Review Article

Cardiovasc Prev Pharmacother 2024;6(1):8-16
eISSN 2671-700X
https://doi.org/10.36011/cpp.2024.6.e1

Cardiovascular Prevention and Pharmacotherapy

Using medical big data for clinical research and legal considerations for the protection of personal information: the double-edged sword

Raeun Kim[1], Jiwon Shinn[2], Hun-Sung Kim[2,3]

[1]*Department of Convergence Public Administration, Hansung University Mirae Plus College, Seoul, Korea*
[2]*Department of Medical Informatics, College of Medicine, The Catholic University of Korea, Seoul, Korea*
[3]*Division of Endocrinology and Metabolism, Department of Internal Medicine, Seoul St. Mary's Hospital, College of Medicine, The Catholic University of Korea, Seoul, Korea*

The advent of medical big data has increased the scope of the clinical use of such data; however, these data have raised serious concerns regarding personal privacy protection, which hinders their usage. For instance, as the pseudonymization or anonymization of data increases, the quality of its clinical use decreases. Thus, a balanced approach is required to maximize clinical data use while protecting personal information as much as possible. However, Korea's existing laws mandate several kinds of consent; soliciting some of these types of consent can be cumbersome. Moreover, while the collection of medical data by hospitals requires considerable time and money, its ownership is difficult to ascertain. To bridge the enormous gap between the protection of personal information and the use of clinical data, the European Union and countries such as Finland have already proposed various modes of guaranteeing the free movement of personal information that simultaneously strengthen people's personal rights. Similarly, Korea has initiated the MyData Service, although it faces several limitations. Therefore, this study reviews Korea's current healthcare big data system, the laws governing data sharing and usage, and compares them with similar laws enacted by the European Union and Finland. It then provides future direction for Korea's personal information protection legislation. Ultimately, governments must expand and elaborate upon the scope and content of personal information protection laws to enable the development of healthcare and other industries without sacrificing either personal information protection or clinical use of medical data.

Keywords: Big data; Delivery of health care; Privacy

INTRODUCTION

Medical services based on digital technologies, such as big data, real-world data, and artificial intelligence, are becoming increasingly popular [1,2]. In the field of digital-based medicine, the emergence of personalized medical services employing big data has led most countries to create big-data platforms for healthcare, which can be used across the industry [3]. Amid increasing use of big data across domains, the European Union (EU) and countries such as Finland have already enacted laws to protect people's personal information. The same is true for Korea; yet Korea's policies for protecting personal information have obstructed data linkages between healthcare institutions or

Received: September 6, 2023; **Revised:** November 21, 2023; **Accepted:** December 18, 2023
Correspondence to Hun-Sung Kim, MD
Department of Medical Informatics, College of Medicine, The Catholic University of Korea, 222 Banpo-daero, Seocho-gu, Seoul 06591, Korea
Email: 01cadiz@hanmail.net

hospitals. Studies have shown that the legal basis for utilizing data in Korea is insufficient, which has led to a failure in meeting industry demands. In 2018, a big-data utilization platform for healthcare was launched in Korea for linking medical data from the National Health Insurance Service (NHIS), the Health Insurance Review and Assessment Service (HIRA), the Korea Disease Control and Prevention Agency (KDCA), and the National Cancer Center. In addition, "three data-related bills (the Personal Information Protection Act [PIPA], Act on Promotion of Information and Communications Network Utilization and Information Protection, and Credit Information Use and Protection Act)" were amended [4–8]. During this process, a special provision for processing pseudonymous information was made, for purposes of statistical writing, scientific research, preservation of public interest records, and establishing the legal basis for instituting a personal information manager (or an honest broker) to utilize pseudonymized personal information without requiring consent [4,7].

Recently, the Korean government established a close public-private cooperation system, with the larger goal of implementing the "My HealthWay System" [9]. While previously, only financial data were digitalized, the establishment of the "My HealthWay System" enables the integration of various types of citizen's data, such as insurance information and credit scores, under the government's My Data Service. These changes imply that Korea's personal information protection system, which had been quite conservative in disclosing medical data, is approaching the assumed global standard. However, compared to other major countries, Korea's current personal information protection laws continue to block the availability of information to a large extent. This paper reviews the current state of Korea's healthcare big data and related laws, and compares it with the EU's General Data Protection Regulation (GDPR) [10], and Finland's Act on the Secondary Use of Health and Social Data [11], to suggest future direction for Korea's personal information protection legislation.

