beyond the scope necessary to achieve the specified utilization purpose or disclosing pseudonymously processed personal information to third parties "except in cases based on laws and regulations"[107] and from collating pseudonymously processed personal information with other information in order to identify a principal.[108]

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

The APPI prohibits the transfer of personal information to a third party located outside of Japan unless:

---

[99] Genetic Information Guidelines, section II(1-4)(xxv). Note that "**informed consent**" is defined as consent given by a principal freely after receiving a sufficient explanation from the PIHBO as to how it will handle personal genetic information and having understood the significance, purpose, methods, expected results, disadvantages, and accuracy of the handling (Genetic Information Guidelines, section II(1-3)(xix)). Further, "**personal genetic information**" is defined as information that indicates an individual's genetic characteristics or constitution based on such characteristics, and that can be used to identify an individual (Genetic Information Guidelines, section II(1-1)(v)).

[100] Genetic Information Guidelines, sections II(1-4)(xxv) and II(2)(iii). See "Informed consent" above.

[101] Medical Sector Guidelines, section I(10).

[102] Medical Sector Guidelines, section I(10).

[103] APPI, Article 2(5).

[104] APPI, Article 16(5)). The definition is similar to that of a PIHBO but refers to "pseudonymously processed information" rather than "personal information."

[105] APPI, Article 2(5).

[106] APPI, Article 41(4).

[107] APPI, Article 41(3).

[108] APPI, Article 41(7).

- the principal gives prior consent to the transfer[109] after having been provided with certain information, including on the personal information protection system of the foreign country and the action that the third party will take to protect personal information;[110]
- the destination country has been whitelisted by the PPC; or
- the recipient third party upholds data protection standards equivalent to the APPI (in practice, these would generally be imposed contractually).

Note that the PPC has also issued guidelines on provision of personal information to third parties located in foreign countries ("**Cross-Border Transfer Guidelines**"), which were released in 2016 and revised in January 2021.[111] Broadly, the Cross-Border Transfer Guidelines require PIHBOs, when seeking principals' consent to cross-border transfer of their personal information, to inform principals that their personal information will be disclosed to a third party located overseas.[112]

In practice, PIHBOs primarily rely upon contractual safeguards and consent (in that order) to transfer personal information outside of Japan. The PPC's list of "adequacy decisions" is significantly shorter than that of the European Commission: to date, only the United Kingdom and several European jurisdictions have been deemed adequate.

8. TRANSPARENCY AND NOTICE

By default, the APPI requires PIHBOs who acquire personal information to inform principals or the public of the utilization purpose for that information, unless the utilization purpose has already been disclosed to the public.[113] PIHBOs must also update principals if the utilization purpose changes.[114]

However, a PIHBO does not need to inform the principal of the utilization purpose or disclose the utilization purpose to the public where:

- there is a possibility that doing so would
  - harm:
    - the life, body, fortune, or other rights and interests of the principal or a third party;[115]
    - the rights or legitimate interests of the PIHBO;[116] or
  - interfere with the performance of the affairs of central or local governments as prescribed by laws or regulations, and it is necessary for the PIHBO to cooperate;[117] or
- the utilization purpose is clear from the circumstances in which the personal information was acquired.[118]

According to the General Guidelines' interpretation, those exceptions apply in very specific situations, such as where information on the utilization purpose would risk undermining legitimate measures taken by the business operator to protect certain interests (e.g., to combat fraud, industrial espionage, or sabotage).[119]

Principals also have a right under the APPI to request that a PIHBO inform them, without delay, of the utilization purpose for any personal information about them that is retained by the PIHBO[120] unless the

[109] APPI, Article 28(1).
[110] APPI, Article 28(2).
[111] Available in Japanese at https://www.ppc.go.jp/files/pdf/211029_guidelines02.pdf.
[112] Cross-Border Transfer Guidelines, section 2-1.
[113] APPI, Article 21(1).
[114] APPI, Article 21(3).
[115] APPI, Article 21(4)(i).
[116] APPI, Article 21(4)(ii).
[117] APPI, Article 21(2)(iii).
[118] APPI, Article 21(2)(iv).
[119] General Guidelines, section 3-3-5.
[120] APPI, Article 32(2).

