CGM M1 PRO

Arztinformationssystem

CGM M1 PRO
SYSTEMINFORMATIONEN

Synchronizing Healthcare

CompuGroup Medical

Inhalt

1 Allgemeine Informationen für den Betrieb von CGM M1 PRO

CGM M1 PRO ist ein Arztinformationssystem mit einer sehr großen Funktionsvielfalt. Mit der richtigen technischen Ausstattung (-> Hardware) lassen Sie CGM M1 PRO zu einem unentbehrlichen Mitarbeiter der Praxis werden.

Damit Sie CGM M1 PRO in vollem Umfang nutzen können und ein reibungsloser Umgang realisiert werden kann, orientieren Sie sich bitte an den folgenden Systemanforderungen.

2 Hardware-Anforderungen

Die folgenden Mindestanforderungen gewährleisten eine reibungslose Funktionalität. Wir empfehlen jedoch, deutlich höhere Werte als die genannten Mindestanforderungen zu wählen. Server dürfen nicht als Arbeitsplatz verwendet werden.

2.1 Server

Mindestanforderungen

- Prozessor (CPU): Dual/Quad Core oder vergleichbar
- Arbeitsspeicher (RAM): 32 GB
- Festplattenkapazität (HD): 320 GB
- Netzwerkverbindung mit 1 Gbit/s

Empfohlene Hardware

- CPU-Quad-Core, ≥ 32 GB RAM, SAS- oder SSD-Festplatten mit automatischer Spiegelung.
- Bei Terminal-Server-Betrieb ist der RAM-Speicher entsprechend größer zu dimensionieren. Netzwerkverbindung von ≥ 1Gbit/s.

Installations-/Update-Empfehlung

- Freie Festplattenkapazität von mindestens 30 GB

2.2 Arbeitsplatzrechner (Client)

Mindestanforderungen

- Prozessor (CPU): Dual Core oder vergleichbar
- Arbeitsspeicher (RAM): 16 GB
- Festplatte (HD): 200 GB
- DVD-Laufwerk
- Netzwerkverbindung 1 Gbit/s

Empfohlene Hardware

- CPU Core, ≥ 16 GB RAM, SSD-Festplatte ≥ 200 GB, Netzwerkanbindung mit ≥ 1 Gbit/s

Installations-/Update-Empfehlung

- Freie Festplattenkapazität von mindestens 10 GB

Die angegebenen Hardwareanforderungen gelten pro Instanz der CGM M1 PRO-Anwendung. Bei mehreren Instanzen an einem Arbeitsplatz addieren sich die Anforderungen. Für eine reibungslose Nutzung sollten die verfügbaren Ressourcen entsprechend eingeplant und gegebenenfalls angepasst werden.

2.3 Arbeitsplatz-Monitor

Gemäß der derzeit gültigen Arbeitsstättenverordnung (ArbStättV) sind für Arbeitsplätze keine bestimmten Monitorgrößen vorgeschrieben. Die flexible Richtlinie gibt vor, dass der Arbeitsplatz ergonomisch der zu leistenden Arbeit angepasst sein muss. Für unser Produkt empfehlen wir einen Bildschirm mit mindestens 24" Bildschirmdiagonale und einer Auflösung von 1.920 x 1.080 Pixeln (entspricht Full-HD).

2.4 Ausfallsicherheit und Archivierung

Unterbrechungsfreie Stromversorgung (USV)

Für einen Server ist der Einsatz einer „Unterbrechungsfreien Stromversorgung“ dringend empfohlen. Diese Geräte wirken einem plötzlichen Stromausfall entgegen, indem die Stromversorgung für einen begrenzten Zeitraum über Akkus sichergestellt wird. Die Steuerungsinformationen der USV müssen an den Server weitergeleitet werden, damit die USV die Speicherung der aktuellen Informationen anstößt und der Server danach ohne Datenverlust heruntergefahren wird, da die Batterien nur einen begrenzten Zeitraum von wenigen Minuten Strom liefern kann.