CONFLICT BETWEEN PROTECTION OF PRIVACY AND PUBLIC INTEREST

Sensitive information

Sensitive information refers to information regarding an individual's ideology, beliefs, labor-union affiliation, political party membership, political opinions, health status, and other kinds of personal information that may significantly infringe on their privacy [12,13]. According to Article 15(1) of the PIPA [4], an information holder can process another person's general personal information after obtaining their consent; however, sensitive information closely concerns an individual's most private aspects. Therefore, for processing sensitive information, Article 23(1) of the same Act [4] mandates seeking consent from the subject of the information, in addition to seeking their consent for processing personal information (i.e., double consent is required). Ultimately, the person concerned must agree to provide their personal information. Considering that simply knowing which disease an individual is afflicted with could reveal their physical or mental inadequacies, medical history is part of sensitive information, as it is closely tied to one's core personality. Other related aspects that require protection include information about who, when, where, what kind of treatment, and the amount of money spent. For example, in the case of hospitals specializing in gynecology, obstetrics, urology, psychiatry, etc., one's possible ailment can be predicted simply by the medical institution's name; combining this with information about medical-care benefits, number of days of hospitalization and visits, and self-payments, one could even infer the individual's specific physical and mental limitations.

Protection of personal information over public interest

The aforementioned context is associated with many legal cases in which judges have set precedents to deal with the contradictions between public interest and protection of personal information [4,14,15]. In the scenario presented in Table 1 [14], the NHIS provided sensitive information of wanted criminals to the chief-of-police that indicated the claimant's type of disease and health status. Considering that sensitive information constitutes the core of an individual's personality and privacy, the judges concluded that the claimant's right to self-determination of personal information had been violated, as the act of providing information was very serious. Therefore, the Constitutional Court ruled that the actions of the NHIS and the chief-of-police violated the individual's right to self-determination regarding information.

Table 1. Cases of unconstitutional provision of sensitive information for public interest [14]

Case	Summary
Situation	At the request of the police chief, Korea's National Health Insurance Service provided details of the medical benefits of wanted criminals.
Issue	Was this provision of health information an unfair infringement on the interests of the data subject or of a third party?
Key point	In principle, the subject of information must consent to the processing of sensitive information (double consent for processing personal and sensitive information), according to Article 23(1) of the Personal Information Protection Act [4].
	While investigating a crime, sensitive information may be provided if it is unavoidable except in cases where there is a possibility of unreasonably infringing on the interests of a data subject or third party according to Article 18(2), seventh paragraph of the Personal Information Protection Act [4] and Article 8, second paragraph of the Enforcement Decree of the Act on the Performance of Duties by Police Officers [15].
Judicial precedent	It has been adjudged that the legitimacy of the purpose of providing information and the suitability of the means must be recognized.
	However, the relatively long-term care benefit details of the past 2 to 3 years do not constitute information that can allow immediately identifying, at least, a suspect's location.
	There are various ways to track the location of criminals. Therefore, it has been adjudged that the act of providing information is not a way to minimize the invasion of privacy.
	In particular, the payment date and the nursing home's name are important pieces of information for predicting the offender's type and the severity of the disease.
	Since the above constitutes comprehensive information about the health status of wanted criminals, it is regarded as sensitive information that is closely related to the intimate aspects of an individual's personality and personal information.
	The Constitutional Court held that sensitive information requires greater protection than does other general personal information because it is related to the core of an individual's personality and privacy.
	Therefore, it was decided that, in this case, the act of providing information violated the principle of excessive prohibition and right to self-determination of personal information.

Most Korean citizens are enrolled in the NHIS, which contains a vast amount of health information included in the National Health Insurance Corporation [16,17]. The NHIS's information about medical-care benefits includes not only individual details but also sensitive information; together, they constitute comprehensive and integrated information about a person's health. The subject of information must provide consent for processing such sensitive information, notwithstanding the provisions of Article 18(2), seventh subparagraph of the PIPA [4].

FACTORS IMPEDING THE USE OF PERSONAL INFORMATION

Restrictions to processing sensitive information: pseudonymized and anonymized information

In principle, a safe pseudonymization method enables the use of sensitive information as pseudonymized information [18]. However, unless existing technology provides a perfectly safe pseudonymization method, an individual's personal information cannot be processed without obtaining their consent. Notably, most of the discussions regarding the processing of personal and sensitive information occurred in the past. The crux of the problem related to processing sensitive information is that the availability of data decreases with the increasing legal requirements for pseudonymization [19]. This is clearly highlighted in the provisions made through Article 3(7) of the PIPA [4]. If personal information can be either anonymously or pseudonymously processed by a personal information manager, it is ideal to stick to the former, as the latter presents several difficulties.

Unrealistic consent requirements of certain laws

Existing laws mandate seeking consent several times, which is another factor hindering the use of personal information. For example, according to Article 15(1) of the PIPA [4], a personal information manager can collect personal information only when the subject of information has provided consent. In addition, according to Article 17(1) of

the same Act [4], the collected personal information can be provided to a third party that solely aims to collect this information (and not use it), only after the individual's consent has been obtained. Again, according to Article 18(1) of the same Act [4], consent must be obtained from the subject of information when the information is used beyond the scope of the original purpose and provided to a third party. The conditions for consent are also quite strict. According to Article 22 of the same Act [4], personal information managers must clearly recognize certain key points, such as whether personal information has been collected, the purpose of its use, the items to be collected and used, and the retention period. They are responsible for informing the subjects and seeking their consent. The fact that it is a legal regulatory provision to protect data subjects' self-determination rights, makes it reasonable at first glance, but further examination clearly shows that seeking "consent" to protect data subjects' rights and interests blocks the possible use of this data to a large extent.

Despite these constraints, the law does stipulate the possible uses of data, other than the case of Article 17(1) second subparagraph of the PIPA [4] mentioned above. The law also regulates possible use, and restrictions, other than those mentioned in Article 18 of the same Act [4]. This creates problems because, apart from the fact that collecting consent at each stage is quite cumbersome, the actual act of collecting information takes so long that the subject of the information cannot often be contacted for seeking additional consent for the subsequent stages. Because of these limitations, the demand to amend the relevant provisions for preventing the loss of valuable medical information resources is gaining strength. Indeed, according to Article 17(4) of the PIPA [4], if a personal information manager deems that there shall be no disadvantage to the data subject within the scope of the original purpose of collection, and necessary safety measures such as encryption have been taken, as prescribed by the Presidential Decree, personal information may be collected without the data subject's consent. However, the reasonable circumstances in which personal medical information may be collected are unambiguous or not easy to define, because there is no unified view or guidelines about what is reasonably related. Whether something is reasonable must ultimately be determined by the court on a case-by-case basis. Consequently, personal information managers have no choice but to conform to requirements for seeking "consent," to avoid legal responsibility. Thus, a lot of medical information is going in vain, without being utilized.

COMPARISONS AND DIFFERENCES WITH FOREIGN CASES

GDPR of the EU

With the EU's formation as a single supranational entity, the economic and social functions of its member states were rapidly integrated [20]. In this process, people's personal information was extensively exchanged, which led the EU to enact the GDPR as a unified guideline for processing personal information [21]. The GDPR inherits and develops the basic spirit of the previous Data Protection Directive (DPD), for protecting and standardizing personal information about the citizens of the member countries [21]. The GDPR establishes standard guidelines for the member states, which in turn have particular legal frameworks for protecting personal data [21,22].

The GDPR protects personal information while allowing for its free movement within the EU [21]. One of the GDPR's characteristics, which acted as the basis of Korea's "MyData Project" [23] is a substantial strengthening of the data subjects' rights. The GDPR not only incorporates individuals' rights to receive (that existed under the DPD), access, and correct information, but also strengthened other rights, such as the right to delete information (the so-called right to be forgotten) [24]. In addition, by newly establishing rights to restrict information processing, enable the portability of personal information, and object, it formed a structure to ensure that only information based on the data subject's right to choose could circulate in the market [25]. According to the GDPR, private companies, including public institutions, are obliged to move personal data to other locations, and correct or delete existing information, if the data subject so desires (right to data portability, right to correct/delete data) [26].

Finland's Act on the Secondary Use of Health and Social Data

In 2019, the Finnish Parliament passed the Act on the Secondary Use of Health and Social Data [11], which introduced strict data-security requirements and authorization proce-

dures. The Act was based on the GDPR's basic spirit, which stipulates that personal information can be secondarily used for preserving public records, and other scientific, historical, and statistical purposes. However, this Act goes a step further than the GDPR, by allowing the collected medical information to be used for development and innovation activities. Therefore, in Finland, private research institutes and companies can use public data for industrial purposes [27]. This Act consolidates fragmented national rules for the use of health and social security data. In addition, it was considered key for reviving the Finnish healthcare industry, as it fostered opportunities for research and innovation across the fields of health, welfare, disease prevention, novel treatment methods, and predictable personalized medicine.

However, in Finland, most of the human governance of the data permission organization is conducted by representatives of government departments, public institutions, and local governments, and only one private welfare and health service provider has been included as mentioned in section 8, first paragraph of the Act [11]. Nevertheless, the Act does allow the possibility of establishing an expert group in accordance with section 8, fourth paragraph, to receive assistance in preparing guidelines for anonymity, data protection, and security for business processing.

Korea's MyData Service

With the amendment to Korea's Credit and Information Use and Protection Act [6] in 2020, Article 33(2), the "personal credit information management business" was established to realize the right to request transmission of personal credit information, to introduce the "My Data Industry" in the financial field. However, MyData is not based on the PIPA, but the Credit Information Use and Protection Act, which applies only to credit information [28]. In this respect, the discussion about the right to self-determination of personal information is still in its infancy. Moreover, by assuming that the subject of information is the owner of data, the position of the institution or hospital remains ambiguous. Thus, it is difficult to expect that hospitals would voluntarily cooperate in responding to each data subject's request, as it requires considerable time and money, in addition to depriving them of depriving them of the right to control their own data. After all, the current legislation does not enable a standardized and integrated way of providing information. Personal information can only be transferred from one medical institution to another. A truly national system of maintaining health records can be implemented only when the relevant laws and regulations are revised.

IMPLEMENTING THE MYDATA SERVICE IN THE MEDICAL FIELD

The Korean Ministry of Health and Welfare has launched a pilot project in 2022. It has recruited around 400 patients from Seoul St. Mary's Hospital (Seoul, Korea) and the Pusan National University Hospital (Busan, Korea), as participants for the MyData Service [23]. The participants were required to use a mobile application for requesting, receiving, and viewing their medical records. A quick glance would show how their data was being used.

Significance of the current MyData Service

The launch of the MyData pilot project in the medical field can be interpreted as acceptance of the basic idea of the GDPR, the EU's personal information protection law. Korea had regarded subjects of information as passively "consenting" while providing information. By contrast, the MyData Service in the medical field assumes the subject of information as an active agent, and grants them the right to self-determination. It allows individuals to decide the amount and the type of information they wish to provide and goes beyond simply guaranteeing the right to decide whether to provide information or not.

Depending on the specifics of the case, the subject of information may withdraw the information provided, or request it to be provided to a third party. This enables them to actively decide on all aspects related to their personal information [9]. Individuals can choose how to move their personal information. This problem-solving method harmonizes the two incompatible goals of "protection of privacy" and "free distribution of data," which were considered sensitive for personal information protection. This change is quite forward-looking, in that Korea's information protection policy is converging with the assumed global standard.