utilization purpose is clear[121] or an exemption applies.[122] Where a PIHBO decides not to inform a principal of the utilization purpose in response to such a request, the PIHBO must still inform the principal of this decision.[123]

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

The APPI lacks an independent legal basis premised on an assessment of the impact of processing on principals, such as the "legitimate interests" basis for processing under the GDPR.

However, the APPI holds PIHBOs accountable in a more general sense by requiring that processing should be fair and lawful, as is implicit in the APPI's prohibitions on collecting personal information by deceit or other improper means[124] and on use of personal information via any method that "has the possibility of fomenting or prompting an unlawful or unfair act."[125]

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

10.1. Using and disclosing personal information without consent under the APPI

As discussed above, the APPI does not require consent where personal information is used for a specified utilization purpose, which must be communicated to the principal at the time of collection, or for a purpose reasonably related to the utilization purpose.

However, consent is generally required to:

- use the personal information for a purpose that is beyond what the principal could reasonably expect based on the specified utilization purpose or that exceeds the scope necessary to achieve the specified utilization purpose ("**secondary purpose**");[126] or
- disclose personal information to a third party.[127]

These consent requirements are subject to exceptions. A PIHBO is not required to obtain consent to use personal information for a secondary purpose, or disclose personal information to a third party, where such change, use, or disclosure is permissible by law[128] or where there is:

- a need to protect human life, body, or fortune, and when it difficult to obtain a principal's consent;[129]
- a special need to improve public health or promote fostering of healthy children, and when it is difficult to obtain a principal's consent;[130] or
- a special need to cooperate with a central government organization or a local government, or a person entrusted by it who is performing activities prescribed by laws and regulations, and when

[121] APPI, Article 32(2)(i).
[122] APPI, Article 32(2)(ii). The relevant exemptions are Articles 21(1)(i), 21(1)(ii), and 21(1)(iii) of the APPI.
[123] APPI, Article 32(3).
[124] APPI, Article 20(1).
[125] APPI, Article 19.
[126] APPI, Article 18(1).
[127] APPI, Article 28(1).
[128] APPI, Article 18(2)(i) (use); APPI, Article 27(1)(i) (disclosure).
[129] APPI, Article 18(2)(ii) (use); APPI, Article 27(1)(ii) (disclosure).
[130] APPI, Article 18(2)(iii) (use); APPI, Article 27(1)(iii) (disclosure).

there is a possibility that obtaining the principal's consent would interfere with the performance of the said activities.[131]

a. Where permissible by law

Under the APPI, a PIHBO may use a principal's personal information for a secondary purpose[132] or disclose personal information to a third party[133] without the principal's consent where such use or disclosure is permissible by law.

The General Guidelines clarify that such use[134] or disclosure[135] would be permitted where:

- the PIHBO must respond to matters related to a police investigation under Article 197(2) of the Criminal Procedure Code or to an investigation based on a warrant issued by a judge under Article 218 of the Criminal Procedure Code;
- the PIHBO must respond to an investigation by the tax office regarding income tax, etc. under Article 74-2 of the National Tax General Rules Act;
- an order for prevention of harm has been made under Article 39(1) the Consumer Product Safety Act in respect of a product, and pursuant to Article 38(3) of the said Act, a seller must provide the manufacturer or importer of the product with information on purchasers of the product to facilitate product recall;
- the PIHBO must respond to inquiries from the bar association under Article 23-2 of the Attorney Act;
- the PIHBO must respond to an active epidemiological survey conducted by a public health center under Article 15(1) of the Act on Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases; or
- following a power outage due to a natural disaster, a General Transmission and Distribution Utility is required, under Article 34(1) of the Electricity Business Act, to provide necessary information to the relevant administrative agency or the head of a local government upon request by the METI in order to expedite the restoration of power.

