SHIN&KIM
법무법인(유) 세종

Legal Insights from the 2024 Casebook for the Personal Information Protection Act by the Personal Information Protection Commission - Focusing on key cases related to healthcare and medicine

2024.10.15

1. Publication of the 2024 PIPA Casebook on the Interpretation of the Personal Information Protection Act (the "PIPA") by the Personal Information Protection Commission

On June 30, 2024, the Personal Information Protection Commission (the "**PIPC**") released a casebook that details exemplary cases interpreting provisions of the PIPA (the "**2024 PIPA Casebook**"). The 2024 PIPA Casebook, available on the PIPC's official website, features 52 selected cases, chosen for their relevance and timeliness. These cases have been updated to reflect the amendments made to the PIPA in September 2023.

** To view the original text (Korean) of the 2024 PIPA Casebook, please click [here].*

2. Highlighted cases in the healthcare and medicine sector

Among the 52 cases published by the PIPC, the most notable cases from the healthcare and medicine sector are highlighted and summarized below.

[Definition of Personal Information] – 2024 PIPA Casebook, p. 5

Q. Does an individual's dental X-ray photograph constitute personal information?
A. (i) While dental x-ray photographs alone may not constitute personal information, (ii) they may be considered personal information if they can be easily combined with other information to identify specific individuals.

Explanation: (i) Dental X-ray photographs, if they do not allow for the identification of an individual on their own, are not likely to be considered personal information protected by the PIPA; (ii) however, if there is **supplementary data, such as medical records**, which can be easily combined with the dental X-rays to identify an individual, then the dental X-ray photographs would be classified as personal information.
※ "Personal information" refers to any information relating to a living individual that can identify a particular individual through details such as full names, resident registration numbers, or images, among others. This also includes information that can be easily combined with other data to identify specific individuals, even if such information on its own does not identify them (see Subparagraph 1 of Article 2 of the PIPA).

** To view the original text (Korean), please click **[here]**.*

S&K Comments: In the healthcare and medicine sector, images or photographs, such as MRIs, CT scans, and X-rays, often do not exist as standalone information but are typically accompanied by patient details, such as name, age, and gender and can be readily combined with additional data, such as medical records. As a result, under the current PIPA, these images or photographs may frequently be considered personal information, requiring special caution.

[Definition of Personal Information] – 2024 PIPA Casebook, p. 8

Q. Does information related to a deceased person constitute personal information?
A. (i) No, in principle, information about a deceased person does not constitute personal information. (ii) However, if information about a deceased person reveals a connection with the bereaved family, it is considered personal information, as it pertains to the living family members.

Explanation: (i) "Personal information" refers to information relating to living individuals, which "can identify a particular individual" or "which on its own cannot identify specific individuals but can be easily combined with other information to do so" (see Subparagraph 1 of Article 2 of the PIPA). Consequently, information about an individual who has passed away, or is legally recognized as deceased, generally do not constitute personal information. (ii) However, if information about a deceased person reveals a relationship with the bereaved family, it may be classified as the personal information of the surviving family members. Even if such information does not immediately identify specific individuals, it may still qualify as personal information if it can be easily combined with other data to allow such identification . Therefore, even if details about a deceased person d do not directly reveal a relationship with the bereaved family, they may may still constitute personal information of the bereaved family if it can be easily combined with other information to identify such relationship.

** To view the original text (Korean), please click **[here]**.*

S&K Comments: Regarding consent forms for processing personal information, it is important to note that even

information pertaining to deceased individuals is considered personal information of the bereaved family. Therefore, obtaining consent from the relevant family members for processing this information is necessary.

[Definition of Personal Information] – 2024 PIPA Casebook, p. 9

Q. Do facial photographs constitute sensitive information?
A. No, facial photographs are generally considered personal information, not sensitive information.

Explanation: Sensitive information includes details such as thoughts and beliefs, membership in and withdrawal from trade unions and political parties, political opinions, health sexual life and other information related to physical, physiological, and behavioral characteristics that may significantly infringe on the privacy of data subjects that are generated through certain technical means to identify specific individuals (see Article 23 of the PIPA; Subparagraph 3 of Article 18 of the Enforcement Decree of the PIPA). Accordingly, while facial photographs, such as those in passports or identification photos, generally constitute personal information, they are not considered sensitive information.

