HINWEISE ZU

DATENSCHUTZ UND DATENSICHERHEIT

DSGVO

In Ihrem Arztinformationssystem wurden Maßnahmen getroffen, um das Programm DSGVO-konform zu gestalten. Wir möchten Sie hiermit daran erinnern, dass Sie selbst dafür Sorge zu tragen haben, dass **Ihre Einstellungen und Prozesse entsprechend eingerichtet sind und genutzt werden.**

Für eine ordnungsgemäße Umsetzung der DSGVO empfehlen wir, die **Passwortrichtlinien in Ihrem Arztinformationssystem zu aktivieren.** Zusätzlich ist es empfehlenswert die **Benutzer mit ihren speziellen Rollen,** und den damit verbundenen Berechtigungen auszustatten. Alle Informationen, um das Programm entsprechend einstellen und konfigurieren zu können, entnehmen Sie bitte dem jeweiligen Produkthandbuch.

PASSWÖRTER

Passwörter müssen eine Länge zwischen **7 und 20 Zeichen, mindestens einen Groß- und Kleinbuchstaben, eine Ziffer, ein Sonderzeichen oder Umlaut** – aber keine Leerzeichen enthalten. Auch wenn Sie diese Funktion deaktivieren können, empfehlen wir, die **Einstellung „auf starke Passwörter prüfen"** aktiviert zu belassen.

In Ihrem Arztinformationssystem kann außerdem eingestellt werden, wie lange Passwörter gültig sind. Nach Ablauf der Gültigkeit erscheint der Dialog zur Passwort-Änderung.

Die Passwörter werden, dem aktuellen Stand der Technik entsprechend, nicht rückführbar (SHA256-Hash mit Random-Salt) in der Datenbank gespeichert. Das Auslesen von Passwörtern ist weder für Hauptbenutzer noch für das Help Center möglich.

DATALOCKER 500 GB

im Webshop bestellen:
aisat-shop.cgm.com

DATENSICHERUNG

Ihre Datensicherung ist im Notfall das einzige Medium von welchem Sie eine **vollständige Rekonstruktion Ihrer Daten** wiederherstellen können.

Umso wichtiger ist eine regelmäßig Überprüfung Ihrer Sicherung. Nicht immer sind Daten, welche sich auf Ihrem Sicherungsmedium befinden, brauchbar oder aktuell.

Unter **www.cgm.com/at-tipps** finden Sie eine Beschreibung, wie Sie selbst zumindest die Aktualität Ihrer Daten überprüfen können. Eine Vollständigkeitsprüfung kann nur Ihr IT-Fachmann mittels Rücksicherung und Funktionstest der Arztsoftware durchführen.

VERSCHLÜSSELTE DATENTRÄGER

Zentraler Bestandteil der Datensicherheit sind verschlüsselte Datenträger. Dies betrifft sowohl die Datenträger der jeweiligen Arbeitsstationen und Server, als auch die externen Sicherungsdatenträger. Es liegt in Ihrer Verantwortung, dass Patientendaten regelmäßig gesichert und verschlüsselt aufbewahrt werden.

Interne und externe Datenträger können per Software verschlüsselt werden (Microsoft Bitlocker), für externe Datenträger empfehlen wir die Systeme von DataLocker (Datenträger mit Pin-Eingabefeld).

Wir raten Ihnen, die Sicherung der Daten Ihres Arztinformationssystems auf einem verschlüsselten Datenträger durchzuführen.

Bei den Datensicherungen ist weiters zu beachten, dass gelöschte Patientendaten auf älteren (nicht aktualisierten) Sicherungen vorhanden sein können.

Wir empfehlen Ihnen, die Verschlüsselung der Datenträger durch einen Hardwarebetreuer der Ordination oder einen CGM/INNOMED Servicespezialisten durchführen zu lassen.

DATENSCHUTZ UND DATENSICHERHEIT

REKONSTRUKTION IM NOTFALL

Muss im Notfall ein Datenträger wiederhergestellt werden, wird dazu der Wiederherstellungsschlüssel benötigt – diese müssen in der Ordination aufliegen. Sollten sie Ihnen nicht bekannt sein, unterstützen wir Sie gerne (kostenpflichtig) bei der Kontrolle der Datenträger und Ausgabe der Schlüssel.

KONFIGURATION DER ARZTSOFTWARE

Bitte kontrollieren Sie regelmäßig Ihre Einstellungen und Vorlagen auf Aktualität. Dies betrifft unter anderem von Ihnen konfigurierte Formulareinstellungen, Laborwerte und -grenzen, Medikationsinteraktionswerte sowie Einstellungen in der Rechnungslegung. Bitte tragen Sie Sorge dafür, dass alle Eingaben aktuell sind und den gesetzlichen Vorgaben entsprechen.

HINWEISE FÜR SUPPORTFÄLLE

Damit die gesetzlichen Anforderungen der DSGVO erfüllt werden, ist für Supportfälle eine **Vereinbarung zur Auftragsverarbeitung (AVV) zu unterfertigen.** Sollte diese AVV nicht vorliegen, können Supportfragen (z.B. Fernwartungen) nicht durchgeführt werden.

Des Weiteren bitten wir Sie eindringlich darum, **unter keinen Umständen Dokumente mit Patientendaten oder Befunde,** die Patientendaten oder Realdaten enthalten (auch nicht zu Testzwecken) per E-Mail, Brief oder Fax **an das Help Center zu übermitteln!**

CGM Arztsysteme Österreich GmbH
Ricoweg 22 | 2351 Wiener Neudorf
T +43 (0) 50 818-100 | arztsysteme.at@cgm.com | **cgm.com**/at

INNOMED Ges. für med. Softwareanwendungen GmbH
Ricoweg 22 | 2351 Wiener Neudorf
T +43 (0) 2236 8000 | office@innomed.at | **innomed.at**

PROTOKOLLIERUNG IN ELGA

Zum Schutz der Daten und zwecks Nachvollziehbarkeit werden in ELGA alle getätigten Zugriffe dokumentiert. Diese sind durch die Patientin/den Patienten über das ELGA Portal jederzeit einsehbar.

MDR-HINWEIS

Auch wenn die Arztinformationssysteme der CGM im Gesundheitswesen eingesetzt werden, handelt es sich bei den Produkten **nicht um Medizinprodukte** im Sinne der Medizinprodukte-Regularien (*Richtlinie 93/42/EWG, die zuletzt durch die Richtlinie 2007/47/EG geändert wurde sowie der Verordnung (EU) 2017/745 betreffend Medizinprodukte (MDR), Medizinproduktegesetz (MPG)*).

Die Softwareprodukte unterstützen die Praxismitarbeiter bei der Terminplanung bzw. Terminverwaltung, der medizinischen und abrechnungsrelevanten Dokumentation, der Verordnung und Ausstellung von Formularen, der Abrechnung von Selbstzahlern und bei vielen weiteren Aufgaben.

Unsere Arztinformationssysteme sind nicht dazu bestimmt, automatisiert und ohne die erforderliche Fach- und Sachkenntnis medizinische Entscheidungen zu treffen, Diagnosen zu stellen oder Maßnahmen für und während Behandlungen von Patienten zu ergreifen!

Sie beziehen gegebenenfalls externe Systeme mit ein, um Berechnungen, Umrechnungen oder ähnliche Aufgaben zu dokumentieren. Sämtliche Aufgaben, die über die reine Dokumentation hinaus gehen, werden von diesen externen Systemen übernommen.

Unsere Softwareprodukte sind primär für Ärztinnen und Ärzte, medizinische Fachangestellte und andere im Gesundheitswesen tätige Personen mit der erforderlichen Fach- und Sachkenntnis bestimmt. Sie sind für die Benutzung durch die MitarbeiterInnen von Arztpraxen ausgelegt.

Weitere Informationen zum Thema Datenschutz und IT-Sicherheit finden Sie auf der Website der Österreichischen Ärztekammer: www.aerztekammer.at/it-sicherheit

Stand: 12/2021