The Medical Sector Guidelines provide that, in addition to the above, a medical institution or healthcare professional may use personal information for a secondary purpose[136] or disclose personal information to a third party[137] without the principal's consent where required for:

- on-site inspections pursuant to the Medical Care Act;
- notification to municipalities regarding unauthorized recipients pursuant to the Long-Term Care Insurance Act; and
- notification regarding child abuse pursuant to the Law Concerning the Prevention of Child Abuse.

Note that Appendix 3 to the Medical Sector Guidelines further lists the obligations with which medical institutions must comply under Japanese laws and regulations.

The Medical Sector Guidelines further clarify that where a medical institution uses personal information without consent based on this exception, the scope of use should be limited to what is necessary, taking into account the purpose behind the relevant laws or regulations.[138]

The Health Insurance Association Guidelines and the National Health Insurance Association Guidelines provide that health insurance associations may use personal information for a secondary purpose[139] or

---

[131] APPI, Article 18(2)(iv) (use); APPI, Article 27(1)(iv) (disclosure).
[132] APPI, Article 18(2)(i).
[133] APPI, Article 27(1)(i).
[134] General Guidelines, section 3-1-5.
[135] General Guidelines, section 3-6-1 read with section 3-1-5.
[136] Medical Sector Guidelines, section IV(3)(ii)1.
[137] Medical Sector Guidelines, section IV(9)(ii) 1.
[138] Medical Sector Guidelines, section IV(3).
[139] Health Insurance Association Guidelines, section III(1)(ii)1; National Health Insurance Association Guidelines, section III(1)(ii)1.

disclose personal information to a third party[140] without a principal's consent where required for, among others, collection of reports pursuant to Article 106 of the National Health Insurance Law or for on-site inspections pursuant to Article 29 or Article 198 of the Health Insurance Law.

b. Protection of life, body, or fortune

Under the APPI, a PIHBO may use a principal's personal information for a secondary purpose[141] or disclose personal information to a third party[142] without the principal's consent where there is a need to protect human life, body, or fortune, and when it is difficult to obtain the principal's consent.

The General Guidelines provide that use[143] or disclosure[144] of personal information would be covered by this exception in any of the following situations:

- A person suffers a sudden illness, or other similar situation occurs, and the person provides information on his/her blood type and family contact information to medical professionals.
- An emergency, such as a large-scale disaster or accident, occurs, and it is necessary to provide the personal information of victims or those injured to family members, government agencies, etc..
- It is necessary to share information on bank accounts to prevent fraud and organized crime and to identify persons who interfere with business operations.
- A manufacturer recalls a product because an accident has occurred in relation to the product, because there is an imminent danger of harm to human life, body, or property or because the seller, repair business, or installation business, has asked the manufacturer to recall the product, and information on purchasers of the product is required.

The Medical Sector Guidelines clarify that use of personal information for a secondary purpose[145] or disclosure of personal information to a third party[146] without a principal's consent would be covered by this exception in the following situations:

- When making inquiries to relevant organizations about patients who are unconscious and unidentified, or when providing necessary information in response to safety confirmations from family members or related persons, etc..
- Explaining to family members and others the medical condition of an unconscious patient or the situation of an elderly person with severe dementia.

Where, due to a large-scale disaster or similar event, a very large number of injured or sick persons are transported to a medical institution at one time, and it would be extremely unreasonable to seek their consent to respond promptly to inquiries from their family members, etc., the Health Insurance Association Guidelines and the National Health Insurance Association Guidelines provide that use of personal information for a secondary purpose[147] or disclosure of personal information to a third party[148] without a principal's consent would be covered by this exception where necessary to provide relevant information on insured persons who have become unconscious, such as contact information on family members, to medical institutions.