Limitations of the current MyData Service

Scholars have pointed out that related laws and regulations are still unable to keep pace with technological development. For example, to establish an exclusively medical MyData Service, private institutions must be able to utilize the data collected by medical institutions. In this case, they would naturally need to have the authority to process the personally identifiable information, including the data subject's resident registration number [27]. However, so far, the current legislation does not specify institutions' legal authority to use medical data. In addition, existing laws (PIPA, Enforcement Decree of Bioethics and Safety Act, Medical Service Act, National Health Insurance Act, etc.) for regulating personal information are ultimately intended to suppress its use. Moreover, they do not provide a unified legal guideline, because they were either enacted or revised according to the needs of the time. Finally, the ambiguous definition of "consent" must be improved. As per existing legislations, only a simplistic service for receiving and utilizing medical information for administrative convenience can be implemented. Without revising the relevant laws and regulations, it shall be impossible to create services that can utilize information from medical and other public institutions, as well as personal health information.

NECESSITY OF CHANGING THE CONCEPT OF PUBLIC INTEREST AND GOOD FOR PERSONAL INFORMATION PROTECTION: THE PRINCIPLE OF PROPORTIONALITY AS A STANDARD FOR PERSONAL INFORMATION PROTECTION

The principle of proportionality originally originated in French and German laws, but over time, it become increasingly important in many legal systems, including the EU laws [29]. The principle of proportionality is derived from the general principle of public law, which weighs measures in favor of public interest against the resulting damages to private interests and fundamental rights [30]. Therefore, administrative measures must be appropriate and necessary for enforcing public interest while balancing any a public interest intervention with private interests [21]. Therefore, the purpose and the effect of the intervention must be proportionate. For example, measures that are favorable to public interest and strongly interfere with private freedoms should be abandoned. Proportionality requires that where several possible measures are available, measures that cause milder interference to private freedoms should be preferred. The GDPR emphasizes that personal data processing must be designed to be in the public interest [10]. An example is that the right to personal data protection is not an absolute right and must be balanced with other fundamental rights based on the principle of proportionality.

The same principle implies that certain categories of data processing may be necessary for protecting public interest in the field of public health without requiring the consent of the data subject [10]. However, the EU's GDPR only strengthens the basic rights of the data subjects in some situations [31]. Interestingly, Finland's secondary health–use law [11] is the only one that applies the principle of proportionality. Thus, countries should strive to balance the protection of personal data and privacy with economic interests.

Until now, the state was seen as a protector of personal information that prevented data leaks in public interest. However, governments must explore the possibility of an environment wherein corporate autonomy and creativity are respected, and data subjects are provided enhanced options. Greater availability of information would lead to the emergence of new industries, improving the growth potential of existing companies, ultimately creating quality jobs. In the current age of low fertility and an aging population, encouraging data use and corresponding healthcare innovations could be an effective solution for saving the humankind from diseases and aging. To this end, the concept of public interest and good, as we know it, must be redefined and the public discourse should focus on the issue of what protects public interest.

CONCLUSIONS: NECESSITY OF CREATING A GOVERNANCE STRUCTURE FOR HEALTHCARE DATA

In the era of digital transformation, the demand for innovation, problem solving, and value creation using medical data is increasing [1]. The basic rights of data subjects are still core values that cannot be waived off. Therefore, despite the changing times, thinking about ways to protect the rights of data subjects and establishing a safe transaction environment will remain the biggest task for legisla-

tors. While avoiding unnecessary or overly restrictive regulations, legislators must strive to protect the core values of the community.

The structured generation of knowledge through the formation of fair processes also requires a well-formed decision-making body. In a highly developed information society, decision-makers need a fair and rational governance processes, irrespective of whether it is an official or private organization [32]. Based on the examples of the EU and Finland, establishing data governance that facilitates the smooth sharing and utilization of healthcare data can be an effective way to facilitate the reuse and sharing of data. High-level administration is increasingly dependent on the participation of private regulators in carrying out the state's takes. Therefore, a consensual arrangement between the state and private actors must be established in many areas [32]. The concept of "governance" is as old as human civilization. It involves the processes of decision-making and implementation. Governance analysis focuses on formal and informal actors involved in decision-making, and formal and informal structures for reaching and executing decisions [33]. To arrive at a more balanced legislation, businesses, experts, civic groups, consumers, governments, and public institutions should engage in dialogue and invite diverse opinions, and the impact of data reuse on data subjects should be thoroughly analyzed. This is because the legitimacy, reliability, and acceptability of decisions will improve only when the knowledge, experience, and wisdom created by collective intelligence are actively respected and utilized.

