Editorial

Healthc Inform Res. 2020 July;26(3):163-165.
https://doi.org/10.4258/hir.2020.26.3.163
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Big Technology and Data Privacy

Kwangmo Yang[1,2]

[1]Department of Medical Humanities, Sungkyunkwan University School of Medicine, Seoul, Korea
[2]Center for Health Promotion, Samsung Medical Center, Seoul, Korea

On January 9, 2020, amendments to three regulations related to data were passed by the National Assembly of the Republic of Korea: the Personal Information Protection Act, the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc., and the Credit Information Use and Protection Act [1]. The amendments of these acts are abbreviated by the media as the "Three Data Bills (TDB)". While the past laws put more emphasis on protection of personal information, the TDB not only provide data protection but also paved the way for data utility.

The potential usefulness of big data in healthcare allows healthcare policy decisions to be made based on data, supports medical developments through data research, and makes data-driven precision medicine achievable [2]. However, the Korean laws have focused mostly on the protection of such data. As a result, academic and industrial circles have been demanding changes to encourage data sharing.

One of the noticeable changes made to the amended TDB is that pseudonymous data is explicitly defined [3]. Article 2 of the Personal Information Protection Act (PIPA) defines pseudonymized information as personal information that is pseudonymized and becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state. Although de-identification or anonymization is not subject to the PIPA, pseudonymization is explicitly defined and falls within the scope of personal data in the Act.

In the amended Act, pseudonymized information may be processed without the consent of data subjects for statistical purposes, scientific research, and the preservation of records for the public interest, and so forth. A specialized institution designated by the Protection Commission or a related administrative agency may combine pseudonymized information stored outside the organization. Moreover, it may become possible to combine claim data of the National Health Insurance Service or the Health Insurance Review & Assessment Service with the patient information stored in hospitals.

The amendment of the PIPA follows the trend of the protection of personal information standards of developed countries. This means that it is also a change to meet the protection standards of the European Union's General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) of the United States.

Meeting strict GDPR personal data protection standards is tough, especially for the companies exporting to Europe. Therefore, Korean laws have been amended to comply with the GDPR requirements to facilitate the export of local products abroad. The GDPR, like the TDB, also defines pseudonymized data as personal data and renders information no longer re-identifiable if there is no additional information [4]. We may infer that the GDPR recommends pseudonymization to process and utilize data.

The HIPAA by the US government achieves the de-identification of protected health information through the expert determination method and safe harbor method [5]. The expert determination method has the disadvantage that it is necessary to appoint an expert for each study, requiring more money and time investment. On the other hand, it also

has an advantage of having the flexibility to determine identification according to technological changes. Each expert must document the methods and results of analysis and may be required to submit documents upon request by the Office for Civil Rights.

The safe harbor method is used for the de-identification or removal of personal information in accordance with the Privacy Rule of HIPAA. If an individual is not identifiable even with the combination of removed data and other information, it is possible to freely collect and process information without the restrictions of the HIPAA. While simplicity is an advantage, the downside is that the value of the data may be reduced.

The GDPR and HIPAA ensure the protection of personal information and allow the flow and use of health information. Korean law has been amended in line with this trend; however, the law still has shortcomings. As many civil society organizations have pointed out, it is a great pity that the TDB does not have the profiling protection measures specified in the EU's GDPR. In a recent Korean case, the government sent a text message for mandatory health checks to those who had been in Itaewon and had access to the telecommunications base station for more than 30 minutes during the massive outbreak of COVID-19 from Itaewon clubs. Although this was to prevent spread of the epidemic, it makes one wonder whether the telecommunications company was obliged to disclose the list of names of individuals who had only been in the area of Itaewon and not in the clubs. It would have been very controversial under a similar circumstance in Europe.

On March 22, 2017, the United Nations Human Rights Council expressed concerns regarding profiling in modern society. It stated that individuals may be discriminated against through profiling and that individual rights are likely to be violated in digital environments [6]. If these changes are permissible, it may undermine and interfere with the freedom of expression and opinion.

The ambiguity and vagueness of the Act needs improvement. According to the amended PIPA, pseudonymized information may be processed without the consent of the data subjects for statistical purposes, scientific research, and the preservation of records for the public interest. In this context, the scope of consent is ambiguous. If literally interpreted, consent may be waived for for-profit organizations when collecting statistical data. Some individuals may find it unacceptable to imply consent. Also, it is unclear whether pharmaceutical companies undertaking clinical research to develop new medications or companies developing digital therapeutics are waived from obtaining consent and are free to use health information for scientific research.

The Korean government also has not made sufficient effort in communicating with Korean citizens. We may refer to the case of the English care.data programme, a national data-sharing initiative for health records, which was discontinued for a number of reasons. The majority of the UK healthcare services are publicly funded. The general practitioners (GP) of the National Health Service (NHS) are organized into regions, and each patient is designated to a GP for medical care. GPs are contracted with the NHS and are paid by the NHS-funded budget. Consequently, patients' health information is stored with GP clinics on-site and is not managed by health authorities.

As a result, the care.data programme was introduced. Essentially, the patients could opt out of the scheme if they wished not to disclose personal information to care.data. More than one million patients have opted out of the care.data programme because of lack of awareness of and trust in the project. Soon after, the project was stopped. Many reports claimed that poor communication was a major factor that resulted in the failure of the project.

Likewise, the changes made to the TDB should be actively communicated to Korean citizens. The majority of the citizens do not understand the changes that the TDB will bring. Experts are also unable to articulate what route should be taken. Nevertheless, it will be a good starting point to transparently talk about why the TDB was amended and how the TDB can be improved. As we are facing the big technology paradigm of the big data era, more efforts should be made to ensure that individual data privacy is not infringed.

ORCID

Kwangmo Yang (https://orcid.org/0000-0002-7176-4935)

References

1. Policy Wiki. Three Data Bills [Internet]. Sejong, Korea: Ministry of Culture, Sports and Tourism; c2020 [cited at 2020 Jul 30]. Available from: http://www.korea.kr/special/policyCurationView.do?newsId=148867915.
2. Ko HS, Lee DJ, Lee SK. Legal feasibility study and guidelines for the utilization of health insurance big data and the provision of health service [Internet]. Wonju, Korea: National Health Insurance Service; 2016 [cited at 2020 Jul 30]. Available from: https://www.gov.kr/portal/gvrnReport/view/G1811000000189871?policyType=G00302

 https://doi.org/10.4258/hir.2020.26.3.163

&srchTxt=%EA%B1%B4%EA%B0%95%EB%B3%B4%ED%97%98.
3. National Law Information Center. Personal Information Protection Act [Internet]. Sejong, Korea: Ministry of Government Legislation; 2017 [cited at 2020 Jul 30]. Available from: http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95.
4. European Commission. EU General Data Protection Regulation (GDPR) [Internet]. Brussels, Belgium: European Commission; c2019 [cited at 2020 Jul 30]. Available from: https://gdpr-info.eu/.
5. US Department of Health & Human Services. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [Internet]. Washington (DC): US Department of Health & Human Services; 2012 [cited at 2020 Jul 30]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.
6. Goldstein K, Tov OS, Prazeres D. The right to privacy in the digital age [Internet]. Geneva, Switzerland: The Office of the High Commissioner for Human Rights; 2018 [cited at 2020 Jul 30]. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf.