

CGM TURBOMED

Systemanforderungen



INHALT

1	Allgemeine Informationen für den Betrieb von CGM TURBOMED	5
2	Hardware-Anforderungen	5
2.1	Windows 11	5
2.2	Server	6
2.2.1	Mindestanforderungen.....	6
2.2.2	Empfohlene Hardware	6
2.3	Arbeitsplatz-Computer	6
2.3.1	Mindestanforderungen.....	6
2.3.2	Empfohlene Hardware	6
2.4	Arbeitsplatz-Monitor	6
2.4.1	Mindestanforderungen.....	6
2.4.2	Empfohlene Monitorunterstützung	7
2.4.3	Anzeigeeinstellungen unter Windows.....	7
2.5	Ausfallsicherheit	7
2.5.1	Unterbrechungsfreie Stromversorgung (USV)	7
2.5.2	Redundante Netzteile	7
2.5.3	RAID-Controller	8
3	Netzwerkconfiguration	8
3.1	Internetanbindung (DSL) / Router	8
3.1.1	Mindestanforderungen.....	8
3.1.2	Empfohlene Anbindung.....	8
3.2	Netzwerk (LAN).....	8
3.3	Managed Firewall (ITSS) Proaktiver Schutz der Praxis-IT	8
3.4	Verkabelung / Architektur	9
3.4.1	Terminal-Server-Betrieb.....	9
3.5	Außenstellenanbindung per Virtual Private Network (VPN)	9
3.5.1	Heimplatzanbindung.....	9
3.5.2	Verbindung zweier Netze (LAN-LAN-Kopplung)	9
3.6	Mobile Endgeräte (Mobile Devices)	10
3.6.1	Tablet.....	10
3.6.2	Smartphone	10
3.7	Monitoring (N-Central).....	10
3.7.1	Mindestanforderungen.....	10
3.7.2	Empfehlung	10
3.8	Endpoint Protection	10
3.8.1	Mindestanforderungen.....	10
3.8.2	Empfohlene Hardware	11

4	Geräte-Anbindung.....	11
4.1	Medizinproduktegesetz (MPG).....	11
4.2	Barcode-Leser für den [Bundeseinheitlichen Medikationsplan] / das Modul [CGM BMP PLUS].....	11
4.3	Drucker.....	11
5	Betriebssysteme	12
5.1.1	Server.....	12
5.1.2	Arbeitsstationen	12
6	Konfiguration.....	13
6.1	Festplatten-Partitionen	13
6.1.1	Server.....	13
6.1.2	Arbeitsplatz	13
6.2	Virtualisierung	13
6.3	Netzwerkconfiguration	14
6.3.1	TCP/IP-Adressierung	14
6.3.2	Firewall-Regeln	14
6.3.3	Portfreischaltungen.....	14
6.3.4	Portkonfiguration.....	14
7	IT-Sicherheit	15
7.1	Allgemeine Empfehlungen zur IT-Sicherheit.....	15
7.2	Betriebssysteme.....	15
7.3	Firewall- und Port-Einstellungen	16
7.4	Besondere Module zur IT-Sicherheit der Compugroup.....	16
7.5	PC Log-In	16
7.6	Externe Softwarelösungen.....	17
7.7	Schlussfolgerung	17
8	Installation	17
8.1	Rechnernamen	17
8.2	Domäne.....	17
8.3	Freigaben (Verzeichnisse)	17
8.4	Umgebungsvariablen.....	18
8.5	Dienstemanagement	18
8.6	Datenbank	18
8.7	Virenschutz	18

8.8	Server-Einstellungen.....	19
8.9	Arbeitsplatz-Einstellungen	19
8.10	Betriebssystem-Einstellungen.....	19
8.11	Standard-Software	19
8.12	Office-Anwendungen	21
8.13	Online-Update(s).....	21
8.14	Fernwartung.....	21
9	Datensicherung.....	21
10	Datensicherheit und Verschlüsselung	21
11	Einrichtung spezifischer Software	22
12	Das Hilfe-System von CGM TURBOMED	23
12.1	Hinweise zur Nomenklatur in diesem Dokument	23
12.2	CGM TURBOMED Gebrauchsanweisung [F1].....	23
12.3	CGM TURBOMED Anwender-Hotline	23

1 Allgemeine Informationen für den Betrieb von CGM TURBOMED

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

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

Generell empfehlen wir die Installation und Konfiguration von CGM TURBOMED und den dafür benötigten Systemen und Komponenten durch CGM TURBOMED Vertriebs- und Servicepartner (VSP) durchführen zu lassen. Dementsprechend sind sämtliche Fragen und Absprachen mit Ihrem zuständigen CGM TURBOMED Vertriebs- und Servicepartner (VSP) abzuklären.

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!

WICHTIG:

- Die Mindestanforderungen gelten ausschließlich für den Betrieb von CGM TURBOMED. Sollten Sie weitere Programme (z.B. CGM PRAXISARCHIV, Software zur Geräteanbindung, Telefonsoftware, Microsoft Produkte) auf Ihren Computern installiert haben, müssen die entsprechenden Systemanforderungen des einzelnen Programms aufaddiert werden.