ARTICLE INFORMATION

Author contributions

Conceptualization: RK, HSK; Data curation: all authors; Formal analysis: all authors; Funding acquisition: HSK; Investigation: HSK; Methodology: HSK; Project administration: HSK; Resources: HSK; Software: HSK; Supervision: HSK; Validation: HSK; Visualization: RK; Writing—original draft: RK; Writing—review & editing: all authors. All authors read and approved the final manuscript.

Conflicts of interest

The authors have no conflicts of interest to declare.

Funding

This study was supported by the Medical AI Education and Overseas Expansion Support Research Program through the National IT Industry Promotion Agency (NIPA) funded by the Korean Ministry of Science, ICT and Future Planning.

ORCID

Raeun Kim, https://orcid.org/0000-0003-1245-7289
Jiwon Shinn, https://orcid.org/0000-0002-9131-6128
Hun-Sung Kim, https://orcid.org/0000-0002-7002-7300

REFERENCES

1. Tanniru MR, Agarwal N, Sokan A, Hariri S. An agile digital platform to support population health: a case study of a digital platform to support patients with delirium using IoT, NLP, and AI. Int J Environ Res Public Health 2021;18:5686.
2. Kim HS, Yoon KH. Lessons from use of continuous glucose monitoring systems in digital healthcare. Endocrinol Metab (Seoul) 2020;35:541–8.
3. Golinelli D, Boetto E, Carullo G, Nuzzolese AG, Landini MP, Fantini MP. Adoption of digital technologies in health care during the COVID-19 pandemic: systematic review of early scientific literature. J Med Internet Res 2020;22:e22280.
4. Korea Law Translation Center. Personal Information Protection Act. Act No. 16930 (February 4, 2020) [Internet]. Korea Legislation Research Institute; [updated 2021 Mar 31; cited 2023 May 17]. Available from: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
5. Korea Law Translation Center. Act on Promotion of Information and Communications Network Utilization and Information Protection Act. Act No. 17348 (June 9, 2020) [Internet]. Korea Legislation Research Institute; [updated 2021 Jul 29; cited 2023 May 17]. Available from: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55570&lang=ENG
6. Korea Law Translation Center. Credit Information Use and Protection Act. Act No. 16957 (February 4, 2020) [Internet]. Korea Legislation Research Institute; [updated 2023 Mar 14; cited 2023 May 17]. Available from: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=63719&lang=ENG
7. Korea.kr. [Three data bills] [Internet]. Korean Ministry of Culture, Sports and Tourism; 2021 [cited 2023 May 17]. Available from: http://www.korea.kr/special/policyCurationView.do?newsId=148867915

