

# HealthDataSpace Connect Connect Privacy Policy

We are pleased to welcome you to our website <https://hdsc.HealthDataSpaceConnect.de>

This web portal is the home of HealthDataSpace Connect, a safe health network for physicians and patients. HealthDataSpace Connect is an offer by Digithurst Bildverarbeitungssysteme GmbH & Co.

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 Connect can be found in the second part of this document.

## Registration with HealthDataSpace Connect Connect

To register for HealthDataSpace Connect 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). 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 Connect. You can register either as a patient or as a physician.

To avoid confusion and to enable correct and clear identification of accounts within HealthDataSpace Connect, we record your first and last name, your date of birth and your gender.

If you register as a medical doctor, we also record the name of your institution, the postal address and the country in which the institution is based. Other information, such as the personal role of a physician account, is used for correct presentation within HealthDataSpace Connect.

After completing all the fields and clicking the "Create Account" button, you will receive an activation link via the e-mail address you provided. If you click on the link in this e-mail, your account will be activated. You will now be redirected to the login page and can log into your account using your e-mail address and the password you have entered.

After logging in, your HealthDataSpace Connect Pass will be displayed. This contains a recovery code that can be used to reset your password in case you forget it. We recommend that you keep the recovery code in a safe place. Without the recovery code, your account data cannot be restored if you forget your password.

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 Connect**

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 Connect**

After logging in, you can view, import, share, upload and download data in your HDS account, view and manage your profile with the associated data (e.g. change your e-mail address), view information about HealthDataSpace Connect or log out again. Further information on data protection in the context of the HealthDataSpace Connect 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 Connect service [hdsc.healthdataspace.de](https://hdsc.healthdataspace.de) we use a so-called session cookie. If you call up images and findings from your HealthDataSpace Connect account in your Internet browser, they are retrieved from our cloud storage. 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 Connect is hosted in data centers in Germany by Hetzner Online GmbH. We process inventory data, contact data, contract data, usage data, meta and communication data of users registered with HealthDataSpace Connect (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 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 Connect 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.

### **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:

Digithurst Bildverarbeitungssysteme GmbH & Co. KG  
Data Protection Officer  
Wasserrunzel 5  
91186 Büchenbach  
Deutschland  
datenschutz@HealthDataSpace.de  
+49 (0)9171 96 71-0

## **Some Advice about Data Privacy at HealthDataSpace Connect**

Below we have compiled information on data protection for you, which you should observe when using the HealthDataSpace Connect.

### **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 Connect in accordance with the EU 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 data centers in Germany. Further details are regulated by a contract for order data processing.

HealthDataSpace Connect is set up so that it can be used in compliance with the EU 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 Connect. This is the only way to guarantee the best data protection possible. 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 HealthDataSpace Connect 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 encryption, we are not able to provide support for patient data. However, outside of HealthDataSpace Connect we offer some general FAQs for frequent questions and answers, e.g. about your account login or the use of the upload or download functions.

HealthDataSpace Connect also stores and processes meta and contact data (first and last name, name of the institution, address, email address) of physicians 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 HealthDataSpace Connect. 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 HealthDataSpace Connect 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.

Please note that the patient must be informed if you wish to pass on patient data to other locations outside the HealthdataSpace Connect. 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 HealthDataSpace Connect only represent copies of the data from your AIS for which these retention periods do not apply. The data must therefore be deleted from HealthDataSpace Connect 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 HealthDataSpace Connect 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 is SSL encrypted and thus protected against unauthorized access. Patient data is available 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 HealthDataSpace Connect: 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 HealthDataSpace Connect. 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 HealthDataSpace Connect 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 HealthDataSpace Connect 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**



HealthDataSpace Connect is set up for you to be used in compliance with the EU General Data Protection Regulation (GDPR). Please follow the standard procedures for handling HealthDataSpace Connect. This is the only way to guarantee the best data protection.

### **Your rights as a data subject**

You decide yourself about your patient data in HealthDataSpace Connect. Hence, it is up to you to upload data there, to process it, to share it with others and to delete data. You can also cancel your user agreement with HealthDataSpace Connect any time. In this case we will delete your user account and all existing data. After deletion you will no longer be able to access your account or your medical data.

Since we cannot access your patient data due to encryption, we are not able to provide support for your patient data. Outside the HealthDataSpace Connect we offer you general FAQs for frequent questions and answers, e.g. about your account login or the use of upload or download functions: <https://healthdataspace.org/faq-patienten/>

If you share your medical data with physicians or any other people via HealthDataSpace Connect, these people are responsible for data processing and compliance with your rights. Data that we require for registration and for billing is processed by us in compliance with the provisions of the data protection laws. We store all personal and medical data in compliance with the legal retention periods and delete it completely after its expiration date. 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 HealthDataSpace Connect will be processed in a secure data center in Germany. The login process is SSL encrypted and thus protected against unauthorized access. Patient data is available in HealthDataSpace Connect in encrypted form only. Hence, only you and the people with whom you share your medical data can decrypt it. All data is located in a secure data center in Germany. The technical and organizational data protection measures taken there are contractually documented and being regularly checked.

### **How to protect your data the best way**

Please be aware to take technical and organisational measures to protect your personal and medical data in HealthDataSpace Connect: Make sure that your user account is only used by you and that your password is not used elsewhere.

Please ensure to avoid that your internet browser saves your passwords in its cache automatically.

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 hard drives and comply with data protection and security regulations. Please be also aware, that the system keys for decrypting patient data are not saved in HealthDataSpace Connect. Therefore, keep the copy of your individual recovery code in a particularly protected location, e.g. a fireproof safe or an outsourced location.