* However, if general facial photographs are **subsequently processed by certain technical means for the purposes such as authentication or identification**, such information may constitute sensitive information under Subparagraph 3 of Article 18 of the Enforcement Decree of the PIPA.

** To view the original text (Korean), please click **[here]**.*

S&K Comments: Recently, there has been a rise in cases where facial photographs are taken for promotional purposes during cosmetic procedures. Since such facial photographs are considered personal information, it is necessary to obtain consent for processing personal information prior to capturing and using. However, facial photographs, in principle, are not considered sensitive information, so obtaining consent to process them as (general) personal information is sufficient.

[Pseudonymized Information] – 2024 PIPA Casebook, p. 29

Q. If pseudonymized information is processed for scientific research or other purposes, can it be sold for a fee?
A. Yes, receiving payments for processing pseudonymized information for purposes such as scientific research is permissible.

Explanation: It is permissible to receive payments to cover costs incurred in providing pseudonymized information for purposes like statistics, scientific research, and archiving of records for public interest, provided the payments are calculated according to appropriate standards. However, the processing of pseudonymized information for sale for purposes beyond the prescribed scope is not allowed (see Article 28-2 of the PIPA).

** To view the original text (Korean), please click **[here]**.*

S&K Comments: As a general rule, processing personal information requires the consent of the data subject. However, for scientific research purposes, such as in **clinical trials**, "pseudonymized information" may be processed **without the consent of the data subject**, and may even be sold for a fee. In this context, it is important to note that the following:
(i) when providing pseudonymized information to a third party, it must not include any data that can be used to identify specific individuals.
(ii) the processing of pseudonymized information for sale must remain within the permitted purposes (i.e., statistics, scientific research, and archiving of records for public interest).

[Pseudonymized Information] – 2024 PIPA Casebook, p. 30

Q. Can pseudonymized information be provided to third parties by deleting only information that directly identify individuals, such as names and resident registration numbers?
A. No, when pseudonymizing data, it is not enough to remove only information that directly identifies individuals. The potential for personal identification must also be comprehensively assessed.

Explanation: When providing pseudonymized information to third parties, any data that could be used to identify specific individuals must be excluded (see Article 28-2 (2) of the PIPA). This means that information such as names, unique identification information, and other information that can directly identify individuals should, in principle, be removed. Additionally, to consider information as having been safely pseudonymized, the risk of re-identification should be mitigated by comprehensively taking into account (a) information, such as "gender," "age," or "residential area," which on its own may not identify individuals but could, when combined with other data, pose a high risk of identification , and (b) unique information , such as rare surnames or information about a member of the National Assembly representing a specific constituency, which has a higher likelihood of identifying individuals.

** To view the original text (Korean), please click **[here]**.*

S&K Comments: The determination of whether information has been pseudonymized, or qualifies as pseudonymized, can vary depending on specific and individual circumstances. As explained in the Q&A above, the sufficiency of pseudonymization should be assessed from a "comprehensive" perspective. It is important to note that simply removing specific data elements may not be sufficient to fully pseudonymize information.

This is particularly relevant in the healthcare and medical research sector, where the risk of identifying individuals can differ based on the characteristics of the condition being studied. For example, if disease A rarely occurs in teenagers, information about two teenage cases could be information that can identify specific individuals.

Additionally, unlike other sectors, the healthcare and medical research sector often deals with atypical data, making it more difficult to apply uniform pseudonymization standards. As a result, the level and method of pseudonymization must be carefully assessed on a case-by-case basis. It is also important to note that the 2024 Pseudonymized Information Processing Guidelines by the PIPC and the Healthcare Data Utilization Guidelines by the PIPC and the Ministry of Health and Welfare (the "**MOHW**") outline specific procedures that must be followed for pseudonymization.

For further details, you can refer to the original texts (Korean) of "2024 Pseudonymized Information Processing

Guidelines" by the PIPC and the "Healthcare Data Utilization Guidelines" by the PIPC and the MOHW through the following links: . [2024 Pseudonymized Information Processing Guidelines], [Healthcare Data Utilization Guidelines]

[Pseudonymized Information] – 2024 PIPA Casebook, p. 31

Q. If a data provider supplies pseudonymized information to a third party and the data subject suffers harm as a result of the use of such information by the third party, will the data provider also be penalized?
A. No, if the recipient of pseudonymized information is at fault for failing to take safeguards or has intentionally re-identified the data subject, only the recipient will be subject to penalties, not the data provider.

Explanation: An entity processing personal information may process pseudonymized information without the consent of the data subject for purposes of statistics, scientific research, and archiving of records for public interest. When pseudonymized information is provided to a third party for these purposes, any data that can be used to identify specific individuals should be excluded (see Article 28-2 of the PIPA). Additionally, a person who processes pseudonymized information is prohibited from processing such information for the purpose of identifying specific individuals (see Article 28-5 (1) of the PIPA). However, if a data that can identify individuals in unintentionally generated during the processing of pseudonymized information, this alone does not result in penalties. Nonetheless, if information that can identify specific individuals is generated during the processing of pseudonymized information, the processing of the relevant information should immediately cease, and the relevant information should be retrieved and destroyed without delay (see Article 28-5 (2) of the PIPA).

** To view the original text (Korean), please click **[here]**.*

S&K Comments: The processing of pseudonymized for scientific research purposes, such as clinical trials, is allowed without the consent of the data subject. As noted earlier, it is also permissible to receive payments for processing pseudonymized information for such research. Moreover, if a third party provided with pseudonymized information fails to comply with its safeguard obligations and causes harm to the data subject, the liability for the harm rests with that third party and not with the entity that provided the pseudonymized information.

[Note] Entities processing personal information are responsible for matters that occur during the pseudonymization process, which, in other words, takes place before the information is provided to a third party. Therefore, it is important to note that entities processing personal information should comply with all applicable obligations during the pseudonymization stage and until the information is provided to a third party, including taking safeguards and ensuring that pseudonymized information cannot be re-identified.

[Disclosure and Leakage of Personal Information] – 2024 PIPA Casebook, p. 35

Q. To what extent can the personal information of patients with infectious diseases be disclosed?
A. In the event of a crisis alert at the level of "caution" or higher, information such as the movement routes of

patients with infectious diseases must be disclosed promptly. However, information not related to the prevention of infectious diseases is excluded from disclosure.

Explanation: When a crisis alert of "caution" or higher is issued due to the spread of an infectious disease, information that the public needs to know to prevent the infectious disease, such as "the movement routes, transportation means, medical institutions visited, and contact persons of patients, as well as the current status of the outbreak and testing of the infectious diseases by region and age group," must be promptly disclosed (see Article 38 (2) of the Framework Act on the Management of Disasters and Safety; Article 34-2 (1) of the Infectious Disease Control and Prevention Act). However, information deemed unrelated to the prevention of infectious diseases, such as "genders, ages, names, and residential addresses at the *Eup/Myeon/Dong* or lower district levels," is excluded from disclosure (see Article 22-2(1) of the Enforcement Decree of the Infectious Disease Control and Prevention Act).

** To view the original text (Korean), please click **[here]**.*

S&K Comments: It is essential to carefully screen information by category and assess appropriateness of disclosure to ensure it remains within the legally permitted scope. Special attention must be paid to ensure withholding certain details, such as "genders, ages, names, and residential addresses at the *Eup/Myeon/Dong* or lower district levels."

[Disclosure and Leakage of Personal Information] – 2024 PIPA Casebook, p. 36

Q. If a list containing the names and residential registration numbers of health checkup subjects is accidentally sent to an incorrect institution, does it constitute a personal information leak?
A. Yes, it constitutes a personal information leak.

Explanation: A loss, theft, or leakage of personal information occurs when personal data escapes the control and management of the entity processing it in violation of relevant laws or without the entity's intent, allowing a third party to access the information (see Article 25 of the Standard Guidelines). Therefore, mistakenly sending a list containing names and residential registration numbers of health checkup subjects to an incorrect institution constitutes a personal information leak, as the information was disclosed to a third party outside the control and management of the entity processing personal information.

** To view the original text (Korean), please click **[here]**.*

S&K Comments: Under the PIPA, if a personal information leak occurs, an entity processing the information must notify the data subject without delay. Specifically, if an entity becomes aware of a personal information leak, it must report to the PIPC or the Korea Internet & Security Agency (the "**KISA**") within 72 hours, if such leak meets any of the following criteria: (i) the personal information of 1,000 or more data subjects has been leaked, (ii) sensitive information or unique identification information has been leaked, or (iii) the leak resulted from unlawful access to the personal information processing systems or information devices used by the entity.

Given that the healthcare and medical sector primarily deals with sensitive information, any leak will typically involve sensitive information or unique identification information (as described in criteria (ii) above), thereby triggering an obligation to report to the PIPC or KISA within 72 hours of becoming aware of such leak.

