HealthDataSpace Privacy Policy

We are pleased to welcome you to our website https://app.healthdataspace.de
This web portal is the home of HealthDataSpace (HDS), a safe health network for physicians and patients. HealthDataSpace is a joint offer by Telepaxx Medical Archiving GmbH (General Manager: Andreas Dobler) and Digithurst Bildverarbeitungssysteme GmbH & Co. KG (General Manager: Rainer Kasan).

We want you to feel safe and comfortable here. The protection of your privacy is very important to us. In the following we would therefore like to inform you to what extent personal data is processed when you access this website. Further information on data protection within the HealthDataSpace service can be found in the second part of this document.

Registration with HealthDataSpace

To register for HealthDataSpace for the first time, you must enter your email address in the registration form and select the type of account required (patient account, physician account, physician's medical staff account). We need this information to send you the information you need to activate your account. Your e-mail address is also your user name. Furthermore, the email address is used to inform you about changes to your HealthDataSpace. You can register either as a patient, as a physician or as medical staff.

If you register as a ***patient***, we will also record your date of birth and gender to uniquely identify your patient information and account as well as to avoid mix-ups.

If you register as a ***physician***, we also record your first and last name, the name of your institution, as well as the postal address and the country in which the institution has its registered office. On the one hand, this information is used to uniquely assign the physician account and to avoid confusion. On the other hand, the information is used for the correct display within HealthDataSpace for the participating members.

If you register as ***medical staff*** of a doctor participating in HealthDataSpace, we record your first and last name as well as the name of your institution, the postal address and the country in which the institution has its registered office. This information is used to uniquely assign the personnel account and to avoid mix-ups. On the other hand, the information is used for correct identification within HealthDataSpace for the participating members.

After filling in all fields and pressing the button "Request account" a pop-up with a PDF opens. It contains the so-called "HealthDataSpace Pass". Your user name and activation code are listed here. The HealthDataSpace passport must not be lost, so keep it safe. You cannot complete registration without the activation code.

As soon as you have clicked the "close" button, the PDF will be closed and an activation request will automatically be sent to the email address you have provided with further information and a confirmation link. If you click on the link marked in this e-mail, you will be redirected to your HealthDataSpace account. Here you will find the General Terms and Conditions (also "License Agreement"), which you must accept for further use by clicking on the empty box. You must also enter the activation code from the HealthDataSpace passport and a new password that you have assigned.

If you then click on the "Activate account" button, you will be activated to use the HealthDataSpace and receive further information by email.

Users can be informed by email about information relevant to offers or registration, such as changes to the scope of offers or technical circumstances. If users have terminated their user account, their data will be deleted with regard to the user account, subject to its storage is necessary for commercial or tax reasons according to Art. 6 Para. 1 lit. c GDPR. It is up to the users to save their data before the end of the contract if they have given notice of termination. We are entitled to irretrievably delete all user data stored during the term of the contract.

Login as a registered user of HealthDataSpace

If the registration was successful, you can log in with your user name and password. We use this data for the registration process and for the audit-proof verification of the authorization to use the account.

Using HealthDataSpace

After logging in, you can view cases, retrieve messages, manage approvals and assignments, view and manage your profile with the associated data (e.g. change the email address), view downloads, view information on HealthDataSpace or log out again in your HDS account. Further information on data protection within the HealthDataSpace service can be found in the second part of this document.

Legal basis of data processing

In accordance with Art. 13 GDPR, we inform you of the legal basis of our data processing. If the legal basis is not mentioned in the data protection declaration, the following applies: The legal basis for obtaining consents is Art. 6 para. 1 lit. a and Art. 7 GDPR, the legal basis for processing for the performance of our services and performance of contractual measures as well as for answering inquiries is Art. 6 para. 1 lit. b GDPR, the legal basis for processing to fulfil our legal obligations is Art. 6 para. 1 lit. c GDPR, and the legal basis for processing to protect our legitimate interests is Art. 6 para. 1 lit. f GDPR. In the event that the vital interests of the data subject or another natural person require the processing of personal data, Article 6(1)(d) GDPR serves as the legal basis.

