

REGULATION

From the Ministry of Health:

REGULATION ON PERSONAL HEALTH DATA

FIRST PART

Purpose, Scope, Basis and Definitions

Goal

**ARTICLE 1 – (1)** The purpose of this Regulation; Law on Protection of Personal Data dated 24/3/2016 and numbered 6698 Within the scope of the provisions of the Ministry of Health, the central and provincial organization units and operating under them. In the processes and practices carried out by health service providers and their affiliated and related organizations to regulate the procedures and principles to be followed.

Scope

**ARTICLE 2 – (1)** This Regulation covers private law real and legal persons processing personal health data and public health data. activities of legal entities related to the processes and practices carried out by the Ministry of Health. covers.

Rest

**ARTICLE 3 – (1)** This Regulation is governed by the Health Services Basic Law No. 3359 dated 7/5/1987. Article 378 of the Presidential Decree on the Organization of the Presidency No. 1 and dated 10/7/2018 It has been prepared based on the sixth paragraph of the article and article 508.

Definitions

**ARTICLE 4 – (1)** In this Regulation;  
a) Open data: Free of charge or not exceeding the cost of preparation, available to everyone over the internet. freely available for any purpose, without any intellectual property rights anonymous, machine-readable, and thus interoperable with other data and systems.  
b) Open health data: Health data that has been turned into open data,  
c) Anonymization: Personal data, even by matching with other data, are in no way identified or rendering it unable to be associated with an identifiable natural person,  
ç) Ministry: The Ministry of Health,  
d) e-Pulse: The health data of the related persons themselves, physicians or third parties authorized by them The system established by the Ministry in accordance with e-Government applications,  
e) General Directorate: General Directorate of Health Information Systems,  
f) Relevant person: The real person whose personal data is processed,  
g) Relevant user: Person responsible for technical storage, protection and backup of data, or Authority and instruction received within the organization of the data controller or from the data controller, excluding the unit persons who process personal data in accordance with  
ğ) KamuNET: Ensuring data communication between public institutions and organizations, made over a more secure virtual network against physical and cyber attacks that are closed to the internet, cyber security minimizing the risks, providing a standard for existing and future safe closed-circuit solutions, developed by the Ministry of Transport and Infrastructure with the aim of establishing the appropriate infrastructure for applications. the project,  
h) Law: Law on Protection of Personal Data dated 24/3/2016 and numbered 6698,  
ı) De-identification: Personal data; cannot be associated with an identified or identifiable natural person together with other data stored in a different environment, provided that technical and administrative measures are taken for processed in a way that cannot be associated with the person concerned,  
i) Personal data: Any information relating to an identified or identifiable natural person,  
j) Personal health data: Any information relating to the physical and mental health of an identified or identifiable natural person. all kinds of information and information about the health service offered to the person,  
k) Destruction of personal data: Deletion, destruction or anonymization of personal data,  
l) Processing of personal data: Fully or partially automatic or any data processing of personal data. to be obtained, recorded, stored by non-automatic means, provided that it is part of the recording system, to be preserved, modified, rearranged, disclosed, transferred, taken over, made available all kinds of activities carried out on health data such as bringing, classifying or preventing its use. process,  
m) Deletion of personal data: Personal data cannot be accessed in any way for the relevant users and cannot be reused. the process of rendering it unusable,  
n) Destruction of personal data: Personal data cannot be accessed by anyone in any way, the process of making it non-returnable and unusable,  
o) Board: Personal Data Protection Board,  
ö) Institution: Personal Data Protection Authority,  
p) Masking: Covering certain areas of personal data with an identified or identifiable natural person. operations such as erasing, scratching, painting and starring in a way that cannot be associated,  
r) Central health data system: Data collected by the Ministry of personal health data system,  
s) Health service provider: Real persons who provide or produce health services, public law and private law legal persons,  
ş) Data controller: Data recording system that determines the purposes and means of processing personal health data. the natural or legal person responsible for the establishment and management of means.  
(2) For the definitions not included in this Regulation, the definitions in the Law and the secondary regulations made by the Authority. The definitions in the regulations apply.

SECOND PART

General Principles and Principles

General principles and principles

**ARTICLE 5 – (1)** In the processing of personal data, the general principles in Article 4 of the Law, in particular, All principles set forth in the Law shall be complied with.  
(2) To be able to follow everyone's health status and to provide health services more effectively and quickly. The necessary registration and notification system is established by the Ministry and its affiliated and related institutions. This system It can also be created electronically in accordance with e-Government applications. For this purpose, by the Ministry, affiliated and Information systems can be established throughout the country, including the relevant institutions.  
(3) No one may copy past health data except when necessary for the provision of health care. cannot be compelled to present or display.  
(4) By health service providers: the place of unauthorized persons in sections such as counters, box offices and desks. to prevent users from receiving personal data of each other, and to enable service recipients in close proximity at the same time, Necessary physical, technical and administrative measures are taken to prevent them from seeing, learning or seizing.  
(5) Printed materials containing personal health data of the patient, such as health care providers, analysis and examination results. applies the necessary partial de-identification or masking measures on the material and takes other measures to make it difficult to determine who it belongs to, in case it is in the hands of unauthorized persons.  
(6) Everyone can apply to the data controller and have the rights set forth in Article 11 of the Law. can use.  
(7) In the application to the data controller, it is prepared by the Authority according to the 13th article of the Law and 10/3/2018 Communiqué on the Procedures and Principles of Application to the Data Controller published in the Official Gazette dated 30356 provisions are complied with.  
(8) In the fulfillment of the obligation to inform, the Authority, as per Article 10 of the Law, In lieu of the Clarification Obligation published in the Official Gazette dated 10/3/2018 and numbered 30356. The provisions of the Communiqué on the Procedures and Principles to be Complied with in its submission are complied with.

