

HealthDataSpace Datenschutzerklärung

Wir freuen uns über Ihren Besuch auf <https://app.healthdataspace.de>. Dieses Webportal ist die Startseite von HealthDataSpace (HDS), einem sicheren Gesundheitsnetzwerk für Ärzte und Patienten. HealthDataSpace ist ein gemeinsames Angebot der Telepaxx Medical Archiving GmbH (Geschäftsführer: Andreas Dobler) und der Digithurst Bildverarbeitungssysteme GmbH & Co. KG (Geschäftsführer: Rainer Kasan).

Wir möchten, dass Sie sich hier sicher und wohl fühlen. Der Schutz Ihrer Privatsphäre hat für uns einen hohen Stellenwert. Im Folgenden möchten wir Sie daher darüber informieren, in welchem Umfang personenbezogene Daten beim Aufruf dieser Webseite verarbeitet werden. Weiterführende Hinweise zum Datenschutz im Rahmen des Dienstes HealthDataSpace finden Sie im zweiten Teil dieses Dokumentes.

Registrierung bei HealthDataSpace

Für die erstmalige Registrierung zum HealthDataSpace müssen Sie im Registrierungsformular Ihre E-Mail-Adresse eingeben und die Art des gewünschten Kontos auswählen (Patienten-Konto, Arzt-Konto, Konto für medizinisches Personal des Arztes). Diese Daten benötigen wir, um Ihnen die Informationen für die Aktivierung des Kontos zuzuschicken. Ihre E-Mail-Adresse ist zugleich der Benutzername. Ferner wird die E-Mail-Adresse genutzt, um Sie über Änderungen Ihres HealthDataSpace zu informieren. Sie können sich wahlweise als Patient, als Arzt oder als medizinisches Personal registrieren.

Falls Sie sich als **Patient** registrieren, erfassen wir außerdem Ihr Geburtsdatum und Ihr Geschlecht, um Ihre Patientendaten und Ihr Konto eindeutig zuweisen zu können und um Verwechslungen zu vermeiden.

Falls Sie sich als **Arzt** registrieren, erfassen wir auch Ihren Vor- und Nachnamen, den Namen Ihrer Institution, die Postanschrift und das Land des Sitzes der Institution. Diese Angaben dienen einerseits der eindeutigen Zuweisung des Arzt-Kontos und sollen Verwechslungen ausschließen, andererseits dienen die Angaben der korrekten Identifizierung innerhalb von HealthDataSpace für die teilnehmenden Ärzte und Patienten.

Falls Sie sich als **medizinisches Personal** eines am HealthDataSpace teilnehmenden Arztes registrieren, erfassen wir Ihren Vor- und Nachnamen sowie die Ihnen zugewiesene Rolle, also Ihre Funktion im HealthDataSpace. Ferner werden der Name Ihrer Institution, die Postanschrift und das Land des

Sitzes der Institution erfasst. Diese Angaben dienen einerseits der eindeutigen Zuweisung des Personal-Kontos und sollen Verwechslungen ausschließen, andererseits dienen die Angaben der korrekten Darstellung innerhalb des HealthDataSpace für die teilnehmenden Patienten.

Nach Ausfüllen aller Felder und Betätigen des Buttons „Konto anfordern“ öffnet sich ein Pop-Up mit einem PDF. Darin ist der sogenannte „HealthDataSpace-Pass“ abgebildet. Hierin werden Ihr Benutzername sowie der Aktivierungscode aufgeführt. Der „HealthDataSpace-Pass“ darf nicht verloren gehen, bewahren Sie ihn daher gut auf. Ohne den Aktivierungscode können Sie die Registrierung nicht abschließen.

Sobald Sie den Button „schließen“ angeklickt haben, wird das PDF geschlossen und automatisch eine Aktivierungsanfrage an die von Ihnen angegebene E-Mail-Adresse mit weiteren Hinweisen und einem Bestätigungs-Link verschickt. Wenn Sie in dieser E-Mail den gekennzeichneten Link anklicken, werden Sie in Ihr HealthDataSpace-Konto weitergeleitet. Hier erhalten Sie die Allgemeinen Vertragsbedingungen (auch „Lizenzvereinbarung“), die Sie für die weitere Nutzung per Klick auf das leere Kästchen akzeptieren müssen. Hier müssen zudem der Aktivierungscode aus dem „HealthDataSpace-Pass“ eingegeben werden, sowie ein neues, von Ihnen vergebenes Passwort.

Wenn Sie anschließend den Button „Konto aktivieren“ anklicken, sind Sie für die Nutzung des HealthDataSpace freigeschaltet und erhalten weitere Informationen per E-Mail.

Als Nutzer können Sie über angebots- oder registrierungsrelevante Informationen, wie Änderungen des Angebotsumfangs oder technische Umstände per E-Mail informiert werden. Wenn Sie ihr Nutzerkonto gekündigt haben, werden deren Daten im Hinblick auf das Nutzerkonto gelöscht, vorbehaltlich deren Aufbewahrung ist aus handels- oder steuerrechtlichen Gründen entspr. Art. 6 Abs. 1 lit. c DSGVO notwendig. Es obliegt den Nutzern, ihre Daten bei erfolgter Kündigung vor dem Vertragsende zu sichern. Wir sind berechtigt, sämtliche während der Vertragsdauer gespeicherten Daten des Nutzers unwiederbringlich zu löschen.

Anmeldung als registrierter Nutzer bei HealthDataSpace

Sofern die Registrierung erfolgreich war, können Sie sich mit Benutzername und Passwort anmelden. Diese Daten verwenden wir für den Anmeldeprozess und für die revisionssichere Überprüfung der Berechtigung zur Nutzung des Kontos.

Nutzung von HealthDataSpace

Nach der Anmeldung können Sie in Ihrem HDS-Konto u.a. Fälle einsehen, Nachrichten abrufen, Freigaben und Zuordnungen verwalten, ihr Profil mit den dazugehörigen Daten einsehen und verwalten (z.B. ändern der E-Mail-Adresse), Downloads einsehen, Informationen zum HealthDataSpace einsehen oder sich wieder abmelden. Weiterführende Hinweise zum Datenschutz im Rahmen des Dienstes HealthDataSpace finden Sie im zweiten Teil dieses Dokumentes.

Rechtsgrundlage der Datenverarbeitung

Nach Maßgabe des Art. 13 DSGVO teilen wir Ihnen die Rechtsgrundlagen unserer Datenverarbeitungen mit. Sofern die Rechtsgrundlage in der Datenschutzerklärung nicht genannt wird, gilt Folgendes: Die Rechtsgrundlage für die Einholung von Einwilligungen ist Art. 6 Abs. 1 lit. a und Art. 7 DSGVO, die Rechtsgrundlage für die Verarbeitung zur Erfüllung unserer Leistungen und Durchführung vertraglicher Maßnahmen sowie Beantwortung von Anfragen ist Art. 6 Abs. 1 lit. b DSGVO, die Rechtsgrundlage für die Verarbeitung zur Erfüllung unserer rechtlichen Verpflichtungen ist Art. 6 Abs. 1 lit. c DSGVO, und die Rechtsgrundlage für die Verarbeitung zur Wahrung unserer berechtigten Interessen ist Art. 6 Abs. 1 lit. f DSGVO. Für den Fall, dass lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person eine Verarbeitung personenbezogener Daten erforderlich machen, dient Art. 6 Abs. 1 lit. d DSGVO als Rechtsgrundlage.

SSL-Verschlüsselung

Um persönliche Daten, die Sie auf unserer Website eintragen (z.B. bei der Registrierung oder Anmeldung) vor unerwünschten Zugriffen möglichst umfassend zu schützen und einem Missbrauch durch Dritte vorzubeugen, wenden wir ein Verschlüsselungsverfahren an. So werden die von Ihnen angegebenen Informationen in verschlüsselter Form mittels SSL-Protokoll (Secure Socket Layer) übertragen und authentisch geprüft. Sie erkennen dies daran, dass in der Statusleiste Ihres Browsers ein Schloss oder Schlüssel als Symbol angezeigt wird und die Adresszeile beginnt mit "https://..."

Cookies

Auf unseren Websites verwenden wir sogenannte Cookies, also kleine Dateien, die auf der Festplatte eines Besuchers gespeichert werden und Daten enthalten, wie z.B. persönliche Seiteneinstellungen und Anmeldeinformationen. In unserem Fall werden temporäre Cookies genutzt, um zu gewährleisten, dass unsere Website korrekt auf Ihrem jeweiligen Endgerät angezeigt wird und die

Seitenladezeiten optimal sind. Sie können Ihre Browser-Einstellungen so anpassen, dass Sie über die Benutzung von Cookies informiert werden.

Auf der Login-Seite für unseren Service HealthDataSpace <https://app.healthdataspace.de> verwenden wir ein sogenanntes Session-Cookie. Wenn Sie in Ihrem Internetbrowser Bilder und Befunde aus Ihrem HealthDataSpace-Konto aufrufen, werden diese von unserem Server im Telepaxx Rechenzentrum geholt. Dort sind Ihre Medizindaten verschlüsselt abgelegt. Beim Anmeldevorgang nimmt unser Server Ihren Benutzernamen und Ihr Passwort entgegen und übermittelt Ihrem Browser dafür eine sogenannte Session-ID in Form eines Cookies (hier: JSESSIONID). Jetzt merkt sich der Server, welche Session-ID zu welchem Benutzer gehört. Der Browser sendet Ihren Cookie automatisch bei jeder Anfrage mit zum Server. Das spart viel Zeit, ist aber genauso sicher wie der Vorgang, bei jeder Anfrage den Benutzernamen und das mehrfach verschlüsselte Passwort erneut zu überprüfen.

Hosting und Erhebung von Zugriffsdaten und Logfiles

HealthDataSpace wird im Rechenzentrum in Deutschland der Firma Telepaxx Medical Archiving GmbH gehostet. Hierbei verarbeiten wir Bestandsdaten, Kontaktdaten, Vertragsdaten, Nutzungsdaten, Meta- und Kommunikationsdaten von bei HealthDataSpace registrierten Nutzern (Patienten, Ärzte und medizinisches Personal) auf Grundlage unserer berechtigten Interessen an einer effizienten und sicheren Zurverfügungstellung dieses Dienstes gem. Art. 6 Abs. 1 lit. f DSGVO i.V.m. Art. 28 DSGVO.

Wir erheben auf Grundlage unserer berechtigten Interessen im Sinne des Art. 6 Abs. 1 lit. f. DSGVO Daten über jeden Zugriff auf den Server, auf dem sich dieser Dienst befindet (sogenannte Serverlogfiles). Zu den Zugriffsdaten gehören Name der abgerufenen Webseite, Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung über erfolgreichen Abruf, Browsertyp nebst Version, das Betriebssystem des Nutzers, Referrer URL (die zuvor besuchte Seite), verkürzte IP-Adresse und der anfragende Provider.

Logfile-Informationen werden aus Sicherheitsgründen (z.B. zur Aufklärung von Missbrauchs- oder Betrugshandlungen) für die Dauer von maximal 2 Monaten gespeichert und danach gelöscht. Daten, deren weitere Aufbewahrung zu Beweiszwecken erforderlich ist, sind bis zur endgültigen Klärung des jeweiligen Vorfalls von der Löschung ausgenommen.

Arten der verarbeiteten Nutzerdaten

- Bestandsdaten (z.B. Namen, Adressen, Geburtsdatum, Geschlecht)

- Kontaktdaten (z.B. Email-Adresse)
- Nutzungsdaten (z.B. besuchte Webseiten, Zugriffszeiten, Dateinamen, übertragenen Datenmenge, Zugriffsstatus)
- Meta-/Kommunikationsdaten(z.B. Geräte-/Browserinformationen, verkürzte IP-Adressen, Spracheinstellungen)
- Vertragsdaten (z.B. Kundenkategorie, Laufzeit)

Inhaltsdaten (z.B. radiologische Bilder, Befunde, Medikationspläne etc.) werden ausschließlich verschlüsselt gespeichert und verarbeitet. Das heißt: HealthDataSpace kann nicht auf diese Inhaltsdaten zugreifen.

Zweck der Verarbeitung

- Zurverfügungstellung des Dienstes HealthDataSpace, seiner Funktionen und Inhalte
- Sicherheitsmaßnahmen

Rechte der betroffenen Personen

Sie haben das Recht, eine Bestätigung darüber zu verlangen, ob betreffende Daten verarbeitet werden und auf Auskunft über diese Daten sowie auf weitere Informationen und Kopie der Daten entsprechend Art. 15 DSGVO. Sie haben entsprechend Art. 16 DSGVO das Recht, die Vervollständigung der Sie betreffenden Daten oder die Berichtigung der Sie betreffenden unrichtigen Daten zu verlangen. Sie haben nach Maßgabe des Art. 17 DSGVO das Recht zu verlangen, dass betreffende Daten unverzüglich gelöscht werden, bzw. alternativ nach Maßgabe des Art. 18 DSGVO eine Einschränkung der Verarbeitung der Daten zu verlangen. Sie haben das Recht zu verlangen, dass die Sie betreffenden Daten, die Sie uns bereitgestellt haben nach Maßgabe des Art. 20 DSGVO zu erhalten und deren Übermittlung an andere Verantwortliche zu fordern. Sie haben ferner gem. Art. 77 DSGVO das Recht, eine Beschwerde bei der zuständigen Aufsichtsbehörde einzureichen.

Widerrufsrecht und Widerspruchsrecht

Sie haben das Recht, erteilte Einwilligungen gem. Art. 7 Abs. 3 DSGVO mit Wirkung für die Zukunft zu widerrufen. Sie können der künftigen Verarbeitung der Sie betreffenden Daten nach Maßgabe des Art. 21 DSGVO jederzeit widersprechen. Der Widerspruch kann insbesondere gegen die Verarbeitung für Zwecke der Direktwerbung erfolgen.

Dauer der Speicherung bzw. Löschung von Daten

Die von uns verarbeiteten Daten werden nach Maßgabe der Art. 17 und 18 DSGVO gelöscht oder in ihrer Verarbeitung eingeschränkt. Sofern nicht im Rahmen dieser Datenschutzerklärung ausdrücklich angegeben, werden die bei uns gespeicherten Daten gelöscht, sobald der registrierte Nutzer sein Nutzerkonto löscht, die Daten für ihre Zweckbestimmung nicht mehr erforderlich sind und der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Sofern die Daten nicht gelöscht werden, weil sie für andere und gesetzlich zulässige Zwecke erforderlich sind, wird deren Verarbeitung eingeschränkt. D.h. die Daten werden gesperrt und nicht für andere Zwecke verarbeitet. Das gilt z.B. für Daten, die aus handels- oder steuerrechtlichen Gründen aufbewahrt werden müssen.

Bestellabwicklung im Onlineshop und Kundenkonto

Wir verarbeiten die Daten unserer Kunden im Rahmen der Bestellvorgänge in unserem Onlineshop, um ihnen die Auswahl und die Bestellung der gewählten Produkte und Leistungen, sowie deren Bezahlung und Zustellung, bzw. Ausführung zu ermöglichen.

Zu den verarbeiteten Daten gehören Bestandsdaten, Kommunikationsdaten, Vertragsdaten, Zahlungsdaten und zu den betroffenen Personen unsere Kunden, Interessenten und sonstige Geschäftspartner. Die Verarbeitung erfolgt zum Zweck der Erbringung von Vertragsleistungen im Rahmen des Betriebs eines Onlineshops, Abrechnung, Auslieferung und der Kundenservices. Hierbei setzen wir Session Cookies für die Speicherung des Warenkorb-Inhalts und permanente Cookies für die Speicherung des Login-Status ein.

Die Verarbeitung erfolgt auf Grundlage des Art. 6 Abs. 1 lit. b (Durchführung Bestellvorgänge) und c (Gesetzlich erforderliche Archivierung) DSGVO. Dabei sind die als erforderlich gekennzeichneten Angaben zur Begründung und Erfüllung des Vertrages erforderlich. Die Daten offenbaren wir gegenüber Dritten nur im Rahmen der Auslieferung, Zahlung oder im Rahmen der gesetzlichen Erlaubnisse und Pflichten gegenüber Rechtsberatern und Behörden. Die Daten werden in Drittländern nur dann verarbeitet, wenn dies zur Vertragserfüllung erforderlich ist (z.B. auf Kundenwunsch bei Auslieferung oder Zahlung).

Nutzer können optional ein Nutzerkonto anlegen, indem sie insbesondere ihre Bestellungen einsehen können. Im Rahmen der Registrierung, werden die erforderlichen Pflichtangaben den Nutzern mitgeteilt. Die Nutzerkonten sind nicht öffentlich und können von Suchmaschinen nicht indexiert werden. Wenn Nutzer ihr Nutzerkonto gekündigt haben, werden deren Daten im Hinblick auf das Nutzerkonto gelöscht, vorbehaltlich deren Aufbewahrung ist aus handels- oder steuerrechtlichen Gründen entspr. Art. 6 Abs. 1 lit. c DSGVO notwendig. Angaben im Kundenkonto verbleiben bis zu dessen Löschung mit anschließender Archivierung im Fall einer rechtlichen Verpflichtung. Es obliegt den Nutzern, ihre Daten bei erfolgter Kündigung vor dem Vertragsende zu sichern.

Im Rahmen der Registrierung und erneuter Anmeldungen sowie Inanspruchnahme unserer Onlinedienste, speichern wir die gekürzte IP-Adresse und den Zeitpunkt der jeweiligen Nutzerhandlung. Die Speicherung erfolgt auf Grundlage unserer berechtigten Interessen, als auch der Nutzer an Schutz vor Missbrauch und sonstiger unbefugter Nutzung. Eine Weitergabe dieser Daten an Dritte erfolgt grundsätzlich nicht, außer sie ist zur Verfolgung unserer Ansprüche erforderlich oder es besteht hierzu eine gesetzliche Verpflichtung gem. Art. 6 Abs. 1 lit. c DSGVO.

Die Löschung erfolgt nach Ablauf gesetzlicher Gewährleistungs- und vergleichbarer Pflichten, die Erforderlichkeit der Aufbewahrung der Daten wird alle drei Jahre überprüft; im Fall der gesetzlichen Archivierungspflichten erfolgt die Löschung nach deren Ablauf (Ende handelsrechtlicher (6 Jahre) und steuerrechtlicher (10 Jahre) Aufbewahrungspflicht).

Bezahlung im Onlineshop mit PayPal

Sollten Sie sich im Rahmen Ihres Bestellvorgangs für eine Bezahlung mit dem Online-Zahlungsdienstleister PayPal entscheiden, werden im Rahmen der so ausgelösten Bestellung Ihre Kontaktdaten an PayPal übermittelt. PayPal ist ein Angebot der PayPal (Europe) S.à.r.l. & Cie. S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg. PayPal übernimmt dabei die Funktion eines Online-Zahlungsdienstleisters sowie eines Treuhänders und bietet Käuferschutzdienste an.

Bei den an PayPal übermittelten personenbezogenen Daten handelt es sich zumeist um Vorname, Nachname, Adresse, Telefonnummer, IP-Adresse, Email-Adresse, oder andere Daten, die zur Bestellabwicklung erforderlich sind, als auch Daten, die im Zusammenhang mit der Bestellung stehen, wie Anzahl der Artikel, Artikelnummer, Rechnungsbetrag und Steuern in Prozent, Rechnungsinformationen usw.

Diese Übermittlung ist zur Abwicklung Ihrer Bestellung mit der von Ihnen ausgewählten Zahlungsart notwendig, insbesondere zur Bestätigung Ihrer Identität, zur Administration Ihrer Zahlung und der Kundenbeziehung. Bitte beachten Sie jedoch: Personenbezogene Daten können seitens PayPal auch an Leistungserbringer, an Subunternehmer oder andere verbundene Unternehmen weitergegeben werden, soweit dies zur Erfüllung der vertraglichen Verpflichtungen aus Ihrer Bestellung erforderlich ist oder die personenbezogenen Daten im Auftrag verarbeitet werden sollen.

Abhängig von der über PayPal ausgewählten Zahlungsart, z.B. Rechnung oder Lastschrift, werden die an PayPal übermittelten personenbezogenen Daten von PayPal an Wirtschaftsauskunfteien übermittelt. Diese Übermittlung dient der Identitäts- und Bonitätsprüfung in Bezug auf die von Ihnen getätigte Bestellung. Um welche Auskunfteien es sich hierbei handelt und welche Daten von PayPal allgemein erhoben, verarbeitet, gespeichert und weitergegeben werden, entnehmen Sie der Datenschutzerklärung von PayPal unter <https://www.paypal.com/de/webapps/mpp/ua/privacy-full>

Fragen und Anregungen

Sie haben die Möglichkeit, Auskunft darüber zu verlangen, welche Daten über Sie bei uns gespeichert sind und zu welchem Zweck diese Speicherung erfolgt. Darüber hinaus können Sie unrichtige Daten berichtigen oder solche Daten löschen lassen, deren Speicherung unzulässig oder nicht mehr erforderlich ist. Ihre Daten bleiben bei uns nur solange gespeichert, wie dies durch gesetzliche Aufbewahrungsfristen vorgegeben ist. Für Auskünfte, Wünsche oder Anregungen zum Thema Datenschutz steht Ihnen unser Datenschutzbeauftragter gerne zur Verfügung unter:

HealthDataSpace Datenschutzbeauftragter
Wasserrunzel 5
91186 Büchenbach

Deutschland
datenschutz@healthdataspace.de
+49 (0)9171 96 71-0

Hinweise zum Datenschutz bei HealthDataSpace

Nachfolgend haben wir für Sie Hinweise zum Datenschutz zusammengestellt, die Sie bei der Nutzung des HealthDataSpace (HDS) in den Ausführungen HDS PRO für Ärzte und HDS Basisversion für Patienten und bitte beachten sollten.

Hinweise für Ärzte und medizinisches Personal

Datenschutzrechtlich verantwortliche Stelle

Als behandelnder Arzt sind Sie bzw. Ihre Organisation für die Einhaltung der Datenschutzbestimmungen beim Einsatz von HealthDataSpace gemäß der Datenschutzgrundverordnung (DSGVO) bzw. den für Ihre Organisation einschlägigen Bestimmungen verantwortlich. Die Digithurst Bildverarbeitungssysteme GmbH & Co. KG wird als Auftragsdatenverarbeiter für Sie tätig und setzt hierfür ein Rechenzentrum der Telepaxx Medical Archiving GmbH am Standort Büchenbach in Deutschland ein. Näheres regelt ein Vertrag zur Auftragsdatenverarbeitung.

HealthDataSpace ist so eingerichtet, dass es konform zur Datenschutzgrundverordnung (DSGVO) genutzt werden kann. Bitte prüfen Sie vor einer Datenverarbeitung, ob die Daten Ihrer Patienten und Mitarbeiter unter Einhaltung der einschlägigen Datenschutzbestimmungen verarbeitet werden dürfen und halten Sie die Standardprozeduren im Umgang mit HealthDataSpace ein. Nur so können wir den Schutz der Daten optimal gewährleisten. Im Zweifel kontaktieren Sie Ihren Datenschutzbeauftragten oder die zuständige Aufsichtsbehörde.

Personenbezogene und besondere personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Patientendaten sind demnach besondere personenbezogene Daten.

Zulässigkeit der Datenverarbeitung

Die Verarbeitung ist nur zulässig, wenn dies auf einer informierten, freiwilligen, widerruflichen und nachweisbaren Einwilligung des Betroffenen beruht oder sich auf eine rechtliche Grundlage stützen kann. Letzteres kann z.B. ein Behandlungsvertrag sein oder die Wahrnehmung lebenswichtiger Interessen des Betroffenen.

Die Verarbeitung von Patientendaten im HDS beruht auf der freiwilligen Überlassung der Daten durch den Patienten selbst und stützt sich damit auf den Behandlungsvertrag. Patientendaten dürfen im Rahmen der Weiterbehandlung auch an andere Ärzte weitergegeben werden. Sofern Daten allerdings an nicht-mitbehandelnde Personen weitergegeben werden, ist eine Einwilligung des Patienten sowie die Entbindung von der Schweigepflicht erforderlich. Beachten Sie bitte, dass ein Zugriff unbefugter Personen ggf. eine für den behandelnden Arzt strafrechtlich relevante Offenbarung nach sich ziehen kann, sofern keine Entbindung von der Schweigepflicht vorliegt. Bitte benutzen Sie für diese sehr individuellen Fälle das in Ihrer Organisation gängige Muster.

Da wir aufgrund der Verschlüsselung der Daten keinen Zugriff auf Patientendaten haben, ist uns ein Support zu Patientendaten nicht möglich. Wir bieten Ihnen außerhalb des HealthDataSpace allgemeine FAQs für häufige Fragen und Antworten, z.B. zu Ihrem Account-Login oder der Benutzung der Upload- oder Download-Funktionen an.

Im Rahmen von HDS PRO werden auch Bestands- und Kontaktdaten (Vor- und Nachname, Name der Institution, Anschrift, Email-Adresse) von Ärzten und medizinischem Personal gespeichert und verarbeitet. Ihre Verarbeitung stützt sich auf das jeweilige Beschäftigungsverhältnis bzw. erfolgt im berechtigten Interesse Ihrer Organisation, wobei Sie aber für den Einzelfall prüfen müssen, ob nicht schutzwürdige Interessen oder betriebliche Regelungen (z.B. Betriebsvereinbarungen) dem entgegenstehen. Sie können in Ihr Profil übrigens auch ein Foto hochladen. Bitte achten Sie bei der Erstellung der Fotos darauf, dass diese nicht unerwünscht zu anderen Clouddiensten hochgeladen werden.

Wir möchten Sie in diesem Zusammenhang darauf hinweisen, dass wir in Ihrem Auftrag auch sogenannte Sekundärdaten bei der Benutzung des HDS verarbeiten. Dies sind etwa Nutzungsdaten oder Log-Protokolle, die wir zur Kontrolle der Sicherheit der IT-Systeme unter Beachtung der gesetzlichen Bestimmungen benötigen.

Datenvermeidung und Datensparsamkeit

Die Datenverarbeitung innerhalb des HDS muss sich an den Grundsätzen der Datensparsamkeit und Datenvermeidung orientieren. Danach sind so wenige

personenbezogene Daten wie nötig und nur so viele wie erforderlich zu verarbeiten. Für das Befüllen von Freitextfeldern stellen Sie bitte für Ihre Mitarbeiter Grundsätze auf, die einen datenschutzkonformen Umgang in diesem Sinne garantieren und vorsehen, dass Freitextfelder nur mit behandlungsbezogenen Daten befüllt werden.

Zweckbindung und Transparenz

Grundsätzlich dürfen personenbezogene Daten nur zweckgebunden verarbeitet werden, d.h., der Zweck der Datenverarbeitung muss vor der erstmaligen Erfassung bereits feststehen.

Wenn Sie Patientendaten innerhalb des HDS an andere Stellen weitergeben, wird der am HDS teilnehmende Patient hierüber automatisch systemseitig informiert. Dadurch wird der Patient in die Lage versetzt, den von ihm freigegeben Link zu seinen Gesundheitsdaten jederzeit zurückzuziehen. Bitte beachten Sie, dass der Patient auch informiert werden muss, sofern Sie Patientendaten außerhalb des HDS an andere Stellen weitergeben möchten.

Für die Weitergabe außerhalb des Behandlungsverhältnisses, die vom bestimmungsgemäßen Gebrauch des HDS nicht mehr umfasst sind, sind eine Einwilligung sowie eine Entbindung von der ärztlichen Schweigepflicht notwendig. Bitte benutzen Sie für diese sehr individuellen Fälle das in Ihrer Organisation gängige Muster.

Anonymisierung und Pseudonymisierung von Daten

Es empfiehlt sich, wo immer möglich von einer Pseudonymisierung oder Anonymisierung Gebrauch zu machen. Eine Anonymisierung liegt vor, wenn sämtliche identifizierende Merkmale aus einem Datensatz entfernt wurden und eine Zuordnung zu einer Person somit unmöglich ist. Pseudonymisierung bedeutet, dass personenbezogene Informationen durch neue, nicht personenbezogene Kennungen ersetzt werden. Dabei ist üblicherweise eine Verkettung der einzelnen Datensätze noch möglich und unter Umständen kann ein Personenbezug noch hergestellt werden.

Löschen und Sperren

Bitte beachten Sie, dass hinsichtlich der Aufbewahrung von personenbezogenen Daten unterschiedliche Speicherfristen gelten. Gemäß § 10 der Musterberufsordnung für Ärztinnen und Ärzte gilt für Patientendaten grundsätzlich eine 10jährige Aufbewahrungsfrist, die sich auf das von Ihnen eingesetzte Arzt-Informationssystem (kurz „AIS“) bezieht. Die Daten innerhalb des HDS PRO stellen nur Kopien der Daten aus Ihrem AIS dar, für welche diese

Aufbewahrungsfristen nicht gelten. Die Daten sind im HDS daher unverzüglich zu löschen, sobald der Zweck ihrer Erfassung entfallen ist.

Rechte der Betroffenen

Bitte beachten Sie, dass die von der Datenverarbeitung mittels des HDS betroffenen Personen unterschiedliche Rechte haben können. Grundsätzlich gehören hierzu Auskunfts-, Benachrichtigungs- und Informationsrechte, das Recht auf Berichtigung, Löschung, Sperrung oder das Recht auf Widerruf der Erlaubnis zur Datenverarbeitung. Bitte beachten Sie auch die ggf. für Ihre Stelle anwendbaren besonderen Informationspflichten des Bürgerlichen Gesetzbuches (BGB) und des Patientenrechtegesetzes.

Technisch-organisatorische Datenschutzmaßnahmen

Wir treffen angemessene Maßnahmen, um den Schutz Ihrer Daten und der Ihrer Patienten bei uns zu gewährleisten. Etwa ist der Loginvorgang am Webportal des HDS per SSL verschlüsselt und damit vor unbefugtem Auslesen der Zugangsdaten gesichert. Patientendaten liegen im HDS und in Ihrer HDS PRO Anwendung in verschlüsselter Form vor, so dass nur Sie und der Patient diese Daten entschlüsseln können. Alle Daten liegen räumlich gesehen in einem sicheren Rechenzentrum in Deutschland. Die dort getroffenen technisch-organisatorischen Datenschutzmaßnahmen sind im Vertrag zur Auftragsdatenverarbeitung dokumentiert und werden regelmäßig kontrolliert.

Treffen auch Sie bitte technische und organisatorische Maßnahmen für den Datenschutz im Umgang mit dem HDS: Definieren Sie, welche Mitarbeiter für welche Vorgänge auf dem System berechtigt sind. Kontrollieren Sie die Einhaltung des Berechtigungskonzepts regelmäßig. Geben Sie keine Daten an unberechtigte Personen weiter. Sofern Sie externe Dienstleister für die Datenverarbeitung oder Wartung und Pflege der IT einsetzen, kontrollieren Sie diese regelmäßig und schriftlich auf Einhaltung des Datenschutzes.

Stellen Sie sicher, dass Ihr Benutzeraccount nur von Ihnen genutzt wird und das Passwort nicht an anderen Stellen verwendet wird. Verwenden Sie bitte insbesondere niemals das gleiche Passwort, das Sie auch für den Zugang zu anderen Systemen nutzen.

Außerdem bieten einige Internet-Browser die Möglichkeit zur Passwortspeicherung an, auch ohne Rückfrage. Diese Funktionen zur Passwortspeicherung im Cache des Browsers dürfen nicht genutzt werden! Übermitteln Sie keine Personendaten unverschlüsselt über das Internet. Dies gilt auch für die Weitergabe von Daten per E-Mail. Sofern Sie mobile Datenträger (USB-Sticks, tragbare Speichermedien, Laptops, Smartphones, Tablets o.ä.)

verwenden, nutzen Sie Verschlüsselungsmechanismen der Festplatten und halten Sie die Datenschutz- und Sicherheitsbestimmungen ein. Zusätzlich ist zu beachten, dass im HDS keine Speicherung der systemseitigen Schlüssel für eine Entschlüsselung der Patientendaten im Rechenzentrum erfolgt. Bewahren Sie daher die Kopie Ihres individuellen Aktivierungscode an einem besonders geschützten Standort, z.B. einem feuersicheren Tresor oder an einem ausgelagerten Standort auf. Verpflichten und informieren Sie Ihre Mitarbeiter auf die Einhaltung des Datenschutzes.

Bitte beachten Sie, dass gemäß des deutschen Datenschutzrechts die Pflicht zur Bestellung eines betrieblichen oder behördlichen Datenschutzbeauftragten besteht, der die Anwendung des HDS PRO ggf. vorab für Ihre Organisation datenschutzrechtlich im Rahmen einer sogenannten Vorabkontrolle bewerten muss. Beziehen Sie Ihren Datenschutzbeauftragten daher rechtzeitig ein. Ferner ist es in der Regel datenschutzrechtlich erforderlich, den HDS PRO in einem gesetzlich vorgeschriebenen Verzeichnis aufzuführen und die Datenverarbeitung zu dokumentieren. Anhand der Gebrauchsanweisung und dieses Dokuments erhalten Sie hierfür bereits wesentliche Informationen. Kontaktieren Sie in Zweifelsfällen den Datenschutzbeauftragten Ihrer Organisation. Im Übrigen unterstützen Sie die Ersteller dieses Dokumentes gerne mit weiteren Informationen.

Hinweise für Patienten

Der HealthDataSpace für Patienten ist ein Angebot der Telepaxx Medical Archiving GmbH. HealthDataSpace ist so eingerichtet, dass er konform zur Datenschutzgrundverordnung (DSGVO) genutzt werden kann. Bitte halten Sie die Standardprozeduren im Umgang mit dem HDS ein. Nur so können wir den Schutz der Daten optimal gewährleisten.

Ihre Rechte als Betroffener

Über Ihre Patientendaten im HDS bestimmen Sie selbst, d.h., Sie haben es selbst in der Hand, Daten dort hochzuladen, zu verarbeiten, mit anderen zu teilen oder die Berechtigungen wieder zu entfernen und Daten zu löschen. Sie werden ferner systemseitig automatisch informiert, sofern eine Person, die Ihren Link zu Ihren Daten erhalten hat, diese mit anderen teilen möchte. Sie können zudem den Nutzungsvertrag des HDS unter Beachtung der Allgemeinen Nutzungsbestimmungen kündigen und wir löschen in diesem Fall den Account mit allen Daten darin. Nach Löschung haben Sie dann keine Möglichkeiten mehr, auf Ihre Daten zuzugreifen.

Da wir aufgrund der Verschlüsselung der Daten keinen Zugriff auf Ihre Patientendaten haben, ist uns ein Support zu Ihren Patientendaten nicht möglich. Wir bieten Ihnen außerhalb des HealthDataSpace allgemeine FAQs für häufige Fragen und Antworten, z.B. zu Ihrem Account-Login oder der Benutzung von Up-load- oder Download-Funktionen an.

Sofern Sie Daten einem Arzt oder einer anderen Person über den HDS zur Verfügung stellen, ist dieser für die Datenverarbeitung und die Einhaltung Ihrer Rechte verantwortlich. Daten, die wir im Rahmen der Registrierung und Anmeldung sowie ggf. zur Abrechnung der kostenpflichtigen Version des HDS benötigen, verarbeiten wir unter Beachtung der Bestimmungen der Datenschutzgesetze. Wir bewahren diese Nutzungsdaten unter Beachtung der gesetzlichen Aufbewahrungsfristen auf und löschen sie nach deren Ablauf vollständig. Gerne erteilen wir Ihnen Auskunft über die zu Ihrer Person verarbeiteten Daten.

Wie wir Ihre Daten schützen

Wir treffen angemessene Maßnahmen, um den Schutz Ihrer Daten bei uns zu gewährleisten. Ihre Daten im HealthDataSpace werden in einem abgesicherten Rechenzentrum der Telepaxx Medical Archiving GmbH im Standort in Büchenbach verarbeitet. Etwa ist der Loginvorgang am Webportal des HDS per SSL verschlüsselt und damit vor unbefugtem Auslesen der Zugangsdaten gesichert. Patientendaten liegen im HDS in verschlüsselter Form vor, so dass nur Sie und die Person, mit der Sie die Daten teilen möchten, Ihre Daten entschlüsseln können. Alle Daten liegen räumlich gesehen in einem sicheren Rechenzentrum in Deutschland. Die dort getroffenen technisch-organisatorischen Datenschutzmaßnahmen sind vertraglich dokumentiert und werden regelmäßig kontrolliert.

Wie Sie Ihre Daten optimal schützen

Treffen auch Sie bitte technische und organisatorische Maßnahmen für den Datenschutz im Umgang mit dem HDS: Stellen Sie sicher, dass Ihr Benutzeraccount nur von Ihnen genutzt wird und das Passwort nicht an anderen Stellen verwendet wird. Verwenden Sie bitte insbesondere niemals das gleiche Passwort, das Sie auch für den Zugang zu anderen Systemen nutzen. Außerdem bieten einige Internet-Browser die Möglichkeit zur Passwortspeicherung an, auch ohne Rückfrage. Diese Funktionen zur Passwortspeicherung im Cache des Browsers dürfen nicht genutzt werden!

Übermitteln Sie keine Personendaten unverschlüsselt über das Internet. Dies gilt auch für die Weitergabe von Daten per E-Mail. Sofern Sie mobile Datenträger (USB-Sticks, tragbare Speichermedien, Laptops, Smartphones,

Tablets o.Ä.) verwenden, nutzen Sie Verschlüsselungsmechanismen der Festplatten und halten Sie die Datenschutz- und Sicherheitsbestimmungen ein. Zusätzlich ist zu beachten, dass im HDS keine Speicherung der systemseitigen Schlüssel für eine Entschlüsselung der Patientendaten im Rechenzentrum erfolgt. Bewahren Sie daher die Kopie Ihres individuellen Aktivierungscodes an einem besonders geschützten Standort, z.B. einem feuersicheren Tresor oder an einem ausgelagerten Standort auf.