A CompuGROUP Company

HEALTH COMMUNICATION SERVICE

medical net

Version 05/2018

DSGVO

Handbuch Datenschutzgrundverordnung

Health Communication Service GmbH
Firmensitz: Pachergasse 4 | A – 4400 Steyr | FN 232545d, LG Steyr
Postanschrift: Ricoweg 22 | A – 2351 Wiener Neudorf
office@hcs.at
T +43 (0) 2236 8000-600
F +43 (0) 2236 8000-777

hcs.at

Synchronizing Healthcare

CGM CompuGroup Medical

DISCLAIMER

Sehr geehrte Damen und Herren,

dieses Handbuch, einschließlich aller Teile unterliegt dem Urheberrecht. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung von HCS unzulässig.

Wir haben aus Rücksicht auf leichtere Lesbarkeit des Handbuches von geschlechtsspezifischen Differenzierungen (wie z.B. Arzt/Ärztin, Assistent/ Assistentin, Patient/Patientin,...) Abstand genommen.

HCS behält sich das Recht vor, jegliche Informationen, die in diesem Handbuch enthalten sind, ohne vorherige Ankündigung zu modifizieren.

Bei der Zusammenstellung der Texte und Screenshots wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Für technische oder typografische Fehler wird seitens HCS keine Haftung übernommen. HCS ist nicht für direkte oder indirekte Folgeschäden haftbar oder verantwortlich, die in Verbindung mit der Ausstattung, der Leistung und dem Einsatz dieses Produkts entstehen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar. Sie können diese per Mail an office@hcs.at richten.

Bitte beachten Sie, dass dieses Handbuch keine Rechtsberatung darstellt und nehmen Sie im Zweifelsfall die Dienste eines Rechtsanwalts in Anspruch.

www.hcs.at

© Copyright 2018, HCS GmbH

Alle Rechte vorbehalten.

Version 5/2018

INHALTSVERZEICHNIS

1. VORWORT

Die Datenschutz-Grundverordnung (DSGVO) ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates von 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. Die DSGVO tritt am 25. Mai 2018 in Kraft.

Es wurden Maßnahmen getroffen, um die Programme der HCS GmbH DSGVO-konform zu gestalten. Alle Informationen, um die Programme entsprechend einstellen und konfigurieren zu können sind den anschließenden Kapiteln, und den entsprechend darin verwiesenen Dokumenten zu entnehmen.

2. VORAUSSETZUNGEN

Um die Produkte der HCS GmbH DSGVO-konform zu betreiben, muss die Benutzerverwaltung in den einzelnen Programmen aktiviert werden.
Eine Kurzanleitung dafür finden Sie im Kapitel 8.1.

3. WICHTIGE HINWEISE FÜR SUPPORTFÄLLE

Damit die gesetzlichen Anforderungen der DSGVO erfüllt bleiben, ist für Supportfälle eine eigene, von der HCS GmbH versendete **Vereinbarung zur Auftragsvereinbarung (AVV)** zu unterfertigen, und an die HCS GmbH zurück zu senden. Sollte diese AVV nicht vorliegen, können Supportfragen (z.B. Fernwartungen) ab dem 25.05.2018 nicht mehr durchgeführt werden.

DIE GENAUEN HINWEISE UND DAS VORGEHEN ZUR AVV SIND DEN AKTUELLEN AUSSENDUNGEN BEZÜGLICH DSGVO ZU ENTNEHMEN.

Des Weiteren wird dringend empfohlen, unter keinen Umständen Dokumente mit Patientendaten oder Befunde, die Patientendaten oder Realdaten enthalten (auch nicht zu Testzwecken) an den HCS Support per Brief, E-Mail oder FAX zu übermitteln!

4. TRANSPARENTE INFORMATION DER BETROFFENEN PERSONEN (ART. 12 DSGVO)

Es ist empfehlenswert, die Datenschutzerklärung (Hilfe dazu ist der entsprechenden ÄK-Vorlage zu entnehmen) vollständig ausgefüllt, auch für die Patienten einsehbar in der Ordination aufzubewahren.

5. AUSKUNFTSRECHT DER BETROFFENEN PERSONEN (ART. 13, 14 UND 15 DSGVO)

5.1. Datenschutzerklärung der Ordination

Es ist empfehlenswert, die Datenschutzerklärung (Hilfe dazu ist der entsprechenden ÄK-Vorlage zu entnehmen) vollständig ausgefüllt, auch für die Patienten einsehbar in der Ordination aufzubewahren.