THIRD PART

Access to Personal Health Data

Access of healthcare personnel to data

**ARTICLE 6 – (1)** Persons in charge of providing health services; only the health data of the person concerned will be given. can be accessed on condition that it is limited to the necessity of the health service.  
(2) The health data of people who have an e-Nabız account are accessed within the framework of their own privacy preferences. Relevant persons are informed in detail about their privacy preferences and consequences. Privacy preference and past health from the disruptions and damages that may occur in the provision of health services due to the inability to view the data. The Ministry is not responsible.  
(3) The health data of people who do not have an e-Pulse account are included in the third paragraph of Article 6 of the Law. the area is limited to exceptional purposes only;  
a) Without any time limit, by the family doctor to whom the person is registered,  
b) Limited to the day the appointment is made by the physician to whom the person makes an appointment to receive health care. and until the processes directly related to the health service received are terminated,  
c) Physicians working in the health service provider that the person enters to receive health care services. provided that it is limited to twenty-four hours,  
d) By the physicians working in the health service provider where the patient is admitted, until discharge from the service provider, accessible.  
(4) The access rules in the third paragraph are determined according to the health service delivery needs of the Ministry and according to the Law. It can be re-evaluated by the General Directorate within the scope of the third paragraph of Article 6. Such a In this case, the requirements are met within the scope of the lighting obligation.  
(5) Confidentiality preference for those who do not want their past health data to be accessed by anyone It is offered via e-Pulse. The past health data of people using this privacy preference can only be obtained from the person himself. Sharing the code to be sent to the phone number declared by the physician with the physician and can be accessed by entering the system.  
(6) Persons with a higher level of privacy, in case of being seen and known by others, Personal health data, which have the risk of adversely affecting life and mental health, are determined by the Ministry. Measured restrictions may be imposed on personnel access to this data.  
**Access to data by ministry units**  
**ARTICLE 7 – (1)** It is anonymized to the central health data system by health service providers. persons authorized to match sent health data with the persons they belong to through the relational database. The unit chiefs of the Ministry are determined separately and request the authorization of these persons from the General Directorate. Each The head of the unit may request the authorization of a maximum of three persons from his unit.  
(2) Users authorized by the General Directorate upon the request of the head of the unit can only exercise this authority. personal data, within the scope of planning and management of services and financing, supervision and regulation can be used in accordance with the principles of conservation legislation.  
(3) The limits of planning and management of health services and its financing, legal and administrative determined by the duties assigned to the relevant unit in the regulations.  
**Access to children's health data**  
**ARTICLE 8 - (1)** Parents can register their children's health records via e-mail without the need for any approval. It can be accessed through the pulse. Discerning children have access to their parents' health histories with e-Pulse. may be subject to permission.  
(2) In case of divorce of the parents, the party that is not left on the right of custody, the benefit of the child and the parent in accordance with the personal data protection legislation and the limits determined by the General Directorate within the framework of the child's health data can be accessed.  
**Access of patient relatives to health data**  
**ARTICLE 9 – (1)** Sharing personal health data with patient relatives does not constitute a violation of the principles of the Law. 18 of the Patient Rights Regulation published in the Official Gazette dated 1/8/1998 and numbered 23420. Act in accordance with the third paragraph of the th article.  
**Lawyers' access to health data**  
**ARTICLE 10 – (1)** Attorneys cannot request their client's health data with a general power of attorney. In the power of attorney prepared to transfer the health data of the client to the lawyer, There must be a special provision showing the express consent for the processing and transfer of personal data.  
**Access to the deceased's health data**  
**ARTICLE 11 - (1)** To obtain the health data of a deceased person, by presenting the certificate of inheritance, legal heirs are individually authorized.  
(2) The health data of a deceased person shall be kept for at least 20 years.