Sonstiges

Zur Vermeidung von Datenverlust sollten zusätzliche Sicherheitsmaßnahmen in Absprache mit dem Vertriebs- und Servicepartner erörtert werden. Dazu können RAID, NAS, redundante Systeme oder andere Maßnahmen gehören, die allerdings auf die entsprechende IT-Infrastruktur angepasst werden müssen.

3 Netzwerk

3.1 Internetanbindung(DSL)-Router

Für Funktionen wie z. B. CGM LIFE, Fernwartung, Online-Update, Windows- und Virenschutz-Updates sowie weitere Online-Dienste sind eine sichere Internetverbindung und ein dafür ausgelegter Router erforderlich.

Mindestanforderungen

Für das reibungslose Übertragen von Daten (Senden und Empfangen) wird eine Übertragungsrate von mindestens 10 Mbit/s benötigt.

Empfohlene Anbindung

Wir empfehlen für den Einsatz - auch zu Zwecken des Supports - eine Übertragungsrate von mindestens 30 Mbit/s, damit das Arbeiten nicht von Ladezeiten (welche von der Datengeschwindigkeit des Providers resultieren) beeinträchtigt werden.

3.2 Verkabelung / Architektur

Terminalserver-Betrieb

CGM M1 PRO ist im Terminalserver-Betrieb funktionsfähig. Geräteanbindungen müssen vorher mit dem CGM M1 PRO-Vertriebs- und Servicepartner abgestimmt werden.

3.3 Architektur

Heimplatzanbindung

Zur stationären Heimplatzanbindung empfehlen wir eine VPN-Verbindung zum Server, über diese auf den Server zugegriffen werden kann. Der Praxis-Server benötigt dazu einen dauerhaft aktiven, leistungsfähigen DSL-Anschluss.

Verbindung zweier Netze (LAN-LAN-Kopplung)

Zur Außenstellenanbindung wird beidseitig DSL mit fester IP-Adresse empfohlen. Der jeweilige Anschluss sollte mit der Option „Fast Path“ geschaltet sein, um eine möglichst geringe Latenzzeit zu erhalten. Auch diese Verbindung sollte mit VPN realisiert werden. Die tatsächlich benötigte Bandbreite ist abhängig von Größe und Nutzung der Außenstelle.

3.4 Mobile Devices für Smartphones und Tablets

Für eine mobile Nutzung von CGM M1 PRO wurde die CGM M1 PRO Meine Patienten-App entwickelt. Der Praxisserver benötigt dazu einen dauerhaft aktiven, leistungsfähigen DSL-Anschluss.

4 Geräte-Anbindung

MPG – Medizinproduktegesetz

Sämtliche Computerarbeitsplätze, die an ein Medizinprodukt angeschlossen sind und somit einen direkten Patientenkontakt haben (z. B. Audiometer, EKG, EEG, Lungenfunktion, Sonographie-Geräte, Endoskopie-Gerät, Perimeter, Phoropter und viele weitere), müssen der DIN-Norm EN 60601-1 entsprechen.

5 Betriebssysteme (alle 64-Bit, ausschließlich deutsche Versionen)

CGM M1 PRO ist für die unten folgenden Betriebssysteme für Windows-kompatible Computer geprüft und zugelassen.

Server

- Microsoft Windows Server 2025
- Microsoft Windows Server 2022 Standard
- Microsoft Windows Server 2022 Essentials
- Microsoft Windows Server 2022 Datacenter
- Microsoft Windows Server 2022 Datacenter: Azure Edition
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2016 Datacenter
- Microsoft Windows Server 2016 Essentials

Für erhöhte Sicherheit und optimale Leistung empfehlen wir die Verwendung eines gehärteten Betriebssystems beim Betrieb von CGM M1 PRO. Bitte beziehen Sie sich auf die offiziellen Microsoft-Richtlinien zur Betriebssystem-Härtung: Leitfaden zu Sicherheitsbaselines | Microsoft Learn.

Arbeitsstationen

- Microsoft Windows 11 Professional und Enterprise, deutsche Version

Für erhöhte Sicherheit und optimale Leistung empfehlen wir die Verwendung eines gehärteten Betriebssystems beim Betrieb von CGM M1 PRO. Bitte beziehen Sie sich auf die offiziellen Microsoft-Richtlinien zur Betriebssystem-Härtung: Leitfaden zu Sicherheitsbaselines | Microsoft Learn.