[Processing of Personal Information] – 2024 PIPA Casebook, p. 53

Q. Can consent for processing personal information, such as for sending promotional materials and providing points, be obtained through an Automatic Response System (ARS)?
A. Yes, an ARS can be used to receive consent for the processing of personal information (including collection, use, and provision.

Explanation: When an entity processing personal information obtains consent from the data subject for processing personal information, the entity must ensure that each consent item is distinguished, clearly communicated, and understood by the data subject. Subject to such requirement, consent can be obtained through various means, including writing, telephone, internet, or e-mail (see Article 22 (1) of the PIPA; Article 17 (2) of the Enforcement Decree of the PIPA). When consent is obtained by telephone, the burden of proof lies with the entity processing the personal information to demonstrate that such consent was obtained. Since simply answering the telephone call does not indicate an intent to consent, it is **necessary to confirm such intent, for example by recording the voice of the data subject.** Also, **the evidence and details of received consent should be retained until the relevant personal information is destroyed.**

** To view the original text (Korean), please click **[here]**.*

S&K Comments : In the healthcare and medical sector, there are often situations where certain prescription programs use ARS for patient enrollment, especially when providing information in writing is difficult or impractical for patients. Under the current PIPA, entities processing personal information are permitted to notify individuals (in a clear manner) of legally required matters and obtain their consent for personal information processing through ARS. However, the burden of proving that verbal consent was obtained rests with the entity processing personal information (i.e., the business operator). Therefore, for practical business purposes, we recommend (i) recording patient responses, such as "Yes, I agree," and (ii) keeping such recordings for the retention period specified in the consent form.

[Processing of Personal Information] – PIPC's 2024 PIPA Casebook, p. 54

Q. Is it necessary to enter into an agreement to delegate personal information processing when an institution conducts a SNS event through an event agency?
A. Yes, a written document according to Article 26 (1) of the PIPA is necessary to delegate matters to handle personal information in relation to an SNS event.

Explanation: When entities processing personal information operating an SNS delegate personal information processing tasks to an event agency, the delegation must be formalized through a written agreement. The

agreement should specify the purpose and scope of the delegated tasks, the obligation to safeguard personal information, other relevant matters. The details of the delegation and the agency must be disclosed, and additional requirements, such as training and supervision of the agency, must also be followed (see Article 26 of the PIPA).

** To view the original text (Korean), please click [here].*

S&K Comments : When entering into service agreements with service providers for tasks, such as operating adverse drug reaction counseling centers, operating call centers, or organizing academic seminars, it is important to also enter into written delegation agreements for the processing of personal information. These agreements must also include all necessary matters as required by the PIPA. Furthermore, once a delegation agreement is in place, the fact of delegation and relevant details should be disclosed in the Privacy Policy. The delegating party is also responsible for the oversight and management of the service provider.

* * *

The Healthcare Team at Shin & Kim LLC is composed of professionals with diverse backgrounds and extensive experience in the healthcare sector, including experts from the Ministry of Health and Welfare, the Ministry of Food and Drug Safety, the Health Insurance Review & Assessment Service, and leading pharmaceutical companies. Shin & Kim's Privacy and Data Security team offers specialized and tailored legal and policy services in the field of personal information and data. With deep expertise and extensive practical experience in various laws related to personal information, including the PIPA, the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Credit Information Use and Protection Act, and the Act on the Protection and Use of Location Information, the team is well-equipped to handle a wide range of issues in this area. Shin & Kim is committed to providing top-quality expert advice, leveraging its diverse industry experience to meet clients' needs. For any questions or additional information regarding the 2024 Casebook, please feel free to contact us at any time.

[Korean version] 개인정보보호위원회 발간 2024년도 개인정보 보호법 해석 사례집에 수록된 보건의료 분야 관련 주요 사례 소개

Key Contacts

Sung Tae Kim
Partner

+82-2-316-4326
stkim@shinkim.com

Jeong Ho Ahn
Partner

+82-2-316-2891
jhahn@shinkim.com

Joe Juneyoung Jang
Partner

+82-2-316-4985
jyojang@shinkim.com

Jee-Eun Roh
Partner

+82-2-316-2573
jeroh@shinkim.com

Ho Sang Yoon
Partner

+82-2-316-2584
hsyoon@shinkim.com