CHAPTER FOUR

Hiding, Correcting Personal Health Data,

Disposal and Transfer

Hiding personal health data

**ARTICLE 12 – (1)** Judicial authorities to hide the data of the persons for whom a confidentiality decision has been made. The requirement of the warrant sent by the Provincial Health Directorate is fulfilled by the Provincial Health Directorate. provincial health department The transaction established by the company is directly reflected in the Identity Sharing System. Confidentiality decisions are only due to their duties. All necessary technical and administrative measures are taken to ensure that it is known by those who need to know.  
**Correction of personal health data**  
**ARTICLE 13 – (1)** The person concerned is entitled to rectify the health data created about him inadvertently. apply to the provincial health directorate to which the health service provider for which the health data is generated is affiliated. provincial health directorate of health services, as a result of the research to be carried out on the relevant health service provider, the health data was created inadvertently. If he reaches the information, he applies to the General Directorate with an official letter and asks for the correction of the accidentally created health data.  
(2) The transaction to be established by the General Directorate is also available in the health service provider's own database. is performed.  
(3) The General Directorate, the health data created by the health service providers themselves. determines the date on which it can be corrected and updates this date as needed. After this date determined by the General Directorate health data generated by the relevant health service provider; health data created before this date It is corrected by the General Directorate upon the request of the provincial health directorate.  
**Destruction of personal health data**  
**ARTICLE 14 – (1)** In the destruction of personal data, Article 7 of the Law is determined by the Authority. Deletion and Destruction of Personal Data prepared and published in the Official Gazette dated 28/10/2017 and numbered 30224 or the provisions of the Regulation on Anonymization shall be complied with.  
**Transfer of personal health data**  
**ARTICLE 15 – (1)** In the domestic transfer of personal health data, Article 8 of the Law, abroad In the transfer, Article 9 of the Law is complied with.  
(2) Subparagraph (b) and third paragraph of the second paragraph of Article 8 of the Law and 28 A protocol is drawn up for transferring it to public institutions and organizations within the scope of the th article. In the protocol, the general principles of the personal data protection legislation and the provisions on data security and which data will be transferred. The transfer of data is via KamuNET if the technical infrastructure is suitable. is performed.  
(3) Requests for the transfer of personal health data, the Ministry unit to which the requested health data is relevant. It is evaluated by the General Directorate in terms of the Law and other relevant legislation, according to the result of the evaluation. process is established.

CHAPTER FIVE

Processing for Scientific Purposes and Open Health Data

Processing for scientific purposes

**ARTICLE 16 – (1)** Data controller within the scope of subparagraph (b) of the first paragraph of Article 28 of the Law Scientific studies can be carried out with the personal health data that has been anonymized by  
(2) Personal health data within the scope of subparagraph (c) of the first paragraph of Article 28 of the Law, Technical and administrative procedures to be taken, provided that they do not violate the privacy or personal rights of private life or constitute a crime. It can be processed for scientific purposes within the framework of precautions.

open health data

**ARTICLE 17 – (1)** By the General Directorate, the central and provincial organizations of the Ministry and affiliated and related law The regulations on data privacy and data security in the systems used in the organizations are taken into consideration. to ensure transparency and accountability in the health system, to guide policies and strategies related to health, to support scientific research in the field of health, and to a website dedicated to this subject in order to ensure the development of related products and services. The procedures and principles regarding making it accessible to everyone over the Internet are determined by the Ministry.

CHAPTER SIX

Data security

Obligations regarding data security

**ARTICLE 18 – (1)** Obligations regarding data security in Article 12 of the Law are complied with. In taking technical and administrative measures, the Personal Data Security Guide prepared by the Authority is taken as a basis.  
(2) In case the processed personal data is obtained by others illegally, the data controller The notification to be made by the Board to the Board shall be based on the provisions of the Law and the Board's regulatory actions regarding this matter.  
**Information security**  
**ARTICLE 19 – (1)** Information carried out in the central units of the Ministry, provincial organization and affiliated and related institutions security processes are determined by the Information Security Policies Directive prepared by the General Directorate.

Adequate precautions

**ARTICLE 20 – (1)** In addition, in the processing of special categories of personal data, the fourth article of Article 6 of the Law made by the Personal Data Protection Board pursuant to subparagraph (ç) of the first paragraph of Article 22. Adequate measures in the secondary regulations are respected.

CHAPTER SEVEN

Miscellaneous and Final Provisions

Sanction

**ARTICLE 21 – (1)** In terms of crimes and misdemeanors regarding personal data protected by this Regulation, Procedures are carried out in accordance with Articles 17 and 18.  
(2) For public servants who do not fulfill the requirements of this Regulation, they are assigned to the disciplinary authority. notification is made and their authorization, if any, is revoked. According to the relevant legislation on real persons and private law legal entities transaction is done.  
(3) Sending data to the central health data system in accordance with the procedures and principles determined by the Ministry to the health service providers who do not do so, the third article of the Additional Ministry 11 of the Health Services Basic Law No. 3359. The procedure is established in accordance with the paragraph.

Cases where there is no provision

**ARTICLE 22 – (1)** There is no provision in this Regulation regarding the processing of personal health data. in cases; The law and related secondary regulations are applied.

Repealed regulation

**ARTICLE 23 – (1)** Personal Health Data published in the Official Gazette dated 20/10/2016 and numbered 29863 The Regulation on Processing and Ensuring Privacy has been repealed.

Force

**ARTICLE 24 – (1)** This Regulation enters into force on the date of its publication.

Executive

**ARTICLE 25 – (1)** The provisions of this Regulation are executed by the Minister of Health.