8. Lee D, Park M, Chang S, Ko H. Protecting and utilizing health and medical big data: policy perspectives from Korea. Healthc Inform Res 2019;25:239–47.
9. Korean Ministry of Health and Welfare. [Press release: the launch of the My HealthWay (a digital highway)] [Internet]. Korean Ministry of Health and Welfare; 2021 [cited 2023 May 17]. Available from: https://www.mohw.go.kr/react/al/sal0301vw.jsp?PAR_MENU_ID=04&MENU_ID=0403&CONT_SEQ=363763
10. EUR-Lex. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (text with EEA relevance) [Internet]. EUR-Lex; 2016 [cited 2023 May 17]. Available from: http://data.europa.eu/eli/reg/2016/679/oj
11. Finnish Ministry of Social Affairs and Health. Act on the Secondary Use of Health and Social Data [Internet]. Finnish Ministry of Social Affairs and Health; 2019 [cited 2023 May 17]. Available from: https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf?t=1559641328000
12. Korea Law Translation Center. Enforcement Decree of the Personal Information Protection Act. Presidential Decree No. 28355 [Internet]. Korea Legislation Research Institute; [updated 2018 May 3; cited 2023 May 17]. Available from: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=45683&lang=ENG
13. Kim YM. A study on the activation of health care big data: focusing on the Finnish case. Bio-Med Law 2019;22:5–38.
14. Constitutional Court of Korea. Decision of August 30, 2018 (2014Hun-Ma368) [Internet]. Constitutional Court of Korea; 2018 [cited 2023 May 17]. Available from: https://isearch.ccourt.go.kr/search.do#view.do?link=40911_010300%20%E2%80%93%20%ED%95%9C%EA%B8%80%ED%8C%90%EB%A1%80:%202014%ED%97%8C%EB%A7%88368
15. Korea Law Translation Center. Enforcement Decree of the Act on the Performance of Duties by Police Officers. Presidential Decree No. 29900 (June 25, 2019), Article 8 [Internet]. Korea Legislation Research Institute; [updated 2020 Sep 18; cited 2023 May 17]. Available from: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=51387&lang=ENG
16. National Health Insurance Sharing Service (NHISS). Data provision guide [Internet]. NHISS of Korea; c2019 [cited 2023 May 17]. Available from: https://nhiss.nhis.or.kr/bd/ab/bdaba001cv.do;jsessionid=s21oa35g1U7B1U5ah1L3ifTEUFH0ke4zLLiezGMJqja00jmpbG3jv7SmEFN9Xmp1.primrose22_servlet_engine10
17. Kyoung DS, Kim HS. Understanding and utilizing claim data from the Korean National Health Insurance Service (NHIS) and Health Insurance Review & Assessment (HIRA) Database for research. J Lipid Atheroscler 2022;11:103–10.
18. Mandl KD, Perakslis ED. HIPAA and the leak of "deidentified" EHR data. N Engl J Med 2021;384:2171–3.
19. Shin SY, Kim HS. Data pseudonymization in a range that does not affect data quality: correlation with the degree of participation of clinicians. J Korean Med Sci 2021;36:e299.
20. Zhao X, Shi C, Li Y. Can European Union (EU) enlargement boost regional economic common growth? Multi-period difference-in-difference (DID) method. J Environ Public Health 2022;2022:4502628.
21. Chico V. The impact of the General Data Protection Regulation on health research. Br Med Bull 2018;128:109–18.
22. Vlahou A, Hallinan D, Apweiler R, Argiles A, Beige J, Benigni A, et al. Data sharing under the general data protection regulation: time to harmonize law and research ethics? Hypertension 2021;77:1029–35.
23. Korea.kr; Korean Ministry of Science and ICT. [9 Trillion for digital new deal this year: speeding up 'digital transformation'] [Internet]. Korean Ministry of Culture, Sports and Tourism; 2022 [cited 2023 May 17]. Available from: https://www.korea.kr/special/policyFocusView.do?newsId=148898510&pkgId=49500747
24. Mondschein CF, Monda C. The EU's General Data Protection Regulation (GDPR) in a research context. In: Kubben P, Dumontier M, Dekker A, editors. Fundamentals of clinical data science. Springer; 2019. p. 55–71.
25. Panetta R, Cristofaro L. A closer look at the EU-funded My Health My Data project. Digit Health Leg 2017:(11);10–1.
26. Shabani M, Borry P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. Eur J Hum Genet 2018;26:149–56.
27. Vikstrom A, Moen H, Moosavi SR, Salakoski T, Salantera S. Secondary use of electronic health records: availability aspects in two Nordic countries. Health Inf Manag 2019;48:144–51.
28. Kim EC, Kim EY, Lee HC, Yoo BJ. The details and outlook of three data acts amendment in South Korea: with a focus on the changes of domestic financial and data industry. Inf Policy 2021;28:49–72.
29. Choi J. [Control of administrative actions by the principle of proportionality in Germany and Korea]. Public Law 2009;37:45–87.
30. Wienbracke M. [Legal methodology]. 2nd ed. CF Müller; 2020.

31. Molnar-Gabor F, Sellner J, Pagil S, Slokenberga S, Tzortzatou-Nanopoulou O, Nystrom K. Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: insights from Germany, Greece, Latvia and Sweden. Semin Cancer Biol 2022;84:271–83.
32. Kim YM. A study on the legality of contracts under public law: focusing on the implications of our administrative law. Public Law J 2020;21:471–512.
33. Fukuyama F. What is governance? Governance 2013;26:347–68.