HealthDataSpace Privacy Policy

HealthDataSpace (HDS) is a cloud-based solution for sharing medical data (e.g. radiological image data and reports) with patients and/or physicians providing further treatment. This solution is offered by both Telepaxx Medical Data GmbH and Digithurst Bildverarbeitungssysteme GmbH & Co. KG as cloud-based Software as a Service to hospitals and physicians in private practice. Telepaxx Medical Data GmbH and Digithurst Bildverarbeitungssysteme GmbH & Co. KG are commissioned by these clients to process personal data for the purpose of making it available to patients or doctors providing further treatment. The responsibility under data protection law towards the persons whose medical data is shared lies with the respective hospital or practice where this data is collected and stored in HDS.
The data protection information or consent for the processing of personal data is obtained from the commissioning hospital or practice.

Use of HealthDataSpace

If you have consented, practices and hospitals may upload your medical data to HealthDataSpace for you in lieu of CD generation. In this case, the facility will provide you with an access code that you can use to retrieve your data. The access code is either a 12-digit alphanumeric code or a QR code. As a protection against unauthorized access, the second factor requested is the date of birth of the person for whom the data is stored. With the access code, the medical data is available for the duration agreed with the customer and is then automatically deleted. If you wish to keep the data longer, you can download it and store it locally. If you wish to have the data deleted immediately, the issuing facility can immediately deactivate the access code and delete the associated content.

Information on the processing of personal data

In order to access medical data through this website (https://api.healthdataspace.de/hdscode2/), we process personal data of HealthDataSpace users.
When access codes are used, in addition to the encrypted user data and the patient's date of birth, only usage data, meta data and communication data are stored on the basis of our legitimate interests in making this service available efficiently and securely pursuant to Art. 6 (1) lit. f DSGVO in conjunction with Art. Art. 28 DSGVO.

Types of processing

- Inventory data (access codes, date of birth)
- Usage data (e.g. websites visited, access times, file names, amount of data transferred, access status)
- Meta/communication data (e.g. device/browser information, shortened IP addresses, language settings)

Based on our legitimate interests within the meaning of Art. 6 para. 1 lit. f. DSGVO, we collect data about each access to the server on which this service is located (so-called server log files). The access data includes the name of the website accessed, file, date and time of access, amount of data transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page), shortened IP address and the requesting provider.

Log file information is stored for security reasons (e.g. for the clarification of abuse or fraud) for a maximum period of 2 months and then deleted. Data whose further storage is required for evidentiary purposes is exempt from deletion until final clarification of the respective incident.

Content data (e.g. radiological images and/or reports, etc.) are not processed by Telepaxx Medical Data GmbH or Digithurst Bildverarbeitungssysteme GmbH & Co. KG as the responsible party, but processed on behalf of the respective customer as an order processor.
When using HDS with the standard viewer (not certified for diagnostic reporting), this data is processed exclusively in encrypted form.
When the teamVIEW web software, which is certified for diagnostic reporting, is used by licensed physicians who continue treatment (licenses are issued by the customer), data is temporarily processed in decrypted form for the duration of a viewing session. All unencrypted data will be deleted at the end of the viewing session.

Purpose of processing

- Provision of the HealthDataSpace service, its functions and content
- Security measures

How your data is protected

Reasonable measures are taken to ensure the protection of your data at HealthDataSpace. When access codes are used, no personal data other than the date of birth is required or

collected. To prevent misuse by third parties, we use an encryption process. Thus, the information you provide is transmitted in encrypted form using the SSL protocol (Secure Socket Layer) and checked for authenticity. You can recognize this by the fact that a lock or key is displayed as an icon in the status bar of your browser and the address line begins with "https://...".

Patient data resides in HealthDataSpace in encrypted form. The encryption of the data takes place at the medical facility (physician’s practice / clinic). There, all images and reports are encrypted with a random key. In addition, a private and a public key pair is generated for each patient. The random key is encrypted with the public key of the patient's target account and uploaded to the cloud. The associated Private Key is encrypted with a 12-digit randomly generated cryptographic key. This is handed over to you by the medical facility.
The technical and organizational data protection measures taken are contractually documented and regularly monitored.

How to optimally protect your data

Take technical and organizational data protection measures when using HealthDataSpace. When using access codes, ensure that they are not accessible to unauthorized persons. Never write down the patient's date of birth, which serves as a second factor, on or in connection with the access code. Do not transmit personal data unencrypted over the Internet. This also applies to the transfer of data by e-mail. If you use mobile data carriers (USB sticks, portable storage media, laptops, smartphones, tablets or similar), use encryption mechanisms of the hard disks and comply with data protection and security regulations. Keep your access code in a specially protected place.

Information on the rights of affected Persons

Right of providing information

You have the right to request confirmation as to whether data in question is being processed and to be informed about this data, as well as to receive further information and a copy of the data in accordance with Art. 15 DSGVO. Since the data is stored completely encrypted and without personal reference , this information cannot be provided on the basis of personal data, but exclusively on the basis of access codes, if these are used. In accordance with Art. 17 DSGVO, you have the right to demand the immediate deletion of the data stored for an access code. A change or addition to the data is not possible due to the encryption. You can download the stored data as required by Art. 20 DSGVO and also transfer it to other responsible parties

by disclosing the access code. You also have the right, pursuant to Art. 77 DSGVO, to lodge a complaint with the competent supervisory authority.

Right of withdrawal and right to object

You have the right to revoke given consents pursuant to Art. 7 (3) DSGVO with effect for the future. You may object to the future processing of data concerning you in accordance with Art. 21 DSGVO at any time. The objection can be made in particular against processing for direct marketing purposes. To do so, please contact the institution from which you received the access code. The latter can deactivate it immediately and delete the data it contains. Data is deleted from HealthDataSpace after a retention period. The duration of the retention period or time until the deletion of data is determined by the customer.
To exercise your rights, you can contact us using the contact information provided in the section Information about the responsible person.

Legal basis of data processing

In accordance with Art. 13 DSGVO, we inform you about the legal basis of our data processing activities. If the legal basis is not mentioned in the privacy policy, the following applies: The legal basis for obtaining consent is Art. 6(1)(a) and Art. 7 DSGVO, the legal basis for processing to fulfill our services and carry out contractual measures and respond to inquiries is Art. 6(1)(b) DSGVO, the legal basis for processing to fulfill our legal obligations is Art. 6(1)(c) DSGVO, and the legal basis for processing to protect our legitimate interests is Art. 6(1)(f) DSGVO. In the event that vital interests of the data subject or another natural person make processing of personal data necessary, Art. 6 (1) lit. d DSGVO serves as the legal basis.

Information about the responsible person

For information, requests or suggestions on the subject of data protection, please contact our data protection officer at:
HealthDataSpace Data Protection Officer
Wasserrunzel 5 91186 Büchenbach
Germany
datenschutz@healthdataspace.de

+49 (0)9171 96 71-0

This data protection information has the status 01.01.2023.