---

[140] Health Insurance Association Guidelines, section III(7)(ii) 1; National Health Insurance Association Guidelines, section III(7)(ii) 1.
[141] APPI, Article 18(3)(ii).
[142] APPI, Article 27(1)(ii).
[143] General Guidelines, section 3-1-5.
[144] General Guidelines, section 3-6-1.
[145] Medical Sector Guidelines, section IV(3)(ii)2.
[146] Medical Sector Guidelines, section IV(9)(ii)2.
[147] Health Insurance Association Guidelines, section III(7)(ii)2; National Health Insurance Association Guidelines, section III(7)(ii)2.
[148] Health Insurance Association Guidelines, section III(1)(ii)2; National Health Insurance Association Guidelines, section III(1)(ii)2.

The Medical Sector Guidelines,[149] the Health Insurance Association Guidelines,[150] and the National Health Insurance Association Guidelines[151] further clarify that situations where it is "difficult to obtain the consent of the individual" include those where the individual does not give consent even after being asked to do so, or where the individual's consent cannot be obtained without going through the procedures for requesting consent.

c. Public health

Under the APPI, a PIHBO may use a principal's personal information for a secondary purpose[152] or disclose personal information to a third party[153] without the principal's consent where there is a special need to improve public health or promote fostering of healthy children, and it is difficult to obtain the principal's consent.

The General Guidelines provide that use[154] or disclosure[155] of personal information would be covered by this exception in any of the following situations:

- where health insurance societies and other insurers conduct health examinations, such information may be used for planning health promotion measures, and improving the effectiveness of health services, epidemiological studies, etc.;
- where the Child Guidance Center, schools, medical institutions, and other related organizations exchange information to cooperate on a response to a student's truancy or delinquent behavior; or
- when it is necessary for the Child Guidance Center, police, schools, hospitals, etc. to exchange information on families where there is a possibility of child abuse.

The Medical Sector Guidelines clarify that use of personal information for a secondary purpose[156] or disclosure of personal information to a third party[157] without a principal's consent would be covered by this exception under the following circumstances:

- providing information to the national or local government through the Regional Cancer Registry Project based on the Health Promotion Law;
- providing information on results of precision heath tests to local governments or screening organizations commissioned by local governments to enable precision control of cancer screening;
- sharing information on child abuse cases with relevant organizations to prevent further abuse;
- providing information to the national government, local governments, or third-party organizations concerning medical accidents, etc., that have occurred at medical institutions to improve safety;
- sharing information to ascertain family members and other persons in close contact with an infected patient to prevent further infection of other patients; or
- sharing personal information, which medical institutions obtain through treatment of patients in clinical practice, with other medical institutions seeking to improve medical services and enhance public health, or with pharmaceutical companies for the purpose of examining the mechanism of disease that lacks effective treatment or medicine.

The Health Insurance Association Guidelines and the National Health Insurance Association Guidelines provide that use of personal information for a secondary purpose [158] or disclosure of personal

---

149 Medical Sector Guidelines, section IV(9)(ii)2.
150 Health Insurance Association Guidelines, section III(7)(ii)2.
151 National Health Insurance Association Guidelines, section III(7)(ii)2.
152 APPI, Article 18(3)(iii).
153 APPI, Article 27(1)(iii).
154 General Guidelines, section 3-1-5.
155 General Guidelines, section 3-6-1.
156 Medical Sector Guidelines, section IV(3)(ii)3.
157 Medical Sector Guidelines, section IV(9)(ii)3.
158 Health Insurance Association Guidelines, section III(1)(ii)3; National Health Insurance Association Guidelines, section III(1)(ii)3.

information to a third party[159] without a principal's consent would be covered by this exception in the following situations:

- providing information obtained from health examinations or cancer screenings to researchers for epidemiological surveys or research without revealing the principal's name; and
- providing information to the national government, local governments, or third-party organizations concerning medical accidents, etc. that occur at medical institutions that report to a relevant government health insurance association for the purpose of improving medical safety.

d. Cooperation with public bodies

Under the APPI, a PIHBO may use a principal's personal information for a secondary purpose[160] or disclose personal information to a third party[161] without the principal's consent where there is a special need to cooperate with a central government organization or a local government, or a person entrusted by it who is performing activities prescribed by laws and regulations and when there is a possibility that obtaining the principal's consent would interfere with the performance of the said activities.

The General Guidelines provide that use[162] or disclosure[163] of personal information would be covered by this exception where:

- a business submits personal information in response to a request by an official from the tax or customs office;
- a business submits personal information in response to a request by the police; and
- it is necessary to respond to surveys or statistical surveys conducted by local governments.

The Medical Sector Guidelines, the Health Insurance Association Guidelines, and the National Health Insurance Association Guidelines clarify that use of personal information for a secondary purpose[164] or disclosure of personal information to a third party[165] without a principal's consent would be covered by this exception in the following situations:

- In the event of a disaster, when the police inquire about the name, address, and extent of injuries of an injured person, etc., from the perspective of maintaining public safety and order; and
- When cooperating in general statistical surveys pursuant to Article 2(7) of the Statistics Act.

10.2. Using and disclosing sensitive personal information without consent under the APPI

By default, consent is required before a PIHBO may acquire personal information requiring special care. However, this general rule is subject to exceptions in Article 17 of the APPI – principals' consent for acquisition of personal information requiring special care is not required where acquisition is permitted by laws and regulations,[166] or where:

- there is a need to protect human life, body, or fortune, and when it is difficult to obtain a principal's consent;[167]

---

[159] Health Insurance Association Guidelines, section III(5)(2)(3); National Health Insurance Association Guidelines, section III(7)(ii)3.
[160] APPI, Article 18(3)(iv).
[161] APPI, Article 27(1)(iv).
[162] General Guidelines, section 3-1-5.
[163] General Guidelines, section 3-6-1.
[164] Medical Sector Guidelines, section III(3)(ii)4, Health Insurance Association Guidelines, section III(1)(ii)4; National Health Insurance Association Guidelines, section III(1)(ii)4.
[165] Medical Sector Guidelines, section IV(9)(ii)4.
[166] APPI, Article 20(2)(i).
[167] APPI, Article 20(2)(ii).

- there is a special need to enhance public hygiene or promote fostering of healthy children, and when it is difficult to obtain a principal's consent;[168]
- there is a special need to cooperate with a central government organization or a local government, or a person entrusted by it who is performing activities prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said activities;[169]
- such information is made public by a principal, a government organization, a local government, or a person set forth in PPC guidance;[170] and
- such information is acquired by visual observation, filming or photographing the principal.[171]

Many of the above exceptions are similar to exceptions to consent requirements in Article 16 of the APPI (use of personal information for secondary purpose) and Article 23 of the APPI (disclosure of personal information to third parties). Where this is the case, the General Guidelines provide that guidance in relation to the exceptions in Articles 16 and 23 of the APPI also applies to equivalent exceptions in Article 17 of the APPI.[172]

a. Healthcare sector

The Medical Sector Guidelines clarify that the APPI would not require consent for acquisition of personal information requiring special care where:[173]

- a doctor, nurse, or other medical professional interviews a family member about the person's medical history when a sudden illness or other situation arises;
- a medical institution obtains personal information of patients that another medical institution previously treated for the purpose of clinical research and public health;
- a medical institution exchanges information on a child protection case with a Child Guidance Center, school, or other relevant organization in order to cooperate in responding to a case of truancy or delinquent behavior of a child, etc.;
- a Child Guidance Center, police, school, hospital, etc. obtains information on possible child abuse from another relevant organization;
- a medical institution or a care-related business operator obtains personal information requiring special care in response to a request by the police; or
- a physically disabled person visits a medical institution, etc. and his/her information is recorded for the purpose of information sharing within the hospital (acquisition by visual inspection), or when a physically disabled person is caught on a security camera installed in a store (acquisition by filming).