Abkündigung

Alle zugelassenen Betriebssysteme werden im Regelfall bis zum Ablaufen des „Extended Support“ von Microsoft unterstützt (siehe auch: http://support.microsoft.com/gp/lifeselectindex).

Im Falle technischer Inkompatibilitäten kann eine frühere Abkündigung dediziert erfolgen.

CGM M1 PRO und die angebundenen CGM-Programme unterstützen keine ARM-Prozessoren.

6 Installation

Die vorzunehmende Installation, Rechnereinstellungen und Konfiguration wird vom zuständigen Vertriebs- und Servicepartner vorgenommen.

6.1 Standard-Software

Neben dem Betriebssystem wird auf den Computern noch folgende Software benötigt, um CGM M1 PRO zu verwenden:

Frameworks und Software

- Aktuelle Version CompuGroup-Java
- Aktuelle Version des Microsoft .NET Frameworks
- Aktuelle Version des Acrobat Readers

Virenschutz

- Jeder Rechner, auch Rechner ohne Anbindung an das Internet/Intranet, muss über ein Virenschutzprogramm verfügen. Die regelmäßige, am besten mehrfach tägliche Aktualisierung des Virenschutzes ist dabei essenziell.

- Für optimale Sicherheit empfehlen wir professionelle Anti-Virensoftware-Lösungen, die Sie bei den autorisierten Vertriebs- und Servicepartnern von CGM M1 PRO erhalten.

6.2 Office-Anwendungen

Für die Arztbriefschreibung (oder auch für statistische Auswertungen) werden von CGM M1 PRO aktuelle Microsoft Office-Anwendungen vorausgesetzt.

Die Textverarbeitung erfolgt über eine Schnittstelle zu Microsoft Word und ist in CGM M1 PRO integriert. Für folgende MS Word-Versionen ist CGM M1 PRO freigegeben:

- Microsoft Word 2016, 32-Bit
- Microsoft Word 2019, 32-Bit
- Microsoft Office 2021, 32-Bit
- Microsoft Office 365, 32-Bit (Wichtig: Bitte achten Sie darauf, die automatische Cloud-Speicherung zu deaktivieren.)
- Microsoft Office 2024, 32-Bit

6.3 Online-Update(s)

Aktuelle Update-Informationen können auf der Website unter cgm.com/m1pro-update eingesehen werden. Das Update kann entweder als herkömmliches Online-Update im CGM M1 PRO-System über die Kachel Zubehör|Online-Update heruntergeladen und installiert werden oder per CGM SMART UPDATE. Informationen zu CGM SMART UPDATE sind über die Website cgm.com/m1pro-smart-update erreichbar. Für den Download der Updates wird eine ausreichend schnelle Internetverbindung vorausgesetzt. Bei einer 16 Mbit/s Internet-Verbindung dauert der Download ca. 30 Minuten.

Ein umfrangreiches Quartalsupdate kann u. U. 5 GB überschreiten. Für diese Fälle wird eine Zip-Datei bereitgestellt, die zunächst heruntergeladen und entpackt werden muss. Im Anschluss daran kann das Setup ausgeführt werden. Auf der zuvor genannten Website finden Sie eine gesonderte Installationsanleitung.

6.4 Fernwartung

Fernwartungen werden nach den geltenden DS-GVO-Regelungen durchgeführt. Hierzu gibt es zentrale Regelungen der CGM (z. B. bleiben Fernwartungszugänge geschlossen und werden durch den Kunden freigeschaltet, Passwörter zu Kundensystemen werden nur für die Fernwartung erteilt, 4-Augen Prinzip durch qualifizierte Personen usw.). Wir verwenden hierzu das Fernwartungsmedium "AnyDesk", welches über CGM M1 PRO zur Verfügung gestellt wird und der Zugang durch den Kunden aktiv freigegeben werden muss. Eine Fernwartung kann zudem nur von CGM M1 PRO durchgeführt werden, wenn ein vom Kunden unterzeichneter AV-Vertrag (Vereinbarung zur Auftragsverarbeitung) vorliegt.

7 Datensicherung

Es ist eine tägliche Datensicherung der patientenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen durchzuführen. Wir empfehlen jedoch eine Datensicherung des gesamten Server-Systems.

7.1 CGM PRAXISARCHIV

Aufgrund geänderter gesetzlicher Vorgaben ist die in CGM M1 PRO integrierte Bild- und Dokumentenablage (-> „Karteikarte“) als alleiniges Archivsystem in den meisten Fällen nicht ausreichend. Für eine revisionssichere Archivierung der Patientendaten, wie diese vom Gesetzgeber verlangt wird, empfehlen wir daher den zusätzlichen Einsatz des TÜV-geprüften CGM PRAXIS-ARCHIVs.

8 Datensicherheit

8.1 Verschlüsselung

Ihr Vertriebs- und Servicepartner steht Ihnen gerne zur Verfügung, um Sie zu beraten, welche Maßnahmen ergriffen werden können, um das System spezifisch für Ihre Praxisumgebung zu härten. Darüber hinaus erhalten Sie Empfehlungen zu den Vorsichtsmaßnahmen, die in Ihrer spezifischen Praxiskonstellation ratsam sind.

Hauptmerkmale der Datensicherheit und -integrität in CGM M1 PRO:

- CGM M1 PRO behält die Authentizität und Integrität der eingegebenen Daten bei.
- CGM M1 PRO verfügt über ein umfangreiches Benutzer- und Rollenverwaltungssystem, das in das Rechteverwaltungs-Framework integriert ist.
- Darüber hinaus werden alle Daten, die innerhalb der Karteikarte eingegeben, geändert oder gelöscht werden, im Protokoll aufgezeichnet.
- Weitere Informationen zu Datensicherheit und Datenschutz finden Sie in Ihrem CGM M1 PRO unter: Hilfe | Datenschutz | Datenschutzerklärung

8.2 Authentizität

Die Authentizität der eingegebenen Daten in CGM M1 PRO wird gewährleistet. CGM M1 PRO verfügt über ein umfangreiches Benutzer- und Rollenkonzept, welches mit der CGM M1 PRO-Rechteverwaltung verknüpft ist. Zusätzlich werden Daten, die innerhalb der Karteikarte eingegeben, verändert oder gelöscht wurden, protokolliert.

Bitte beachten Sie auch unsere gesonderten Hinweise unter IT-Sicherheit.

9 IT-Sicherheit

Die Gewährleistung von IT-Sicherheit und Datenschutz ist in der Medizinbranche von größter Bedeutung. CGM M1 PRO verpflichtet sich zu höchsten Sicherheitsstandards, um die sensiblen Daten von Patienten und Praxen zu schützen. Dieses Kapitel gibt allgemeine Empfehlungen zur IT-Sicherheit sowie spezielle Hinweise zu den Sicherheitsmodulen der Compugroup, den Funktionen zu CGM AUTHENTICATE, den Betriebssystemen, Firewall- und Port-Einstellungen und externen Softwarelösungen.

9.1 Allgemeine Empfehlungen zur IT-Sicherheit

- **Regelmäßige Updates:** Halten Sie sowohl Ihre CGM M1 PRO-Software als auch das zugrunde liegende Betriebssystem stets auf dem neuesten Stand. Installieren Sie alle verfügbaren Updates zeitnah, um Sicherheitslücken zu schließen und neue Funktionen zu nutzen.
- **Starke Passwörter:** Verwenden Sie komplexe Passwörter mit mindestens 12 Zeichen, die aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie leicht zu erratende Passwörter und ändern Sie diese regelmäßig. Ändern Sie Standardpasswörter auf allen Geräten und Systemen unverzüglich nach der Einrichtung.]
- **Zugriffsrechte:** Weisen Sie Benutzern nur die benötigten Zugriffsrechte zu. Nutzen Sie die Möglichkeit, Rollen und Berechtigungen in CGM M1 PRO zu definieren, um Datenzugriffe zu steuern. Für eine optimale tägliche Nutzung des CGM M1 PRO wird empfohlen, dass Benutzer im Regelbetrieb ein Standard-Windows-Konto ohne Administratorrechte verwenden.
- **Sicherheitsbewusstsein:** Schulen Sie alle Mitarbeiter regelmäßig in Bezug auf IT-Sicherheit und Datenschutz. Sensibilisieren Sie sie für Phishing-Angriffe und andere Bedrohungen.
- **Datensicherung:** Führen Sie regelmäßige Datensicherungen durch und bewahren Sie Sicherungskopien an einem separaten Ort auf. Nutzen Sie die integrierten Backup-Funktionen von CGM M1 PRO.
- Überprüfen Sie regelmäßig, ob die Backups fehlerfrei wiederhergestellt werden können. Schützen Sie Ihre Backups zudem vor unerlaubtem Zugriff, Verlust und unbeabsichtigtem Überschreiben (z. B. durch einen Verschlüsselungstrojaner).

9.2 Betriebssysteme

- **Unterstützte Betriebssysteme:** Stellen Sie sicher, dass Sie eine unterstützte Version des Betriebssystems verwenden (z. B. Windows 11, siehe Betriebssysteme (alle 64-Bit, ausschließlich deutsche Versionen). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM M1 PRO.
- **Sicherheitseinstellungen:** Aktivieren Sie die integrierten Sicherheitsfunktionen des Betriebssystems, wie Windows Defender, um zusätzlichen Schutz vor Malware und Viren zu gewährleisten.

9.3 Firewall- und Port-Einstellungen

- **Firewall-Regeln:** Aktivieren Sie die Firewall Ihres Betriebssystems und konfigurieren Sie sie so, dass verdächtige Verbindungen blockiert werden. Erstellen Sie spezifische Firewall-Regeln, um den Netzwerkzugriff auf CGM M1 PRO zu kontrollieren.
- **Port-Management:** Schließen Sie alle nicht benötigten Ports, um unautorisierte Zugriffe zu verhindern. Prüfen Sie regelmäßig die offenen Ports auf Ihrem System und passen Sie die Einstellungen gegebenenfalls an.
- **Netzwerküberwachung:** Implementieren Sie Werkzeuge zur Überwachung des Netzwerkverkehrs, um ungewöhnliche Aktivitäten zu erkennen. Dies hilft, potenzielle Sicherheitsvorfälle frühzeitig zu identifizieren.
- **Incident Response Plan**: Seien Sie auf potenzielle Sicherheitsvorfälle vorbereitet, indem Sie einen klaren Reaktionsplan erstellen. Dieser Plan sollte definieren, wie schnell und effektiv auf Sicherheitsverletzungen reagiert wird. Legen Sie Verantwortlichkeiten, Kommunikationswege und konkrete Maßnahmen zur Schadensbegrenzung fest, um im Ernstfall handlungsfähig zu bleiben.

9.4 Besondere Module zur IT-Sicherheit der Compugroup

- **Security Monitoring:** Nutzen Sie das integrierte Monitoring-Tool zur Überwachung von ungewöhnlichen Aktivitäten und Sicherheitsvorfällen. Dies umfasst die Protokollierung von Zugriffen und Änderungen innerhalb der Software.
- **Verschlüsselung:** Alle sensiblen Daten werden sowohl bei der Speicherung als auch bei der Übertragung durch moderne Verschlüsselungstechniken geschützt. Stellen Sie sicher, dass die Verschlüsselungseinstellungen in den Softwareoptionen aktiviert sind.
- **Antiviren-Integration:** Integrieren Sie eine zuverlässige Antivirensoftware, die in Echtzeit Sicherheitsbedrohungen erkennt und blockiert. Halten Sie diese Software stets auf dem neuesten Stand.

