

Regulation on Processing and Protecting the Privacy of Personal Health Data

Authors: Gönenç Gürkaynak, Esq., İlay Yılmaz, Nazlı Pınar Taşkiran, ELİG, Attorneys-at-Law

The Regulation on Processing and Protecting the Privacy of Personal Health Data (“Health Data Regulation”) has recently been published on the Official Gazette, on October 20, 2016 and came into force on the same date.

This regulation is not only applicable to the health institutions and the data subjects whose personal data is processed, but also covers real persons and legal entities who process health data within the scope of a legislation. Therefore, all companies processing health data for reasons such as employment procedures, periodic inspection or due to obligations arising from social security legislation will be subject to the provisions of the Health Data Regulation.

The purpose of the Health Data Regulation is to set out the procedures and principles to protect personal health data and to ensure its privacy, to regulate the provisions regarding the system which will be established to collect, process, transfer the personal health data and to access to such data and regarding the security and supervision of the systems in which the personal health data are recorded, and regarding notifications to the Ministry of Health (“Ministry”) on the employee movements during the provision of health services.

Most of these definitions are in line with the Turkish DP Law, and certain additional definitions are introduced, which are specifically defined for the Health Data Regulation, such as, the Ministry, the information security administrator, the general management, personal health record system, committee, central health data system, undersecretary, health service provider, and intervention team of cyber incidents. Under the Health Data Regulation, personal health data means any kind of health information relating to an identified or identifiable real person.

Health Data Regulation sets out principles for the protection, processing, transferring and erasure of personal health data. As per Article 6 of the Health Data Regulation, the data processor is obliged to protect the privacy of personal health data and obey the rules and standards of data protection and processing which will be determined by the Ministry. In case of a data breach, health service providers should notify the Ministry in the form prescribed under the same provision. Health service providers should take all the necessary measures which will be determined by the Ministry in order to protect the privacy of the personal health data. If there is a suspicion of a possible data breach a notification should be made to the Ministry and a pre-drafted form should be used to make this notification. The notification may also be submitted to the Ministry by electronic means. After an investigation regarding the personal health data breach, following the investigation carried out on the relevant breach, data subjects will be informed by the Commission of Personal Health Data which is established under the Ministry.

Personal health data can be processed without the data subject's explicit consent; (i) to protect public health, (ii) to perform preventive medicine, medical diagnosis, treatment and nursing services and (iii) to manage and plan health services and financing; by the persons who are under confidentiality obligation (e.g. doctors) and by the authorized institutions and organizations.

Transfer of personal health data is regulated under Article 8 of the Health Data Regulation. The personal health data may be transferred; for preserving public health, performing preventive medicine, medical diagnosis, treatment and nursing services; managing and planning health services and financing by way of taking precautions which will be determined by the Data Protection Board, to the relevant institutions and organizations, if it is clearly regulated by laws. Additionally, data transfer in between the institutions and organizations which are requesting the data within the scope of their duties and responsibilities that are regulated by law and the Ministry along with the institutions and organizations under the Ministry would be regulated by a protocol prescribing the relevant measures for transfer of personal health data and other requirements. Moreover the requests for (i) transfer of personal health data abroad and (ii) any other transfer apart from the ones stated above will be governed by the Turkish DP Law and the Health Data Commission established under the Ministry shall evaluate these transfer requests. Therefore, it appears at this early stage that both the Board and the Health Data Commission will be in charge for personal health data.

Provisions for erasure of personal health data are also in line with the Turkish DP Law. In the event that the reasons for which the personal health data are processed are no longer valid, personal health data should be erased or anonymized by the data controller ex officio or upon the demand of the data subject, regardless of whether the personal data has been processed in accordance with the relevant legislation. In cases where there is an erasure request for a personal health data and if processing the data may be necessary for the establishment, exercise or defense of a legal claim, or if it is possible to use the data by law enforcement authorities, personal health data will be archived under a registry which will be established by the Ministry.

Finally, the Health Data Regulation fills the legal gap of how to protect personal health data, by regulating the abovementioned provision, along with other rules such as rights of the data subjects. Even though it refers to the Turkish DP Law in many of its provisions, the Health Data Regulation introduces a new regime on personal health data, in a more strict way.

Article contact: Gönenç Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published in ELIG, Attorneys-at-Law Legal Insights Quarterly, December 2016)