SSL encryption

In order to protect personal data that you enter on our website (e.g. during registration or login) from unwanted access as comprehensively as possible and to prevent misuse by third parties, we use an encryption procedure. The information you enter is transmitted in encrypted form using SSL protocol (Secure Socket Layer) and checked authentically. 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://...".

Cookies

On our websites we use so-called cookies, i.e. small files that are stored on a visitor's hard drive and contain data such as personal page settings and login information. In our case, temporary cookies are used to ensure that our website is displayed correctly on your respective terminal and that the page loading times are optimal. You can adjust your browser settings so that you are informed about the use of cookies.

On the login page for our HealthDataSpace https://app.healthdataspace.de service we use a so-called session cookie. If you call up images and findings from your HealthDataSpace account in your Internet browser, they are retrieved from our server in the Telepaxx data center. Your medical data is stored there in encrypted form. During the registration process, our server receives your user name and password and sends your browser a so-called session ID in the form of a cookie (here: JSESSIONID). Now the server remembers which session ID belongs to which user. The browser automatically sends your cookie to the server with every request. This saves a lot of time, but is just as safe as the process of checking the user name and the multiple encrypted password again for each request.

Hosting and collecting access data and log files

HealthDataSpace is hosted in the data center in Germany by Telepaxx Medical Archiving GmbH. We process inventory data, contact data, contract data, usage data, meta and communication data of users registered with HealthDataSpace (patients, doctors and medical personnel) on the basis of our legitimate interests in an efficient and secure provision of this service in accordance with Art. 6 Para. 1 lit. f GDPR in conjunction with. Art. 28 GDPR.

We collect data on the basis of our legitimate interests within the meaning of Art. 6 para. 1 lit. f. GDPR data on each access to the server on which this service is located (so-called server log files). Access data includes the name of the accessed website, file, date and time of access, transferred data volume, 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 a maximum of 2 months for security reasons (e.g. to investigate misuse or fraud) and then deleted. Data whose further storage is required

for evidentiary purposes are excluded from deletion until the respective incident has been finally clarified.

Types of user data processed

- Inventory data (e.g. names, addresses, date of birth, gender)
- Contact details (e.g. email address)
- usage data (e.g. visited websites, access times, file names, transferred data volume, access status)
- Meta/communication data(e.g. device/browser information, shortened IP addresses, language settings)
- Contract data (for example, customer category, term)

Content data (e.g. radiological images, findings, medication plans, etc.) are stored and processed in encrypted form only. This means that HealthDataSpace cannot access any content data.

Purpose of processing

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

Rights of data subjects

You have the right to request confirmation as to whether the data concerned are being processed and to request information about these data as well as further information and a copy of the data in accordance with Art. 15 GDPR. They have correspondingly. In accordance with Article 16 of the GDPR, you have the right to request the completion of data concerning you or the correction of inaccurate data concerning you. In accordance with Art. 17 GDPR, you have the right to demand that relevant data be deleted immediately or, alternatively, to demand a restriction on the processing of the data in accordance with Art. 18 GDPR. You have the right to request that the data concerning you that you have provided to us be received in accordance with Art. 20 GDPR and to request its transmission to other persons responsible. In accordance with Art. 77 GDPR, they also have the right to file a complaint with the competent supervisory authority.

Right of revocation and right of objection

You have the right to revoke consents granted pursuant to Art. 7 para. 3 GDPR with effect for the future You can object to the future processing of the data concerning you in accordance with Art. 21 GDPR at any time. The objection may be lodged in particular against processing for direct marketing purposes.

Duration of storage or deletion of data

The data processed by us will be deleted or their processing restricted in accordance with Articles 17 and 18 GDPR. Unless expressly stated in this data protection declaration, the data stored with us will be deleted as soon as the registered user deletes his user account, the data is no longer required for its intended purpose and there are no legal storage obligations to prevent deletion. If the data are not deleted because they are necessary for other and legally permissible purposes, their processing is restricted. This means that the data is blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax reasons.

Order processing in the webshop and customer account

We process the data of our customers in the context of the order processes in our online shop to enable them to select and order the selected products and services, as well as their payment and delivery, or execution.

The data processed includes inventory data, communication data, contract data, payment data and the persons concerned, our customers, interested parties and other business partners. The processing takes place for the purpose of providing contractual services in the context of operating an online shop, billing, delivery and customer services. We use session cookies for storing the contents of the shopping cart and permanent cookies for storing the login status.

Processing is carried out on the basis of Art. 6 Para. 1 lit. b (execution of order processes) and c (legally required archiving) GDPR. The information marked as necessary is required to establish and fulfil the contract. We disclose the data to third parties only within the framework of delivery, payment or within the framework of legal permits and obligations to legal advisors and authorities. The data will only be processed in third countries if this is necessary for the fulfilment of the contract (e.g. at the customer's request upon delivery or payment).

Users can optionally create a user account, in particular by viewing their orders. During the registration process, the required information will be communicated to the users. The user accounts are not public and cannot be indexed by search engines. If users have terminated their user account, their data will be deleted with regard to the user account, subject to its storage is necessary for commercial or tax reasons according to Art. 6 Para. 1 lit. c GDPR. Data in the customer account remain up to its deletion with subsequent archiving in the case of a legal obligation. It is up to the users to save their data before the end of the contract if they have given notice of termination.

When registering, re-registering and using our online services, we store the shortened IP address and the time of the respective user action. The data is stored on the basis of our legitimate interests as well as the user's protection against misuse and other unauthorized use. A passing on of this data to third parties does not take place in

principle, unless it is necessary for the pursuit of our claims or there is a legal obligation according to Art. 6 Abs. 1 lit. c GDPR.

The deletion takes place after the expiry of statutory warranty and comparable obligations, the necessity of data storage is reviewed every three years; in the case of statutory archiving obligations, the deletion takes place after their expiry (end of commercial law (6 years) and tax law (10 years) storage obligation).

Payment in the webshop with PayPal

If you decide to pay with the online payment service PayPal as part of your order process, your contact details will be transmitted to PayPal as part of the order triggered in this way. PayPal is an offer of PayPal (Europe) S.à.r.l. & Cie. S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg. PayPal acts as an online payment service provider and trustee and offers buyer protection services.

The personal data transmitted to PayPal is usually first name, last name, address, telephone number, IP address, email address, or other data required for order processing, as well as data related to the order, such as number of items, article number, invoice amount and taxes in percent, invoice information, etc.

This transfer is necessary to process your order using the payment method you have selected, in particular to confirm your identity, to administer your payment and the customer relationship. Please note, however, that PayPal may also pass on personal data to service providers, subcontractors or other affiliated companies if this is necessary to fulfil the contractual obligations arising from your order or if the personal data is to be processed on behalf of PayPal.

Depending on the payment method selected via PayPal, e.g. invoice or direct debit, the personal data transmitted to PayPal is transmitted by PayPal to credit agencies. This transfer serves to verify your identity and creditworthiness with regard to the order you have placed. You can find out which credit agencies are involved and which data are generally collected, processed, stored and passed on by PayPal in the PayPal data protection declaration at https://www.paypal.com/de/webapps/mpp/ua/privacy-full

Questions and suggestions

You have the option of requesting information about what data about you is stored by us and for what purpose it is stored. In addition, you may have incorrect data corrected or data deleted that is inadmissible or no longer necessary to be stored. Your data will only be stored by us for as long as this is prescribed by legal retention periods. 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
Deutschland
datenschutz@healthdataspace.de
+49 (0)9171 96 71-0

Hints for the HealthDataSpace Privacy Policy

Below we have compiled information on data protection for you, which you should observe when using the HealthDataSpace (HDS) in the versions HDS PRO for doctors and HDS basic version for patients.

Information for physicians and medical staff

Data protection responsible body

As the treating physician, you or your organization are responsible for compliance with data protection regulations when using HealthDataSpace in accordance with the General Data Protection Regulation (GDPR) or the regulations relevant to your organization. Digithurst Bildverarbeitungssysteme GmbH & Co. KG acts as an order data processor for you and uses a computer centre of Telepaxx Medical Archiving GmbH in Büchenbach, Germany. Further details are regulated by a contract for order data processing.

HealthDataSpace is set up so that it can be used in compliance with the General Data Protection Regulation (GDPR). Before processing your data, please check whether the data of your patients and employees may be processed in compliance with the relevant data protection regulations and follow the standard procedures in dealing with HealthDataSpace. This is the only way we can guarantee optimum data protection. If in doubt, contact your data protection officer or the responsible supervisory authority.

Personal and special personal data

Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person. Specific types of personal data include information about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life. Patient data are therefore special personal data.

Admissibility of data processing

Processing is only permitted if it is based on the informed, voluntary, revocable and verifiable consent of the data subject or if it can be based on a legal basis. The latter can be e.g. a treatment contract or the perception of vital interests of the affected person.

The processing of patient data in the HDS is based on the voluntary provision of the data by the patient himself and is thus based on the treatment contract. Patient data may also be passed on to other doctors as part of further treatment. However, if data are passed on to non-treating persons, the patient's consent and release from confidentiality are required. Please note that access by unauthorized persons may result in a disclosure relevant under criminal law for the attending physician, if no release from the duty of confidentiality exists. Please use the sample common in your organisation for these very individual cases.

Since we do not have access to patient data due to the encryption of the data, we are not able to provide support for patient data. Outside the HealthDataSpace we offer you general FAQs for frequent questions and answers, e.g. about your account login or the use of the upload or download functions.

HDS PRO also stores and processes master and contact data (first and last name, name of the institution, address, email address) of doctors and medical staff. Their processing is based on the respective employment relationship or takes place in the legitimate interest of your organization, whereby you must, however, check for each individual case whether this is contrary to interests worthy of protection or company regulations (e.g. works agreements). You can also upload a photo to your profile. When creating photos, please make sure that they are not uploaded unwantedly to other cloud services.

In this context, we would like to point out that we also process so-called secondary data on your behalf when using the HDS. These include usage data or log protocols that we need to monitor the security of our IT systems in compliance with legal regulations.

Data avoidance and data economy

Data processing within the HDS must be based on the principles of data economy and data avoidance. Thereafter, as little personal data as necessary and only as much as necessary is to be processed. For the filling of free text fields, please establish principles for your employees that guarantee data protection-compliant handling in this sense and provide that free text fields are only filled with treatment-related data.

Appropriation and transparency

In principle, personal data may only be processed for a specific purpose, i.e. the purpose of the data processing must already have been determined before the initial recording.

If you transfer patient data within HDS to other locations, the system automatically informs the patient participating in HDS. This enables the patient to withdraw the link to his health data released by him at any time.

Please note that the patient must also be informed if you wish to pass on patient data to other locations outside the HDS. For the transfer outside the treatment relationship, which are no longer covered by the intended use of the HDS, consent and release from medical confidentiality are necessary. Please use the sample common in your organisation for these very individual cases.

Anonymization and pseudonymization of data

It is recommended to make use of pseudonymization or anonymization wherever possible. An anonymization occurs when all identifying characteristics have been removed from a data record and an assignment to a person is therefore impossible. Pseudonymization means that personal information is replaced by new, non-personal identifiers. Usually it is still possible to concatenate the individual data records and under certain circumstances a personal reference can still be established.

Deleting and locking

Please note that different storage periods apply with regard to the storage of personal data. According to § 10 of the Model Occupational Code for Physicians, patient data is generally stored for a period of 10 years, which refers to the physician information system you have used ("AIS" for short). The data within the HDS PRO only represent copies of the data from your AIS for which these retention periods do not apply. The data must therefore be deleted from HDS without delay as soon as the purpose of its collection has ceased to exist.

Rights of the parties concerned

Please note that the persons affected by data processing via the HDS may have different rights. In principle, this includes rights to information, notification and information, the right to correction, deletion, blocking or the right to revoke permission for data processing. Please also note the special information obligations of the German Civil Code (BGB) and the Patient Rights Act that may apply to your position.

Technical-organizational data protection measures

We take appropriate measures to ensure the protection of your data and that of your patients with us. For example, the login process at the HDS web portal is SSL encrypted and thus protected against unauthorized reading out of the access data. Patient data is available in HDS and your HDS PRO application in encrypted form so that only you and the patient can decrypt this data. All data is located in a secure data center in Germany. The technical-organizational data protection measures taken there are documented in the contract for order data processing and are regularly checked.

Please also take technical and organisational measures for the data protection in handling HDS: Define which employees are authorized for which processes on the system. Check compliance with the authorization concept regularly. Do not pass on

any data to unauthorized persons. If you use external service providers for data processing or maintenance and care of IT, check these regularly and in writing for compliance with data protection. Make sure that your user account is only used by you and that the password is not used elsewhere. In particular, never use the same password that you use to access other systems.

In addition, some Internet browsers offer the option of storing passwords, even without consultation. These functions for storing passwords in the browser cache must not be used! Do not transmit unencrypted personal data over the Internet. This also applies to the transmission of data by e-mail. If you use mobile data carriers (USB sticks, portable storage media, laptops, smartphones, tablets, etc.), use encryption mechanisms on the hard drives and comply with data protection and security regulations. It should also be noted that the system keys for decrypting patient data are not stored in the HDS. Therefore, keep the copy of your individual activation code in a specially protected location, e.g. a fireproof safe or an outsourced location. Obligate and inform your employees on the observance of data protection.

Please note that under German data protection law there is an obligation to appoint a company or official data protection officer, who may have to assess the application of HDS PRO for your organization in advance within the framework of a so-called prior data protection check. Please consult your data protection officer in good time. Furthermore, it is generally required under data protection law to list the HDS PRO in a legally prescribed index of procedures and to document data processing. The instructions for use and this document will provide you with essential information on this. If in doubt, contact your organization's data protection officer. The authors of this document will be happy to provide you with further information.

Information for patients

The HealthDataSpace for patients is an offer of Telepaxx Medical Archiving GmbH. HealthDataSpace is set up so that it can be used in compliance with the General Data Protection Regulation (GDPR). Please follow the standard procedures for handling the HDS. This is the only way we can guarantee optimum data protection.

Your rights as a data subject

You decide yourself about your patient data in the HDS, i.e. it is up to you to upload data there, to process it, to share it with others or to remove the authorizations again and to delete data. You will also be automatically informed by the system if a person who has received your link to your data wishes to share it with others. You can also terminate the HDS usage agreement in compliance with the General Terms of Use and we will delete the account and all data in it in this case. After deletion, you will no longer be able to access your data.

Since we do not have access to your patient data due to the encryption of the data, we are not able to provide support for your patient data. Outside the HealthDataSpace we offer you general FAQs for frequent questions and answers, e.g. about your account login or the use of upload or download functions.

If you provide data to a doctor or another person via HDS, he is responsible for data processing and compliance with your rights. Data that we require for registration and registration and, if necessary, for billing the paid version of the HDS, are processed by us in compliance with the provisions of the data protection laws. We store this usage data in compliance with the legal retention periods and delete it completely after its expiry. We will be happy to provide you with information about the data processed about you.

How we protect your data

We take appropriate measures to ensure the protection of your data with us. Your data in the HealthDataSpace will be processed in a secure data center of Telepaxx Medical Archiving GmbH in Büchenbach. For example, the login process at the HDS web portal is SSL encrypted and thus protected against unauthorized reading out of the access data. Patient data is available in HDS in encrypted form so that only you and the person with whom you want to share the data can decrypt your data. All data is located in a secure data center in Germany. The technical and organizational data protection measures taken there are contractually documented and are regularly checked.

How to protect your data optimally

Please also take technical and organisational measures for the
HDS Privacy: Make sure that your user account is only used by you and that your password is not used elsewhere. In particular, never use the same password that you use to access other systems.

In addition, some Internet browsers offer the option of storing passwords, even without consultation. These functions for storing passwords in the browser cache must not be used!

Do not transmit unencrypted personal data over the Internet. This also applies to the transmission of data by email. If you use mobile data carriers (USB sticks, portable storage media, laptops, smartphones, tablets, etc.), use encryption mechanisms on the hard drives and comply with data protection and security regulations. It should also be noted that the system keys for decrypting patient data are not stored in the HDS. Therefore, keep the copy of your individual activation code in a specially protected location, e.g. a fireproof safe or an outsourced location.