9.5 CGM AUTHENTICATE

- **Sichere Anmeldeverfahren:** Nutzen Sie die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA) beim Login in die CGM M1 PRO-Software. Dies erhöht die Sicherheit erheblich und schützt vor unbefugtem Zugriff.
- **Automatische Abmeldung:** Aktivieren Sie die Funktion zur automatischen Abmeldung nach einer festgelegten Inaktivitätszeit. Dies verhindert, dass unbefugte Personen Zugriff auf Ihr System erhalten, wenn ein Benutzer seinen Arbeitsplatz verlässt.
- **Anmeldeprotokolle:** Überwachen Sie regelmäßig die Anmeldeprotokolle, um unautorisierte Zugriffe frühzeitig zu erkennen. Die Protokolle können im Administrationsbereich von CGM M1 PRO eingesehen werden.

Allgemeine Informationen zu CGM AUTHENTICATE erhalten Sie über unsere Website.
Ihr Vertriebs- und Servicepartner berät Sie gerne.

9.6 Externe Softwarelösungen

- **Zuverlässige Software:** Verwenden Sie nur vertrauenswürdige externe Softwarelösungen, die den Datenschutzanforderungen entsprechen. Informieren Sie sich über die Sicherheitszertifikate und Datenschutzrichtlinien der jeweiligen Anbieter.
- **Integration von Drittanbietersoftware:** Stellen Sie sicher, dass integrierte Drittanbietersoftware (z. B. Praxisverwaltungssysteme, Abrechnungssoftware) ebenfalls sicher konfiguriert ist. Überprüfen Sie die Kompatibilität mit CGM M1 PRO und halten Sie diese Software ebenfalls regelmäßig updated.
- **Datenschutzbestimmungen:** Beachten Sie stets die datenschutzrechtlichen Bestimmungen und stellen Sie sicher, dass die externe Software die notwendigen Maßnahmen zum Schutz sensibler Patientendaten umsetzt.

9.7 Schlussfolgerung

Die Implementierung der oben genannten Empfehlungen und Module ist entscheidend für die Sicherheit Ihrer Praxisdaten und die Einhaltung der gesetzlichen Vorgaben. CGM M1 PRO unterstützt Sie dabei, Ihre IT-Sicherheitsstrategie zu optimieren. Bei Fragen oder Unterstützung wenden Sie sich bitte an Ihren zuständigen Vertriebs- und Servicepartner.

10 Änderungshistorie

Version	Datum	Änderung	Autor
1.0	08.11.2018	Übernahme und allgemein Aktualisierung CGM M1 PRO	Volkmar Roth, Sarah März
2.0	27.06.2019	Betriebssystem Server 2019 hinzugefügt	Sarah März
3.0	20.12.2019	Änderungen Betriebssystem und Office-Anwendung	Sarah März
3.1	06.02.2020	Anpassung 2.3 Arbeitsplatz- Monitor / Auflösung Anpassung 6.4 Fernwartung	Sarah März
3.2	16.07.2020	Anpassung Word- und Java- Versionen	Sarah März
3.3	27.04.2021	Windows 8 unter Betriebssystem gelöscht	Sarah März
3.4	03.02.2021	Aktualisierung Betriebssysteme, Word, Entfernung Endpoint Protection	Sarah März
3.5	18.02.2022	Aktualisierung Angaben Betriebssysteme	Sarah März
3.6	03.08.2022	Aktualisierung Angaben Betriebssysteme (Win Server 2012 entfernt)	Sarah März
3.7	19.08.2022	Hinweis „ausschließlich deutsche Versionen“ bei Betriebssystemen hinzugefügt.	Sarah März
3.8	20.02.2024	Umfassende Aktualisierung des gesamten Dokuments	Melanie Diel
3.9	02.04.2025	Allgemeine Aktualisierung Porteinstellungen	Melanie Diel
3.10	03.04.2025	Ergänzung IT-Sicherheit	Sarah März
3.11	31.03.2026	Ergänzungen Serverbetriebssysteme und Office-Anwendungen	Sarah März, Hannes-Nils Unger

CGM M1 PRO

Arztinformationssystem

CompuGroup Medical Deutschland AG
Geschäftsbereich
Arztsysteme Maria Trost 25,
56070 Koblenz
info.m1pro@cgm.com

cgm.com/m1pro

Synchronizing Healthcare

CompuGroup Medical