The Health Insurance Association Guidelines[174] and the National Health Insurance Association Guidelines[175] further clarify that the APPI would not require consent for acquisition, use, or disclosure of personal information requiring special care where:

- a business obtains personal information on its employees' health checks, etc.;
- a person suffers a sudden illness, or another similar situation occurs, and a doctor or nurse belonging to the National Health Insurance Society interviews the person's family member about his/her medical history;
- a business acquires personal information requiring special care in response to a voluntary request by the police; and

---

168 APPI, Article 20(2)(iii).
169 APPI, Article 20(2)(iv).
170 APPI, Article 20(2)(vii).
171 APPI, Article 20(2)(viii) read with Cabinet Order Article 9.
172 General Guidelines, section 3-3-2.
173 Medical Sector Guidelines, section IV(6) (pages 33).
174 Health Insurance Association Guidelines, section III(4).
175 National Health Insurance Association Guidelines, section III(4).

- a PIHBO acquires personal information requiring special care through entrustment, business succession, or joint use pursuant to Article 23(5) of the APPI.

b. Credit sector

The Credit Sector Guidelines[176] clarify that the APPI would not require consent for acquisition, use, or disclosure of personal information requiring special care for:

- obtaining, using, or storing a copy of a family register or other documents that can identify the person to whom sensitive information pertains, for the purpose of identifying the person;
- obtaining, using, or storing information on the legal domicile of a bankrupt in order to verify the identity of the bankrupt with respect to information on the bankrupt published in the Official Gazette, etc.; and
- acquiring, using, or disclosing to the extent necessary for the execution of the transfer of rights and obligations through inheritance procedures, etc.

10.3. Exemptions to the APPI

The APPI does not apply to the handling of personal information in the following circumstances:

- handling of personal information by a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his/her business) for the purpose of use in the press;[177]
- handling of personal information by a person who practices writing as a profession for the purpose of use in writing;[178]
- handling of personal information by a religious body for the purpose of use in a religious activity or an activity accessory thereto;[179] and
- handling of personal information by a political body for the purpose of use in a political activity or an activity accessory thereto.[180]

Collection, use, and disclosure of personal information by the above organizations for the above purposes would not be subject to the APPI's requirements, including requirements to obtain consent in certain circumstances.

However, the APPI still requires such organizations to strive to take necessary and appropriate action to secure, and ensure proper handling of, any personal information that they handle.[181]

10.4. Research purposes (including medical research)

Prior to the 2021 amendments, the APPI used to provide a comprehensive exemption for universities or other organizations or groups which are involved in academic studies in respect of handling of personal information for the purpose of academic study. However, following these amendments, this exemption has been abolished and substituted by a number of more limited exceptions.

Note that under Japanese law, clinical trials may be subject to the Act on Quality, Efficacy and Safety Assurance of Pharmaceuticals, Medical Devices and Other Products[182] and related laws and regulations, such as the Ministerial Ordinance Concerning Standards for Conducting Clinical Trials on Drugs,[183] as well as ethical and other guidelines established by relevant organizations, such as the

---

[176] Credit Sector Guidelines, section II(2)(ii).

[177] APPI, Article 57(1)(i). Note that "**press**" is defined as informing a large number of unspecified people of an objective fact as such (including stating an opinion or view based thereon) (APPI, Article 57(2)).

[178] APPI, Article 57(1)(ii).

[179] APPI, Article 57(1)(iii).

[180] APPI, Article 57(1).

[181] APPI, Article 57(3).

[182] Act on Quality, Efficacy and Safety Assurance of Pharmaceuticals, Medical Devices and Other Products Act No. 1 of 1960, as amended). No. 45.

[183] Ordinance of the Ministry of Health and Welfare No. 28 of 1997.

Ethical Guidelines for Life and Medical Science Research on Human Beings issued by the Ministry of Education, Culture, Sports, Science and Technology, together with the MHLW and METI.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG