MOROĞLU ARSEVEN

Turkey Introduces Rules for Personal Health Data, Allowing Increased Access for Data Subjects and Regulator Oversight

8 Nov 2016

The Ministry of Health of the Turkish Republic ("**Ministry**") has announced procedures and principles for protecting personal health data, ensuring data privacy, as well as processing and transferring personal health data. It also establishes a central system, enabling data subjects to access, amend and share their own personal health data.

The Regulation on Processing Personal Health Data and Protecting Its Privacy ("**Regulation**") was published in Official Gazette number 29863 on 20 October 2016, entering into force on the same date.

Turkey introduced a new data protection regime in 2016, under the Data Protection Law number 6698 ("**Law**") published in Official Gazette number 29677 on 7 April 2016. Further information about the Law and its implementation can be found here. The most recent health-related Regulation is issued in line with the Law.

The Personal Health Data Commission ("**Commission**") will be established under the Ministry to determine the Ministry of Health's policies on personal data in line with the Law and principles of Data Protection Board. It will oversee and monitor personal health data issues, including considering transfer requests, monitoring compliance, as well as resolving complaints and disputes.

Procedure for processing personal health data

A legislative confidentiality obligation applies to everyone who processes personal health data, or accesses such data as part of their duties.

Except for certain limited purposes (below), personal health data can only be processed by informing the data subject in detail about the purpose of processing the personal health data and by obtaining and maintaining explicit written consent from the data subject. Different from the Law, explicit consent for processing personal health data must be in writing, under the Regulation.

Persons or authorized institutions and organizations who are subject to confidentiality obligations, as well as authorized institutions and organizations, can process personal health data without obtaining explicit consent of the data subject, if it is processed for:

- Protecting public health.
- Preventive medicine.
- Medical diagnosis.
- Nursing and treatment activities.
- Planning and administering health services and related financing.

General principles on processing personal health data

General principles apply when processing personal health data:

- Processing must comply with the law and be done in good faith.
- Maintain data accuracy and keep it up to date (if necessary).
- Process data only for specific, clear and legitimate purposes.
- Data should be related, limited and proportional to the purposes of the processing.
- Data should be preserved only for the period necessary for the purpose of the processing.

Employees of health service providers can only process and access personal health data to the extent necessary to provide required health services.

Anonymizing and deleting personal health data

Anonymized personal health data can be published or transferred for the purposes of determining health policies, calculating health costs, or in scientific and statistical studies.

Even if personal health data is processed by complying with the Law and Regulation, if the purpose of processing such personal health data no longer exists, then at the data subject's request, such personal health data must be anonymized or deleted. Even after such deletion or anonymization, such data will still be archived for ten years in the central system for the purpose of maintaining, using or protecting a right, or if and when needed to be served to the judicial authorities by the Ministry without losing the integrity of such data and archived data cannot be accessed except for these purposes. Personal health data transferred to the central database can be deleted from the central database ten years after being registered in the system.

Transferring personal health data

Personal health data can be transferred by and among public institutions and organizations provided that:

- Precautions determined by the Data Protection Board are taken.
- A protocol for transferring personal health data is in place between such public institutions and organizations and the Ministry (or its affiliated institutions and organizations).
- Such transfer is required by law for the purposes of:
    - Protecting public health.
    - Preventive medicine.
    - Medical diagnosis.
    - Nursing and treatment activities.
    - Planning and administering health services and their financing to the public institutions and organizations.

Except for these purposes, personal health data cannot be transferred, unless it is anonymized.

Once established, the Personal Health Data Commission will consider transfer requests for purposes falling outside this scope, as well as requests to transfer data abroad. Consideration will address the Law's provisions and take into account the delicate nature of genetic data.

Data subject rights

A data subject can revoke his or her consent to transfer and process data at any time (unless stipulated by a law, regulation or adjudication). However, revocation will not affect the processes which have already been carried out by that time.

Every citizen can create a user account via the e-government portal or with their family practitioner. Accounts can be used to:

- Track health services provided to the person.
- Manage health records, including:
    - Request removal of certain data.
    - Add missing information.
    - Correct or delete information
    - Deactivate their account.
- Review processes and results of treatment applied in health institutes.
- Access all personal health data from everywhere.
- Share personal health data with authorized third persons.

The Law outlines the rights of personal data subject generally, including rights to:

- Be informed about whether personal health data is being processed.
- Request information about personal health data processing.
- Access and request the personal health data
- Be informed of the processing purpose and whether the data is used in line with these purposes.
- Be informed about third parties receiving the personal health data, in Turkey and abroad.
- Request rectification of incomplete or inaccurately processed health data.
- Request erasure or destruction of data.
- Object to a result obtained and analyzed by means of exclusively automated systems against his/her interest.
- Request for damages in case of a breach.

Data controller responsibilities

The Regulation requires data controllers to collaborate with the information security administrator in the relevant city, or authorized person from the Cyber Cases Intervention Team. This obligation applies to personal health data only, not all personal data contemplated by the Law.

The Law outlines general responsibilities and necessary measures for data controllers to protect personal data. Notably, data controllers should inform data subjects about:

- The data controller's identity (or representative, if any).
- Purposes of processing personal data.
- Transfer of the data and purposes of the transfer.
- Data collection procedure and its legal ground.
- The data subject's rights, as per Article 10 of the Regulation.

Additionally, data controllers are responsible for the safety of collected data and must:

- Prevent unlawful processing of personal health data.
- Prevent unlawful access to personal health data.
- Preserve personal health data.
- Prevent possible data loss in the system they are responsible for.

Health service provider responsibilities

The Regulation defines "Health service provider" as all real persons or public or private legal persons, providing or producing health services.

Health service providers are responsible for establishing systems to manage electronic records, as well as related security and privacy measures. Such systems should also be capable of transferring electronic health records to the central health data system, in line with standards set by the Ministry and Data Protection Board.

Personal Health Data Commission and Health Information Systems General Management

The Personal Health Data Commission will be established under the Ministry Counsellor. No specific deadline is set for the Ministry of Health to establish the Personal Health Data Commission.

Once established, the Commission will consist of ten members and its role will be to:

- Assist the Ministry's policies.
- Provide opinions.
- Resolve disputes.
- Evaluate requests regarding data transfers.
- Review complaints.
- Make necessary checks.

The Commission will be empowered to make checks in related locations, to ensure lawful processing of personal health data and privacy protection.

The Health Information Systems General Management will be responsible for establishing a central data system and issuing regulations on operation of this system.

Please see this link for the full text of the resolution of the Regulation (only available in Turkish).

Related Practices

- Privacy and Data Protection
- Information Technologies

Related Attorneys

- DR. E. SEYF? MORO?LU, LL.M.
- BURCU TUZCU ERS?N, LL.M.