© Health Communication Service GmbH. Alle Rechte vorbehalten

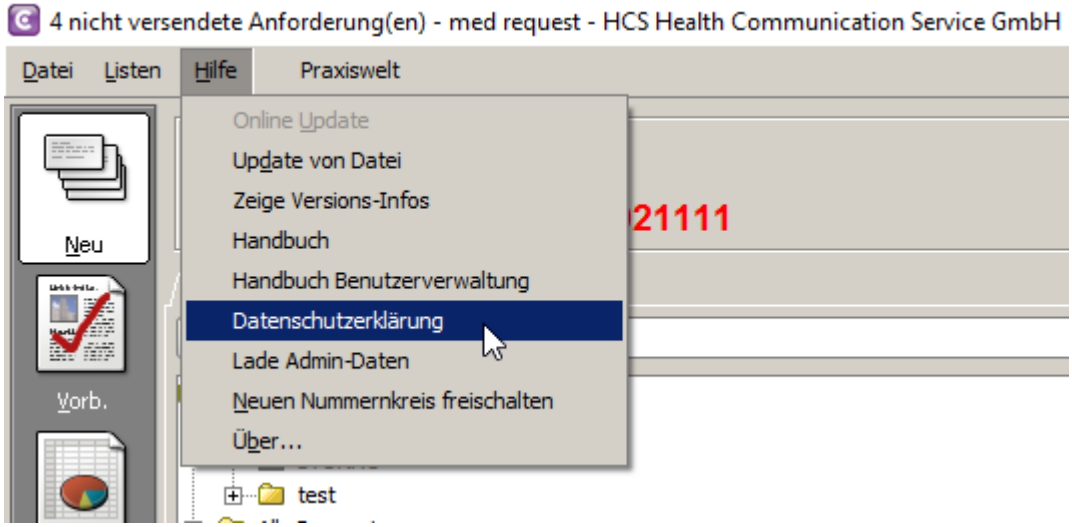
5.2. HCS Datenschutzerklärungen

Die Datenschutzerklärung des jeweiligen Produkts ist in den Produkten selbst zu finden:

5.2.1. med connect – HCS.Connector

5.2.2. med connect – HCS.Connector.Neon

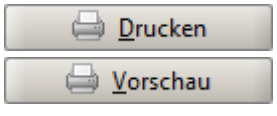
5.2.3. med request



5.3. Ausdruck von Patientendaten

5.3.4. med request

Jede mit **med request** erzeugte (vorbereitet oder abgeschlossen) Anforderung zum Patienten kann einzeln ausgedruckt werden.
Hierfür muss **med request** mit dem gewünschten Patienten aufgerufen werden. In den Ansichten „Vorbereitet“ und „Gesendet“ können mithilfe des Buttons Drucken oder Vorschau die einzelnen Überweisungsscheine ausgedruckt werden:



© Health Communication Service GmbH. Alle Rechte vorbehalten

5.3.5. med connect

Jeder mit **med connect** versendete oder empfangene Befund kann in den Protokollen HCS.Connector oder HCS.Connector.Neon gesucht und mit dem Button „Drucken“ ausgedruckt werden:

NÄHERE INFORMATIONEN DAZU SIND IM BENUTZERHANDBUCH DES JEWEILIGEN PRODUKTS ZU ENTNEHMEN.

6. LÖSCHEN VON DATEN (ART. 17 DSGVO)

In **med connect** ist standardmäßig eine automatische Löschung aktiviert, welche alle übertragenen Befunde älter als 186 Tage endgültig löscht. Zusätzlich können jüngere Befunde über den Löschbutton im HCS.Connector oder HCS.Connector.Neon endgültig manuell gelöscht werden. Voraussetzung dafür ist ein Benutzer mit den dafür notwendigen Rechten. Nähere Informationen dazu sind im Dokument „Benutzerberechtigungsverwaltung“ und im aktuellsten Benutzerhandbuch zu finden.

In **med request** können alle Daten eines Patienten nur direkt in der Programmdatenbank endgültig gelöscht werden. Hierzu kontaktieren Sie bitte die HCS Support-Hotline.

7. RECHT AUF DATENÜBERTRAGBARKEIT (ART. 20 DSGVO)

Wird der Export von Patientendaten in maschinenlesbarer Form aus der Datenbank von **med request** benötigt, kann dieser über den HCS Support angefordert werden. Es ist empfehlenswert, in diesem Fall, fristgerecht mit dem HCS Support in Kontakt zu treten.

Jeder mit **med connect** versendete oder empfangene Befund kann in den Protokollen HCS.Connector oder HCS.Connector.Neon gesucht und mit dem Button „Speichern“ in maschinenlesbarer Form gesichert werden.

8. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 DSGVO)

8.1. Benutzerberechtigungen

Benutzerberechtigungsverwaltung wird bei Neuinstallationen standardmäßig aktiviert und das Administratorkennwort vom Kunden selbst vergeben.
Die Benutzerberechtigungsverwaltung regelt die Berechtigung der Funktionen jedes Systembenutzers. Bei der Neuanlage eines Benutzers, müssen jegliche Berechtigungen aktiv zugewiesen werden.

NÄHERE INFORMATIONEN DAZU SIND IM DOKUMENT BENUTZERBERECHTIGUNGSVERWALTUNG DES JEWEILIGEN PRODUKTS ZU ENTNEHMEN.

© Health Communication Service GmbH. Alle Rechte vorbehalten

9. SICHERHEIT DER VERARBEITUNG (ART. 32 DSGVO)

9.1. Benutzerverwaltung

Die sichere, verschlüsselte Anmeldung und die entsprechende Zuordnung zum Tätigkeitsbereich sind durch die Aktivierung und Konfiguration der Benutzerberechtigungsverwaltung gegeben. Durch verschiedene Berechtigungsrollen kann gesteuert werden, ob der Benutzer

- Patientendaten einsehen darf oder nicht
- dazugehörige Befunddaten einsehen darf oder nicht
- diese Daten löschen darf oder nicht

Nur Benutzer mit Administratorenrechten kann Änderungen an der Benutzerverwaltung vornehmen.

Nach dem ersten Login und nach zurücksetzen des Passworts durch einen Administrator, wird der Benutzer beim nächsten Login aufgefordert sein Passwort zu ändern. Damit wird sichergestellt, dass nur der Benutzer selbst sein Passwort kennt.

NÄHERE INFORMATIONEN DAZU SIND IM DOKUMENT BENUTZERBERECHTIGUNGSVERWALTUNG DES JEWEILIGEN PRODUKTS ZU ENTNEHMEN.

9.2. Protokollierung

Definierte vom Benutzer ausgeführte Funktionen in den Programmen der HCS, werden protokolliert, zum Beispiel Aktionen in der Benutzerverwaltung oder die Befundanzeige.

NÄHERE INFORMATIONEN DAZU SIND IM DOKUMENT BENUTZERBERECHTIGUNGSVERWALTUNG DES JEWEILIGEN PRODUKTS ZU ENTNEHMEN.

9.3. Verschlüsselte Datenträger

Ebenfalls zentraler Bestandteil der Datensicherheit sind verschlüsselte Datenträger. Dies betrifft die Datenträger der jeweiligen Arbeitsstationen und Server. Der Status kann in **med request** unter „Hilfe“ – „Über…“ und in **med connect** unter „Support“ – „Systemdiagnose“ eingesehen werden.

ES WIRD EMPFOHLEN, DIE VERSCHLÜSSELUNG DER DATENTRÄGER VOR ORT DURCH DEN HARDWAREBETREUER DER ORDINATION DURCHFÜHREN ZU LASSEN.

9.4. Backup und Restore

Wir empfehlen dringend, die HCS Programme auf verschlüsselten Datenträgern zu sichern.

10. MELDUNG VON DATENPANNEN (ART. 33 DSGVO)

Die Meldung von Datenpannen (z.B. der Verlust einer unverschlüsselten externen Datensicherung) kann über ein Formular, welches bei der Ärztekammer aufliegt, durchgeführt werden.

NÄHERE INFORMATIONEN ZUM FORMULAR KÖNNEN BEI DER JEWEILIGEN ÄRZTEKAMMER ERFRAGT WERDEN.

© Health Communication Service GmbH. Alle Rechte vorbehalten

A CompuGROUP Company

HEALTH COMMUNICATION SERVICE

© **Health Communication Service GmbH**
Alle Rechte vorbehalten

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt,
ohne ausdrückliche schriftliche Erlaubnis der Health Communication Service GmbH
darf kein Teil dieser Unterlage für welche Zwecke auch immer vervielfältigt oder
übertragen werden, unabhängig davon, auf welche Art oder mit welchen Mitteln,
elektronisch oder mechanisch dies erfolgt.

Synchronizing Healthcare

CompuGroup Medical