2.1 Windows 11

Microsoft Windows 11 hat eine deutlich höhere Systemanforderung als Windows 10. Sollten Sie Windows 11 nutzen, kommen diese Systemanforderungen zusätzlich zu unseren Mindestanforderungen hinzu. Für den Betrieb von Windows 11 wird folgende Hardware benötigt (Stand 09.2021):

- Einen unterstützten 64-Bit-Prozessor mit mindestens zwei Kernen und 1 GHz Leistung
- 8 GB Arbeitsspeicher
- 64 GB Festplattenspeicher
- ein TP-Modul Version 2.0
- eine DirectX 12-kompatible-Grafikkarte oder APU
- Bildschirm mit 1.280 x 720 Pixeln und mindestens 19 Zoll

2.2 Server

2.2.1 Mindestanforderungen

- Prozessor (CPU): Intel CPU Generation i5 QuadCore Desktop 2 GHz oder vergleichbar
- Arbeitsspeicher (RAM): 8 GB
- Festplattenkapazität (HD): 200 GB
- DVD-Laufwerk mit Schreibfunktion (Double-Layer)
- Netzwerkverbindung mit 1 Gbit/s

2.2.2 Empfohlene Hardware

- Prozessor (CPU): CPU Xeon Quad-Core
- Arbeitsspeicher (RAM): 16 GB (bei Terminal-Server-Betrieb ist der RAM-Speicher entsprechend größer zu dimensionieren. Siehe Kapitel 3.4)
- Festplatte(n):
 - SAS-HDD oder SSD Festplatten im redundanten RAID-Festplattenverbund
 - Raid-Controller mit Absicherung des Schreibcache bei Stromausfall bzw. plötzlichem Ausfall des Servers
 - Aktiviertes TPM-Modul mit Verschlüsselung der Partitionen

2.3 Arbeitsplatz-Computer

2.3.1 Mindestanforderungen

- Prozessor (CPU): Intel CPU Generation i3 DualCore Desktop 1,6 GHz oder vergleichbar
- Arbeitsspeicher (RAM): 4 GB
- Festplatte (HD): 50 GB
- DVD-Laufwerk mit Schreibfunktion (Double-Layer)
- Netzwerkverbindung mit 100 Mbit/s

2.3.2 Empfohlene Hardware

- Prozessor (CPU): CPU Core i7
- Arbeitsspeicher (RAM): 8 GB
- Festplatte (HD): SSD mit 120 GB und mindestens 25 GB freier Kapazität für Installation/Update
- Netzwerkverbindung mit 1 Gbit/s

2.4 Arbeitsplatz-Monitor

2.4.1 Mindestanforderungen

Gemäß der derzeit gültigen Bildschirmarbeitsverordnung (BildscharbV) ist für Arbeitsplätze eine Bildschirmgröße (Diagonale) von mindestens 19" (Bildschirmauflösung 1280x1024) vorgegeben. Monitore mit einer größeren Bildschirmdiagonale sowie einer höheren Bildschirmauflösung sind empfehlenswert.

2.4.2 Empfohlene Monitorunterstützung

Wir empfehlen den Einsatz von 24" Monitoren mit einer Bildschirmauflösung von 1920x1080. Um das bestmögliche Ergebnis zu erreichen, verwenden Sie einen Monitor mit Seitenverhältnis 16:9 oder 16:10.

Bei größeren Monitoren, bzw. solchen mit abweichendem Seitenverhältnis, empfehlen wir, die nativen Einstellungen beizubehalten. Auflösungen können nach unten hin variabel eingestellt werden. Das Bild muss dann jedoch bei unterschiedlichen Auflösungen über die verschiedenen Monitoreinstellungen, wie z. B. die Skalierung, angepasst werden.

2.4.3 Anzeigeeinstellungen unter Windows

Unter älteren Windows-Versionen haben Sie noch die Möglichkeit, individuelle Einstellungen bzgl. der Größenänderung einzelner Elemente wie Titelleisten, Menüs etc. vorzunehmen. Unter Windows 10 entfallen diese individuellen Konfigurationsmöglichkeiten jedoch seit dem Windows-Update 1703.

Sie wurden zu einer einheitlichen prozentualen Skalierung von Texten, Apps und anderen Elementen zusammengefasst. Eine eingegebene Skalierungsgröße wirkt sich daher auf alle Elemente gleichermaßen aus.

Hieraus ergibt sich der Nachteil, dass es bei Abweichungen vom Format 16:9 oder 16:10 und höheren Auflösungen als 1920x1200 zu Seiteneffekten, wie kaum leserlichen Menüleisten oder Titelzeilen, zu groß skalierten Untermenüs etc. kommen kann. Sollte dies auch bei Ihnen zutreffen, so sprechen Sie mit Ihrem CGM TURBOMED Vertriebs- und Servicepartner (VSP), der Sie gerne bei der Einrichtung berät.

2.5 Ausfallsicherheit

2.5.1 Unterbrechungsfreie Stromversorgung (USV)

Für einen Server ist der Einsatz einer "Unterbrechungsfreien Stromversorgung" dringend empfohlen. Diese Geräte schützen den Server vor Spannungsspitzen im Stromnetz und 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.

2.5.2 Redundante Netzteile

Je nach Ihren Anforderungen an die Ausfallsicherheit Ihres Systems, kann es erforderlich sein, dass redundante Netzteile in Ihrem Server verbaut sind. Diese Maßnahme ist optional und daher empfehlen wir hierzu, dass Sie sich bei Fragen mit Ihrem CGM TURBOMED Vertriebs- und Servicepartner (VSP) in Verbindung setzen.

2.5.3 RAID-Controller

Ein RAID-System bestehend aus mehreren Festplatten ist ebenfalls von Vorteil und kann entweder auf Geschwindigkeit oder Datensicherheit ausgelegt werden. Hierbei sollte das RAID als RAID-5 oder

RAID-10, jedoch mindestens als RAID-1 angelegt werden. Sollten Sie dennoch Fragen haben oder Hilfe benötigen, dann wenden Sie sich vertrauensvoll an Ihren Vertriebs- und Servicepartner (VSP).

3 Netzwerkkonfiguration

3.1 Internetanbindung (DSL) / Router

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

3.1.1 Mindestanforderungen

Für das reibungslose Übertragen von Daten (Senden und Empfangen) wird eine Übertragungsrate von mindestens 6 Mbit/s benötigt (dies entspricht einem DSL 6000-Anschluss).

3.1.2 Empfohlene Anbindung

Wir empfehlen, auch um den Support im Bedarfsfall zu erleichtern, eine Übertragungsrate von mindestens 16 Mbit/s (dies entspricht einem DSL 16000-Anschluss).

3.2 Netzwerk (LAN)

Eine Kupferverkabelung ist, sofern **nicht** anders definiert, für eine Client- und Server-Endgeräteeinbindung zu verwenden. Für den Serverbereich kann aufgrund von verschiedenen Technologien eine LWL-Anbindung (Lichtwellenleiter) notwendig sein. Für PCs, Notebooks, Messgeräte oder andere Geräte mit Netzwerkanschluss muss eine Kupferverkabelung als Anbindung an das Praxisnetzwerk vorgesehen werden. Für die strukturierte Verkabelung sind mindestens Kabel der Kategorie CAT6A und passende CAT6A-Netzwerkdosen und Netzwerkkomponenten (Patchpanels, Switches etc.) mit RJ45-Steckern bzw. -buchsen vorzusehen.

3.3 Managed Firewall (ITSS) Proaktiver Schutz der Praxis-IT

Die CGM MANAGED FIREWALL ist eine All-in-one Lösung, die Ihr Netzwerk umfassend vor unerwünschten Zugriffen schützt. Sie bietet Ihnen integrierte, mehrschichtige Sicherheit: Firewall, IPS, Antivirus, Anti-Bot, Applikations-Kontrolle, URL-Filterung und E-Mail-Sicherheit - und dies alles kombiniert in einem kleinen kompakten Gehäuse.

Die CGM MANAGED FIREWALL beschützt Ihre Daten. Dabei hält unser Team den Schutzschirm immer auf dem aktuellsten Stand: Anpassungen der Sicherheitsstrategie und Updates erfolgen automatisch im Hintergrund. Die CGM MANAGED FIREWALL sorgt für maximale Datensicherheit - heute und in Zukunft.

Mit der CGM MANAGED FIREWALL sichern Sie Ihr IT-System gegen **nicht** gewünschte Netzwerkzugriffe. Die Lösung überwacht den laufenden Datenverkehr und entscheidet anhand festgelegter, intelligenter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden. Gleichzeitig werden Angriffe von außen aufgespürt und bekämpft. Mit der einzigartigen SandBlast-Funktion werden auch bislang unbekannte Bedrohungen entdeckt. Dieser Zero-Day-Schutz umfasst im Besonderen eingehende E-Mails, die heutzutage das Haupteinfallstor für Malware, Trojaner etc. sind. Unbekannte Dateien leitet die Firewall an das CGM-Rechenzentrum in Frankfurt. In der sogenannten CGM Threat Cloud findet nahezu in Echtzeit eine Überprüfung auf eine etwaige Bedrohung statt.

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

3.4 Verkabelung / Architektur

3.4.1 Terminal-Server-Betrieb

CGM TURBOMED ist für den Einsatz im Terminal-Server-Betrieb freigegeben. Bei der Ermittlung der Terminal-Server-Hardware muss der Bedarf an Arbeitsspeicher, Prozessorleistung und die im Server vorhandene Grafikkarte gemäß den Anforderungen des Kunden individuell definiert werden (z.B. Anzahl der Benutzer sowie den Umfang der eingesetzten Software der einzelnen Terminal-Sitzungen). Pro Benutzer, welche gleichzeitig auf dem Terminalserver angemeldet sind, empfehlen wir mindestens 4 GB Arbeitsspeicher einzuplanen.

Da die Bemessung des passenden Servers auch von zukünftigen Praxisgegebenheiten abhängig ist, sollte die Konfiguration der passenden Hardware mit dem CGM TURBOMED Vertriebs- und Servicepartner (VSP) durchgeführt werden.

3.5 Außenstellenanbindung per Virtual Private Network (VPN)

3.5.1 Heimplatzanbindung

Zur stationären Heimplatzanbindung empfehlen wir einen verschlüsselten Remote-Desktop-Zugang (RDP). Der Praxis-Server benötigt dazu einen dauerhaft aktiven, leistungsfähigen DSL-Anschluss.

3.5.2 Verbindung zweier Netze (LAN-LAN-Kopplung)

Zur Außenstellenanbindung wird beidseitig mindestens ein DSL-Anschluss mit fester IP-Adresse empfohlen. Der jeweilige Anschluss sollte mit der Option [**Fast Path**] geschaltet sein, um eine

möglichst geringe Latenzzeit zu erhalten. Die benötigte Bandbreite ist abhängig von Größe und Nutzen der Außenstelle.

3.6 Mobile Endgeräte (Mobile Devices)

3.6.1 Tablet

Für eine mobile Nutzung von CGM TURBOMED wurde CGM TURBOMED MOBIL entwickelt. Per App kann auf iOS-Geräten auf den Praxisserver zugegriffen werden. Dabei können Patientendaten eingesehen und neue Dokumentationen abgelegt werden. Der Praxis-Server benötigt dazu einen dauerhaft aktiven und leistungsfähigen DSL-Anschluss.

3.6.2 Smartphone

CGM TURBOMED MOBIL wurde **nicht** für die Nutzung auf einem Smartphone konzipiert.

3.7 Monitoring (N-Central)

Wir empfehlen Ihnen, einen Service- oder Wartungsvertrag mit Ihrem CGM TURBOMED Vertriebs- und Servicepartner (VSP) abzuschließen und das Monitoring auf Ihrem Praxissystem zu installieren.

3.7.1 Mindestanforderungen

- Prozessor (CPU): x86 oder x64
- Arbeitsspeicher (RAM): 512 MB
- Verfügbare Festplattenkapazität (HD): 500 MB
- Sonstige Softwarekomponenten:
 - Microsoft .NET Framework 2.0.50727
 - Microsoft .NET Framework 4.5.2 (oder höher)

3.7.2 Empfehlung

- Betriebssystem: Windows 10 Pro

3.8 Endpoint Protection

3.8.1 Mindestanforderungen

- Prozessor (CPU): 1 GHz (32-Bit) Intel Pentium
- Arbeitsspeicher (RAM): 1 GB (100 MB exklusiv OfficeScan)
- Verfügbare Festplattenkapazität (HD): 800 MB
- Betriebssystem:
 - Windows 10 32-Bit / 64-Bit Home
 - Windows 10 32-Bit / 64-Bit Pro
 - Windows 10 32-Bit / 64-Bit Education
 - Windows 10 32-Bit / 64-Bit Enterprise
- Betriebssystemupdates:

- Anniversary Update
- Creators Update
- Fall Creators Update
- Sonstige Voraussetzungen:
 - Monitor mit einer Mindestauflösung von 1024x768 bei 256 (oder mehr) Farben
 - Windows Internet Explorer 11.0 bei webbasierter Installation
 - Remote-Registrierung aktiviert
 - Drucker-/Dateifreigabe in der Windows-Firewall zugelassen (falls aktiviert)
 - Standardmäßigen lokalen Administrator aktiviert

3.8.2 Empfohlene Hardware

- Prozessor (CPU): 2 GHz AMD/Intel 64-Bit-Prozessor
- Arbeitsspeicher (RAM): 2 GB
- Verfügbare Festplattenkapazität (HD): 1 GB

4 Geräte-Anbindung

4.1 Medizinproduktegesetz (MPG)

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

4.2 Barcode-Leser für den [Bundeseinheitlichen Medikationsplan] / das Modul [CGM BMP PLUS]

Für das Einlesen des Barcodes auf dem Bundeseinheitlichen Medikationsplan werden das Modul [CGM BMP Plus] (dieses muss freigeschaltet werden) und ein sogenannter Barcode-Leser benötigt. Aufgrund der speziellen Anforderungen sind derzeit ausschließlich Barcode-Leser der Marke Zebra verifiziert und zugelassen:

- Barcode-Leser Zebra DS4801 2D USB
- Barcode-Leser BT Zebra DS6878-HC 2D

Die Geräte sind über Ihren autorisierten CGM TURBOMED Vertriebs- und Servicepartner zu beziehen.

4.3 Drucker

Bei der Bedruckung von Papiervorlagen gibt es prinzipiell **keine** Einschränkungen bei der Druckerwahl. Zur Nutzung der Blankoformularbedruckung ist jedoch die Verwendung eines Laserdruckers vorgeschrieben. Eine druckerspezifische Zertifizierung ist dabei **nicht** notwendig.

Folgende Drucker wurden bereits erprobt und sind mit CGM TURBOMED kompatibel, woher wir empfehlen, auf eines dieser Modelle zurückzugreifen:

Nadeldrucker:

- Epson LQ-630
- Epson LQ-690
- Epson PLQ-20
- OKI ML5100FB
- Wenger PD 5

Laserdrucker (für Blankoformularbedruckung vorausgesetzt):

- Brother HL-L5100DN
- HP LaserJet Pro M102w
- Kyocera ECOSYS P2040dn
- Kyocera ECOSYS P3050dn
- Kyocera ECOSYS P3055dn
- Wenger MediPrint Z3
- Wenger MediPrint Z4

5 Betriebssysteme

CGM TURBOMED ist für die unten genannten Betriebssysteme auf Windows-kompatiblen Computern geprüft und zugelassen.

5.1.1 Server

- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2016 Datacenter
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2022 Standard
- Microsoft Windows Server 2022 Datacenter
- Microsoft Windows Server 2022 Essentials
- Microsoft Windows Server 2025 Standard
- Microsoft Windows Server 2025 Datacenter
- Microsoft Windows Server 2025 Essentials

5.1.2 Arbeitsstationen

- Windows 10 Professional, deutsche Version, 64-Bit
- Windows 11 Professional, deutsche Version, 64-Bit

Service-Pack

Anlehndend an die Aussage von Microsoft endet der Support eines Service Packs 24 Monate nach Erscheinen der nächsten Service Pack-Version.

Abkündigung

Alle zugelassenen Betriebssysteme werden bis zum Ablauf des "Extended Support" von Microsoft unterstützt. Eine Liste mit den entsprechenden Angaben zu den einzelnen Betriebssystemen des Herstellers Microsoft finden Sie unter <http://support.microsoft.com/gp/lifeselectindex>.

6 Konfiguration

6.1 Festplatten-Partitionen

6.1.1 Server

Die Festplattenkonfiguration ist entsprechend den zu erwartenden Anforderungen der Praxis anzupassen.

Ein RAID-System bestehend aus mehreren Festplatten ist hier von Vorteil und kann entweder auf Geschwindigkeit oder Datensicherheit ausgelegt werden. Hierbei sollte das RAID als RAID-5 oder RAID-10, jedoch mindestens als RAID-1 angelegt werden.

Ebenfalls ist die Trennung von Betriebssystem und Daten auf verschiedenen Partitionen anzuraten.

Die Größe der einzelnen Partitionen richtet sich nach

- dem eingesetzten Serverbetriebssystem (Minimalanforderungen sind durch Microsoft definiert)
- der mittelfristig in der Praxis zu erwartenden Datenmengen

Eine generelle Vorgabe kann **nicht** getroffen werden.

6.1.2 Arbeitsplatz

Es gibt **keine** bestimmten Anforderungen an die Festplattenkonfiguration an einem Arbeitsplatz. Jedoch sollte der freie Speicherplatz 25 GB **nicht** unterschreiten.

6.2 Virtualisierung

Die Virtualisierung eines CGM TURBOMED-Servers ist möglich. Beim Einsatz von Virtualisierungslösungen muss die Hardware jedoch entsprechend dimensioniert sein, um **keine** Performanceeinbußen bei der Verwendung von CGM TURBOMED befürchten zu müssen.

Auch die Datensicherung in einer virtuellen Umgebung muss fachgerecht durchgeführt werden, um Datenverluste zu vermeiden.

Eine Virtualisierung von CGM TURBOMED ist sowohl mit VMware als auch mit Microsoft Hyper-V möglich.

Eine Umsetzung sollte ausschließlich durch Ihren CGM TURBOMED Vertriebs- und Servicepartner (VSP) erfolgen.

6.3 Netzwerkkonfiguration

6.3.1 TCP/IP-Adressierung

Die Konfiguration des Adressbereiches richtet sich nach den Anforderungen in Ihrer Praxis. Auch die Verwendung von DHCP oder festen IP-Adressen richtet sich nach Ihrem individuellen Bedarf und kann sich von Praxis zu Praxis unterscheiden.

6.3.2 Firewall-Regeln

Bei der Konfiguration der Firewall sollte die Deny-All-Strategie angewendet werden. Diese besagt: "Alles, was **nicht** ausdrücklich erlaubt ist, bleibt verboten!". Nur durch diese Strategie kann ein erhöhter Schutz vor ungewolltem Eindringen in das Praxisnetzwerk angenommen werden.

6.3.3 Portfreischaltungen

Je nach eingesetzter Software sind Portfreischaltungen notwendig, um die Funktion der Software gewährleisten zu können. Diese müssen dann entsprechend in den eingesetzten Firewalls und deren Richtlinien konfiguriert werden.

6.3.4 Portkonfiguration

Je nach eingesetzter Software können Portkonfigurationen notwendig werden. Dies ist insbesondere dann zur Gewährleistung der Softwarefunktionen notwendig, wenn entsprechende Ports bereits durch andere Software genutzt werden und somit **nicht** mehr zur Verfügung stehen. Ggf. sind zusätzlich entsprechende Konfigurationen auf den eingesetzten Routern notwendig.

7 IT-Sicherheit

Die Gewährleistung von IT-Sicherheit und Datenschutz ist in der Medizinbranche von größter Bedeutung. CGM TURBOMED 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 PC Log-In-Funktionen, den Betriebssystemen, Firewall- und Port-Einstellungen und externen Softwarelösungen.

7.1 Allgemeine Empfehlungen zur IT-Sicherheit

- **Regelmäßige Updates:** Halten Sie sowohl Ihre CGM TURBOMED 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 TURBOMED zu definieren, um Datenzugriffe zu steuern.
- **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 TURBOMED**.
- **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**).

7.2 Betriebssysteme

- **Unterstützte Betriebssysteme:** Stellen Sie sicher, dass Sie eine unterstützte Version des Betriebssystems verwenden (z. B. Windows 10, Windows 11). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM TURBOMED.
- **Sicherheitseinstellungen:** Aktivieren Sie die integrierten Sicherheitsfunktionen des Betriebssystems, wie Windows Defender, um zusätzlichen Schutz vor Malware und Viren zu gewährleisten.

7.3 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 TURBOMED 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.

7.4 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.

7.5 PC Log-In

- **Sichere Anmeldeverfahren:** Nutzen Sie die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA) beim Login in die CGM TURBOMED 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 TURBOMED eingesehen werden.

7.6 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 TURBOMED und halten Sie diese Software ebenfalls regelmäßig geupdated.
- **Datenschutzbestimmungen:** Beachten Sie stets die datenschutzrechtlichen Bestimmungen und stellen Sie sicher, dass die externe Software die notwendigen Maßnahmen zum Schutz sensibler Patientendaten umsetzt.

7.7 Schlussfolgerung

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

8 Installation

8.1 Rechnernamen

Der Rechnername darf **keine** Umlaute enthalten. Ansonsten sollten die einzelnen Systeme aussagekräftige Namen besitzen, um in einem Support- und Fernwartungsfall schnellstmöglich einen Überblick über das Netzwerk zu erhalten. Dabei sollten Serversysteme auch einen entsprechenden Hinweis im Computernamen besitzen, um diesen schnellstmöglich als Server identifizieren zu können. Die Clientnamen sollten ebenfalls eindeutige Namen besitzen, um diese zuordnen zu können. Hier empfiehlt sich eine durchgängige Nummerierung der einzelnen Clients im Netzwerk.

8.2 Domäne

Die Verwendung einer Domäne ist ab fünf Arbeitsplätzen anzuraten. Hierdurch wird der Konfigurationsaufwand im Gegensatz zur Konfiguration einzelner Arbeitsplätze erheblich reduziert.

8.3 Freigaben (Verzeichnisse)

Damit CGM TURBOMED ordnungsgemäß funktioniert, wird im Rahmen der Installation das CGM TURBOMED-Installationsverzeichnis (bspw. [C:\TurboMed]) im gesamten Praxisnetz freigegeben.

8.4 Umgebungsvariablen

CGM TURBOMED benötigt für den Betrieb **keine** eigenen Umgebungsvariablen. Jedoch können durch einzusetzende Fremdsoftware (wie bspw. das KBV-Prüfmodul) Angaben in den Umgebungsvariablen notwendig sein. Als Beispiel wäre hier Java zu nennen.

8.5 Dienstemanagement

Durch die Installation von CGM TURBOMED können neue Windows-Dienste angelegt werden. Diese müssen bspw. bei der Datensicherung berücksichtigt werden. Zusätzlich können neue Windows-Dienste im Rahmen eines CGM TURBOMED-Updates angelegt werden, die zur Gewährleistung einer reibungslosen Funktion von CGM TURBOMED notwendig sind.

8.6 Datenbank

Die eingesetzte Datenbank von CGM TURBOMED ist eine objektorientierte Datenbank des Herstellers [**Versant**]. Derzeit kommt [**Versant FastObjects 12**] zum Einsatz und wird regelmäßig im Rahmen eines CGM TURBOMED-Updates aktualisiert.

8.7 Virenschutz

Ein Virenschutz ist auf jedem Computer in der Praxis zu installieren und zu konfigurieren. Hierbei sollte der Virens Scanner automatisch nach aktuellen Virendefinitionsupdates suchen und sich selbst aktualisieren.

Für den reibungslosen Betrieb von CGM TURBOMED ist die Konfiguration des Virens Scanners unabdingbar. Hier muss neben der Datei [**TurboMed.exe**] einige weitere Module in Abhängigkeit Ihrer Nutzung als Ausnahme eingetragen werden:

CGM ASSIST	[C:\TurboMed\Programm\WinS\wkflsr32.exe]
CGM BUBBLEMANAGER	[C:\TurboMed\Programm\WinS\bubblemanagerhostsystem.exe]
CGM MinervaHostsystem	[C:\TurboMed\Programm\WinS\MinervaHostsystem.exe]
ZULU Platform x32 Architecture	[C:\CG\Java\bin\javaw.exe]
ifap PraxisCENTER	[C:\ifapDB\praxisCENTER3\ipc.exe]

Grund: CGM TURBOMED muss bspw. Software der KBV verwenden, welche die Abrechnungsdaten verschlüsselt. Ein Virens Scanner könnte diese Verschlüsselung fälschlicherweise als einen Krypto-Trojaner interpretieren und daher die zum Betrieb von CGM TURBOMED notwendige Datei [**TurboMed.exe**] vom System löschen.

Zusätzlich kann es im Rahmen eines CGM TURBOMED-Updates erforderlich sein, den Virenschutz temporär zu deaktivieren, um den Installationsvorgang zu beschleunigen und **nicht** zu gefährden, da andernfalls einige Dateien fälschlicherweise als Virus erkannt und gelöscht werden könnten.

8.8 Server-Einstellungen

Um eine reibungslose Funktion von CGM TURBOMED sicherzustellen, ist es erforderlich, dass einige Systemkomponenten, z. B. durch den Windows-Autostart, beim Systemstart automatisch mit gestartet werden.

Die erforderlichen Dienste sind so konfiguriert, dass diese automatisch starten. Hier sollten **keine** Änderungen an der Konfiguration vorgenommen werden.

8.9 Arbeitsplatz-Einstellungen

Um eine reibungslose Funktion von CGM TURBOMED sicherzustellen, ist es erforderlich, dass einige Systemkomponenten, z. B. durch den Windows-Autostart, beim Systemstart automatisch mit gestartet werden. Auch hier sollten **keine** Änderungen an der Konfiguration vorgenommen werden.

8.10 Betriebssystem-Einstellungen

Das Betriebssystem sollte so eingestellt werden, dass ein maximaler Schutz gegen unbeabsichtigtes Löschen von Daten sowie Ausführen unerwünschter (Schad)Software existiert und eine Prüfung auf das Ausführen unerwünschter Dateien (Dateiausführungsverhinderung) konfiguriert ist.

Zusätzlich sollte das Betriebssystem immer auf dem aktuellsten Updatestand gehalten werden, um mögliche Sicherheitslücken rechtzeitig zu schließen.

Die Konfiguration der Windows-Benutzer mit eingeschränkten Zugriffsrechten und eingeschalteter Benutzerkontensteuerung (UAC) sind elementare Sicherheitsmechanismen und sollten daher keinesfalls deaktiviert werden.

Des Weiteren sollte jeder Mitarbeiter einen eigenen Windows-Benutzer mit entsprechenden Zugriffs- und Sicherheitsberechtigungen erhalten und benutzen.

8.11 Standard-Software

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

- Internet Explorer Version 10 (oder aktueller)
- CompuGroup JAVA Version 17.0.3
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 4.5.2 (oder aktueller) - wird von CGM TURBOMED installiert
- Visual C++ 2005 Service Pack 1 x86 - wird von CGM TURBOMED installiert
- Visual C++ 2008 Service Pack 1 x86 - wird von CGM TURBOMED installiert

- Visual C++ 2010 Service Pack 1 x64 - wird von CGM TURBOMED installiert
- Visual C++ 2010 Service Pack 1 x86 - wird von CGM TURBOMED installiert
- Visual C++ 2012 x86 - wird von CGM TURBOMED installiert
- Visual C++ 2013 x86 - wird von CGM TURBOMED installiert
- Visual C++ 2015 x86 - wird von CGM TURBOMED installiert
- Adobe Acrobat Reader in seiner aktuellen Version
- Virenschutz

Jeder Computer, auch solche ohne Anbindung an das Internet/Intranet, muss über ein Virenschutzprogramm verfügen. Die regelmäßige, am besten tägliche, Aktualisierung des Virenschutzes ist dabei essentiell.

Für optimale Sicherheit ist ein kostenloses Programm aus dem Internet **nicht** ausreichend. Wir empfehlen als Minimallösung den Einsatz des Produktes **[McAfee VirusScan Enterprise]**. Weitere professionelle Lösungen können über die autorisierten CGM TURBOMED Vertriebs- und Servicepartner (VSP) bezogen werden.

8.12 Office-Anwendungen

Für die Briefschreibung oder auch für Auswertungen werden von CGM TURBOMED aktuelle Microsoft Office-Anwendungen empfohlen.

Als Textverarbeitung ist eine Schnittstelle zu Microsoft Word in CGM TURBOMED integriert. Für folgende Microsoft Word-Versionen ist CGM TURBOMED freigegeben:

- Microsoft Word 2010, 32-Bit, deutsche Version
- Microsoft Word 2013, 32-Bit, deutsche Version
- Microsoft Word 2016, 32-Bit, deutsche Version
- Microsoft Word 2019, 32-Bit, deutsche Version (laut Microsoft erst ab Windows 10 nutzbar)
- Microsoft Word 2024, 32- & 64-Bit, deutsche Version

8.13 Online-Update(s)

CGM TURBOMED bietet die Möglichkeit, alle CGM TURBOMED-Updates online zu beziehen. Diese finden Sie auf unserer Webseite <https://service.turbomed.de>. Zusätzlich lassen sich CGM TURBOMED-Updates über das **CGM SMART UPDATE** automatisch und im Hintergrund herunterladen. Informationen hierzu finden Sie auf der Webseite: www.cgm.com/turbomed-smartupdate.

8.14 Fernwartung

Für die, durch CGM TURBOMED durchgeführte, Fernwartungen wird primär die Software **[Any-Desk]** verwendet. Diese wird standardmäßig zusammen mit CGM TURBOMED ausgeliefert. Der Aufruf erfolgt wie gewohnt über das Fragezeichen **[?]** in der CGM TURBOMED-Menüleiste. Klicken Sie hier auf den Eintrag **[CGM REMOTE Support]**¹.

9 Datensicherung

Es ist eine tägliche Datensicherung der patientenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen durchzuführen. Wir schlagen daher vor, dass Sie eine vollständige Daten-sicherung des gesamten Server-Systems vornehmen. Je nach Konfiguration des Systems empfehlen wir darüber hinaus auch die Sicherung sämtlicher Arbeitsplätze. Zur Abstimmung und individuellen Einschätzung ziehen Sie Ihren CGM TURBOMED Vertriebs- und Servicepartner (VSP) hinzu.

10 Datensicherheit und Verschlüsselung

Es wird empfohlen Softwareprogramm **[BitLocker]** zu verwenden. Diese Verschlüsselung beeinträchtigt die Nutzung von CGM TURBOMED **nicht**.

11 Einrichtung spezifischer Software

Sollte weitere, spezifische Software auf Ihrem System eingerichtet werden, so ist in jedem Fall der CGM TURBOMED Vertriebs- und Servicepartner (VSP) einzubeziehen, um die gesonderten Systemvoraussetzungen der spezifischen Software zu berücksichtigen.

Sollten die Systemanforderungen in der Praxis von den in diesem Dokument genannten Systemanforderungen für den Betrieb von CGM TURBOMED abweichen, kann es zu Beeinträchtigungen beim Betrieb von CGM TURBOMED kommen.

Für weiterführende Fragen wenden Sie sich gerne direkt an Ihren autorisierten CGM TURBOMED Vertriebs- und Servicepartner (VSP).

12 Das Hilfe-System von CGM TURBOMED

12.1 Hinweise zur Nomenklatur in diesem Dokument

Um einzelne Steuer- oder Anzeigeelemente sowie Eingabetexte in diesem Dokument so zu kennzeichnen, dass sie sowohl bei der Anzeige auf Ihrem Monitor als auch bei einem Schwarz-Weiß-Ausdruck gut zu identifizieren sind, wird auf eine eindeutige Formatierung des erklärenden Textes zurückgegriffen, die folgenden Formatierungsregeln unterliegt:

- **[alle Steuer- oder Anzeigeelemente sowie Eingabetexte, Pfadangaben, Aufrufpfade, Hyperlinks und andere Verlinkungen in eckigen Klammern]**
- [\[Pfadangaben in einer Dateistruktur, sowie Aufrufpfade innerhalb des Programms in blau und in eckigen Klammern\]](#)
- [Hyperlinks oder andere Verlinkungen in blau, unterstrichen](#)

12.2 CGM TURBOMED Gebrauchsanweisung [F1]

Bei Fragen zur Bedienung von CGM TURBOMED steht Ihnen direkt im Programm eine umfangreiche Gebrauchsanweisung zur Verfügung, die Sie an jeder beliebigen Programmstelle durch Betätigen der Taste **[F1]** aufrufen können. Diese öffnet sich in demjenigen Kapitel, das dem von Ihnen vor dem Betätigen der Taste **[F1]** verwendeten CGM TURBOMED-Modul entspricht. Über diesen kontextsensitiven Aufruf der Gebrauchsanweisung hinaus, steht Ihnen selbstverständlich auch eine Suchfunktion zur Verfügung, die Ihnen das Auffinden weiterer Kapitel erleichtert.

12.3 CGM TURBOMED Anwender-Hotline

WIR SIND FÜR SIE DA!

Hotline & Servicezeiten

Telefon: +49 (0) 261 8000-2345¹

Fax: +49 (0) 261 8000-3345

E-Mail: hotline.turbomed@cgm.com

oder im Internet unter cgm.com/turbomed

¹ Unsere Hotline-Zeiten: Montag bis Freitag von 08:00 bis 19:00 Uhr außer an bundeseinheitlichen Feiertagen.

CompuGroup Medical Deutschland AG

Geschäftsbereich TURBOMED

Maria Trost 23, 56070 Koblenz

T +49 (0) 261 8000-2345

F +49 (0) 261 8000-3365

info@turbomed.de

cgm.com/turbomed

cgm.com/de

